

2019

# Empirical Assessment of Mobile Device Users' Information Security Behavior towards Data Breach: Leveraging Protection Motivation Theory

Anthony Duke Giwah

Nova Southeastern University, [adgiwah@gmail.com](mailto:adgiwah@gmail.com)

This document is a product of extensive research conducted at the Nova Southeastern University [College of Engineering and Computing](#). For more information on research and degree programs at the NSU College of Engineering and Computing, please click [here](#).

Follow this and additional works at: [https://nsuworks.nova.edu/gscis\\_etd](https://nsuworks.nova.edu/gscis_etd)

Part of the [Computer Sciences Commons](#)

## Share Feedback About This Item

---

### NSUWorks Citation

Anthony Duke Giwah. 2019. *Empirical Assessment of Mobile Device Users' Information Security Behavior towards Data Breach: Leveraging Protection Motivation Theory*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (1073)  
[https://nsuworks.nova.edu/gscis\\_etd/1073](https://nsuworks.nova.edu/gscis_etd/1073).

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact [nsuworks@nova.edu](mailto:nsuworks@nova.edu).

Empirical Assessment of Mobile Device Users' Information Security Behavior  
towards Data Breach: Leveraging Protection Motivation Theory

by  
Anthony Duke Giwah

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

College of Engineering and Computing  
Nova Southeastern University

2019

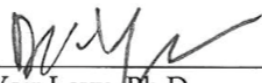
We hereby certify that this dissertation, submitted by Anthony Giwah, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

  
Ling Wang, Ph.D.  
Chairperson of Dissertation Committee

3/28/2019  
Date

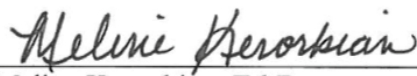
  
Inkyoung Hur, Ph.D.  
Dissertation Committee Member

3/28/2019  
Date

  
Yair Levy, Ph.D.  
Dissertation Committee Member

3/28/2019  
Date

Approved:

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

3/28/2019  
Date

College of Engineering and Computing  
Nova Southeastern University

2019

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

## Empirical Assessment of Mobile Device Users' Information Security Behavior towards Data Breach: Leveraging Protection Motivation Theory

by  
Anthony Duke Giwah  
March 2019

User information security behavior has been an area of growing demand in information systems (IS) research. Unfortunately, most of the previous research done in user information security behavior have been in broad contexts, therefore creating a gap in the literature of similar research that focuses on specific emerging technologies and trends. With the growing reliance on mobile devices to increase the flexibility, speed and efficiency in how we work, communicate, shop, seek information and entertain ourselves, it is obvious that these devices have become data warehouses and platform for data in transit.

This study was an empirical and quantitative study that gathered data leveraging a web-survey. Prior to conducting the survey for the main data collection, a Delphi study and pilot study were conducted. Convenience sampling was the category of nonprobability sampling design used to gather data. The 7-Point Likert Scale was used on all survey items. Pre-analysis data screening was conducted prior to data analysis. The Partial Least Square Structural Equation Modeling (PLS-SEM) was used to analyze the data gathered from a total of 390 responses received.

The results of this study showed that perceived threat severity has a negative effect on protection motivation, while perceived threat susceptibility has a positive effect on protection motivation. Contrarily, the results from this study did not show that perceived response cost influences protection motivation. Response efficacy and mobile self-efficacy had a significant positive influence on protection motivation. Mobile device security usage showed to be significantly influenced positively by protection motivation. This study brings additional insight and theoretical implications to the existing literature. The findings reveal the PMT's capacity to predict user behavior based on threat and coping appraisals within the context of mobile device security usage. Additionally, the extension of the PMT for the research model of this study implies that mobile devices users also can take recommended responses to protect their devices from security threats.

## Acknowledgements

I would like to sincerely thank and extend profound gratitude to my chair person, Dr. Ling Wang for the step-by-step guidance, supervision and encouragement throughout the entire dissertation process. Dr. Ling Wang is a phenomenal professor and I could not have reached the various milestones without her meticulous stewardship.

This study would not have come to successful completion without the support and invaluable input from Dr. Yair Levy and Dr. Inkyoung Hur who sat on the dissertation committee. Dr. Yair Levy's extensive knowledge in the field of Information Systems is one to aspire for. Additionally, Dr. Inkyoung Hur's attention to detail and knowledge of the literature always led to insightful feedback. I was simply blessed to have such a committee.

My gratitude goes to my aunt, Mrs. Margaret Armanio who has continuously given me support and encouragement from thousands of miles away. This doctoral degree is one of the many pursuits of mine she inspired. I also dedicate this to my daughter, Eleora Duke with the words from the poem "The Ladder of St. Augustine" by Longfellow (1851), "The heights by great men reached and kept, / Were not attained by sudden flight, / But they, while their companions slept, / Were toiling upward in the night " (p. 286).

# Table of Contents

**Abstract** iii

**List of Tables** vii

**List of Figures** viii

## **Chapters**

### **1. Introduction 1**

Background 1

Problem Statement 2

Dissertation Goal 6

Research Question 8

Hypotheses 8

Relevance and Significance 14

Barriers and Issues 16

Assumptions 17

Limitations 17

Delimitations 17

Summary 18

### **2. Literature Review 19**

Overview 19

Theoretical Foundation 19

Past Literature and Identification of Gaps 24

Analysis of the Research Methods Used 28

Mobile Device Data Breach 29

Synthesis of the Literature 30

Summary 31

### **3. Methodology 32**

Overview of Research Methodology/Design 32

Research Method 32

Instrument Development and Validation 34

Ethical Consideration 42

Population and Sample 42

Pre-analysis Data Screening 44

Data Analysis Strategy 45

Format for Presenting Results 45

Resource Requirements 46

Summary 46

### **4. Results 48**

Pre-Analysis Data Screening 48

Data Analysis 51

Findings 54

## **5. Conclusions, Discussion, Limitations and Summary 57**

Conclusions 57

Discussion 60

Limitations and Future Studies 64

Summary 65

## **Appendices**

A. Survey Questionnaire 68

B. IRB Approval 73

C. Mahalanobis Distance and Box Plot 74

D. Rerun of Mahalanobis Distance and Box Plot after deleting Extreme Cases 77

E. Normality and Scatter Plot 80

F. PLS Analysis 82

G. Model Fit, Reliability and Validity, Coefficient, Outer Loading 83

H. Rerun of PLS Analysis with RE5, RE6, MDSU5, MDSU6, and MDSU7 deleted 87

I. Model Fit, Reliability and Validity, Coefficient, Outer Loading 88

J. Significance with Bootstrapping 91

## **References 93**

## **List of Tables**

### **Tables**

1. Constructs Items and Instrument Source 37
2. Construct Reliability and Validity 52
3. Model Fit and Accepted Values 53
4. Discriminant Validity 54
5. Summary of Hypotheses Tests 56



## **List of Figures**

### **Figures**

1. Proposed Research Model 8
2. PLS Analysis Result for Mobile Device Security Usage 55

## Chapter 1

### Introduction

#### **Background**

Mobile devices are transforming the way we collect, process, and store data. While the growth in their use can be attributed to the convenience they offer, mobile device users, however, face data theft and breaches as they rely more on these emerging technologies for task performance and everyday experiences. Mobile device user behavior has been cited as a significant factor for these data breaches. Zahadat, Blessner, Blackburn, and Olson (2015) pointed out that data breach is a significant problem and a major factor of information security violation, because of users' failure to adhere to best security practices when using personal mobile devices.

According to Goode, Hoehle, Venkatesh, and Brown (2017), the Verizon Business 2015 report revealed that a minimum of five major data breach incidents occur each day. The Ponemon Institute study in 2015 also revealed that data breaches occurred either due to insider user negligence or deliberate attempts, which have resulted in costs beyond \$4 million for victimized organizations (Tyler, 2016). In an earlier Ponemon Institute 2013 industry survey report, it indicated that more than 40 percent data breaches are as a result of user negligence and non-compliance with security policies (Johnston, Warkentin, & Siponen, 2015). The Verizon 2013 annual data breach report also noted that "29% (percent) of the data breaches investigated were found to have leveraged social tactics, the human factor in circumventing data security" (Thompson, Ravindran, & Nicosia, 2015, pp. 320-321).

As mobile device usage through personal ownership and corporate deployment expands, the information security behavior of its users is becoming an important area of

focus for organizations alike. The need to understand the information security behavior of computing systems users is not a new phenomenon. As stated by Ögütçü, Testik, and Chouseinoglou (2016), “even the best technology that can be used to mitigate numerous IS security problems cannot work successfully unless the people in organizations do the right thing” (p. 83).

The challenge of protecting data from breaches is further compounded by the growth in mobile device usage which makes data more dispersed and easily available to both authorized and unauthorized persons. Warkentin, Johnston, Walden, and Straub (2016) noted that the increase in the use of personal mobile devices for work was also to account for the possibilities in data breaches due to the inability of users to follow security rules, either due to complacency or ignorance. As the security challenges presented by mobile devices and the need for secure user behavior has become more apparent, this research study intended to understand the factors that contribute to the information security usage of mobile device users. Previous studies have generally looked into user security behavior in information systems. However, a published study that researched mobile device security usage of mobile device users by determining the effects of perceived threat severity, perceived threat susceptibility, perceived response costs, response efficacy, mobile self-efficacy, and protection motivation has not been found.

### **Problem Statement**

There have been numerous studies done on user information security behavior. However, these previous studies, hence the existing literature, focus more broadly on computing systems and security, thereby leaving a vacuum for similar research that focuses on specific emerging technology trends and their associated security threats. This study was

an attempt to fill that gap by investigating the information security behavior of mobile device users in the context of data breach. Mobile devices certainly pose security challenges not common to traditional stationary computing systems, hence differences in the user behavior towards their security.

As pointed out by Tu, Turel, Yuan, and Archer (2015), mobile devices present unique risks that can lead to adverse outcomes, which explains the need for users to take special measures to reduce or prevent them. According to He, Chan, and Guizani (2015), the security principles of mobile devices are different compared to conventional computing systems, necessitating a different user security approach. Understanding the user behavior of mobile device users is highly important. Tu and Yuan (2012) pointed out that, 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. O'Neill (2014) and Tu et al. (2015) posited that the size of mobile devices makes them easy to take everywhere and they can easily get lost or stolen, thereby leading to the possibility of data loss through unauthorized access to the numerous data wielding applications on the devices. Additionally, Das and Khan (2016) noted that besides the possibility of losing mobile devices and the data they carry, mobile device users themselves expose them to risks of breach by connecting them to unsecure and vulnerable public networks.

Mobile devices have less security and data protection compared to computer systems that are stationed (Ben-Asher et al., 2011). Oberheide and Jahanian (2010) in an earlier study pointed out that malware and spyware detection through behavioral detection engines on mobile devices are inadequate. Compared to conventional computing systems, it is more difficult to effectively implement anti-malware and anti-spyware on mobile devices because

of their limited software platforms and this exposes them easily to malware and spyware (Oberheide & Jahanian, 2010). Mobile device software platforms are sometimes obscure and locked to mobile carriers which makes it challenging and difficult for mobile device users to update their anti-malware, anti-virus and firewall software, consequently exposing them to vulnerabilities that can lead to data breaches (Oberheide & Jahanian, 2010). In a study on mobile security, Li and Clark (2013) noted that mobile devices have become more vulnerable to data breach because users are significantly relying on numerous mobile applications which have the tendency to expose the devices to malicious codes. Oberheide and Jahanian (2010) found that attackers prefer more to engage in data breach attempts through malicious applications, and mobile devices present the vulnerable platform needed. Mobile device users often bear the responsibility to secure their own devices due to personal ownership, compared to enterprises equipped with better security tools for protecting stationary computing systems (Tu & Yuan, 2012). This phenomenon leaves mobile devices less protected and more vulnerable to data breach. As Leavitt (2011) pointed out, mobile encryption software for instance remains scarce than those for traditional computers, and the few available are difficult to find and unaffordable for users.

Willison and Warkentin (2013) and Crossler et al. (2013) mentioned that research in user information security behavior have generally always been high in demand. However, the few attempts made at research in information security and mobile devices together have looked into other issues rather than the security behavior of mobile device users. Some of the few studies around mobile devices are the works done by Keith, Thompson, Hale, Lowry, and Greer (2013) on information disclosure through location-based services on mobile devices, and the study by Allam, Flowerday, and Flowerday (2014) on smartphone

information security awareness. Lee, Warkentin, Crossler, and Otondo (2016) utilized the theory of planned behavior (TPB) to study user attitude in relation to their participation in a program that encourages the use of personal mobile devices for work. The technology acceptance model (TAM) and the theory of reasoned action (TRA) was relied upon by Lebek, Degirmenci, and Breitner (2013) to examine employee perceived concerns and perceived benefits, and its impact on their attitude towards using mobile devices.

The growing popularity and usage of mobile devices as the paramount computing tool for different activities cannot be understated (Kuznekoff & Titsworth, 2013). This is evident in how the majority of previous research attempts on mobile devices have focused on how users are leveraging mobile devices in unconventional ways and in areas such as: learning (Martin & Ertzberger, 2013), healthcare (Boruff, & Storie, 2014), and finance (Fenu & Pau, 2015). Even though it is clear that mobile device users are utilizing them in a myriad of ways, what still remains unexplored in the research on mobile devices is the information security usage behavior of its users in the context of data breach.

The lack thereof, or minimal exploration in this area may be attributed to the suggestion made by Alhogail, Mirza, and Bakry (2015) that within the information security 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 has become more commonly associated with security incidents. Flores and Ekstedt (2016) noted that, the unpredictability of human behavior makes it imperative to try to understand user information security behavior because it has become the weakest link, and the focus of information security compromise.

## **Dissertation Goal**

With the rise in data breaches targeting mobile device users, there was an opportunity to investigate the problem. The goal of this study was to verify, with empirical data, the antecedent factors that contribute to the information security usage of mobile device users in the context of data breach. Specifically, the purpose of the research was to determine the effect of the independent variables - perceived threat severity, perceived threat susceptibility, perceived response costs, response efficacy, mobile self-efficacy, and protection motivation on the dependent variable - mobile device security usage, towards the protection of data from breach. To accomplish this goal, this study proposed a research model and subsequent hypotheses based on the relationships between the constructs used. The research model was based on constructs from the protection motivation theory (PMT).

The rationale for leveraging the PMT is its potential to predict user security behavior with emphasis on the cognitive processes that mediate change in them (Rogers, 1983). Information security behavior and decisions of mobile device users are based on cognitive and decision heuristics (Almuhimedi et al., 2015). Tsohou, Karyda, and Kokolakis (2015) noted that cognitive factors influence users' information security behavior and their compliance or noncompliance decisions.

Boss et al. (2015) and Posey et al. (2015), posited that the PMT is based on threat appraisal and coping appraisal, and how these two components influence protection motivation. Hence the PMT constructs adapted for the development of the research model and the general purposes of study had perceived threat severity, perceived threat susceptibility, perceived response costs, response efficacy, and mobile self-efficacy, as

determinants of protection motivation, which directly influences mobile device security usage.

Previous researchers have relied on modified versions of the PMT constructs identified in this study to research the phenomena of user security behavior in various contexts. Posey, Roberts, and Lowry (2015) utilized threat severity, threat vulnerability, self-efficacy, and response costs in their study on the impact of organizational commitment on insiders' security behavior. Threat severity, threat vulnerability, self-efficacy, and response costs were adapted by Crossler and Bélanger (2014) in their study to develop a unified security practices (USP) instrument. Johnston and Warkentin (2010) in their study on fear appeals and information security behavior, used the PMT constructs of threat severity, threat susceptibility, and self-efficacy to develop the fear appeals model (FAM). Also, in an earlier study on how internet users can take more responsibility for their security behavior online, LaRose, Rifon, and Enbody (2008) leveraged the PMT constructs of threat severity and threat susceptibility to develop a framework for promoting safe online behavior.

The research model developed for this study has been presented as Figure 1. The PMT, constructs, and justification for leveraging them have been elaborated upon in chapter 2 - literature review. The research study intended to measure these constructs through the use of convenience sampling to collect data from a specific target group, and in this case, mobile device users. The unit of analysis in this study was individuals and the cross-sectional method was appropriate because there was no need for the collection of data at different points in time.

Also, by analyzing the data that was collected, it was the intention of this study to interpret the results and draw conclusions that will be useful to understanding the information



security behavior of mobile device users. An additional goal of this study was that the provision of recommendations will add to existing knowledge on mobile device security and the protection of data on mobile devices.

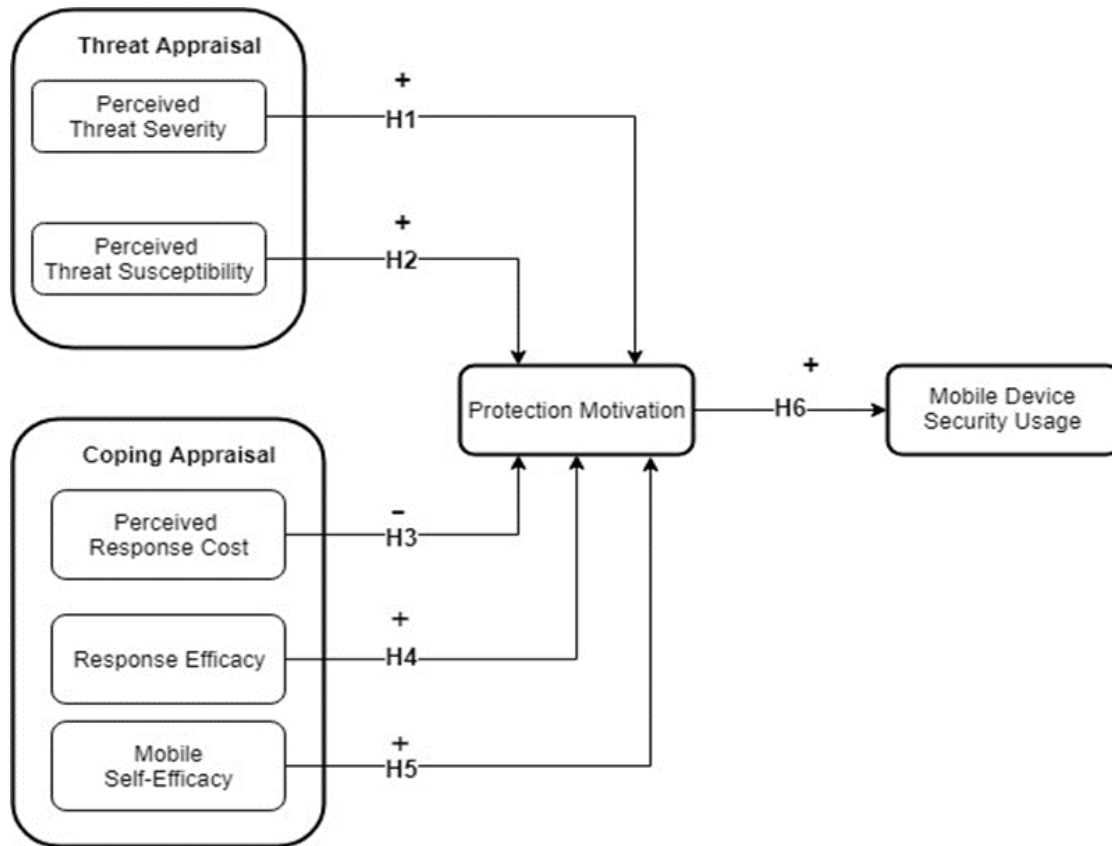


Figure 1: Proposed Research Model

## Research Question

Based on the constructs and elements that were leveraged for this study, the below research question was developed:

*RQ: What are the factors influencing the usage of mobile device security by users to protect their data from breach?*

## Hypotheses

The research model which was based on this study's foundational theory suggested that perceived threat severity, perceived threat susceptibility, perceived response costs,

response efficacy, and mobile self-efficacy are constructs that shape protection motivation, which leads to mobile device security usage. Based on the proposed research model, constructs relationships, and the research question, the highlighted hypotheses below were proposed for this study.

Warkentin, Johnston, Walden, and Straub (2016) in a recent study on fear appeals and the expectations of individuals behavior in security situations, noted that heightened threat severity led individuals to assess the effectiveness of their responses in mitigating the threat. As explained by Burns, Posey, Roberts, and Lowry (2017) in their recent research on how users capitalize their cognitive abilities in information security threat and coping mechanisms, they posited that a high level of perceived threat severity motivates users to take measures to protect themselves. Janis (1967) in an earlier study contended that adaptive response occurs when there is high level perception about threats, which then drives in users a motivation to eventually behave in a manner consistent with behavior that reduces or gets rid of the threat. Posey et al. (2015) asserted that threat severity influences users' protection motivation. Tu et al. (2015) also explained that users are likely to undertake adaptive responses due to increased perceptions of threat severity. 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. Based on this argument and positive association between threat severity and protection motivation, the below hypothesis was developed:

***H1: The higher the perceived threat severity of data breaches, the higher the protection motivation of mobile device users.***

When individuals perceive there is a high chance of being vulnerable to security threats, they tend to assess how it can be mitigated and conversely if they perceive minimal threat vulnerability or lack thereof, the response outcomes are negative (Herath & Rao, 2009). It can be deduced from Herath and Rao (2009) that the protection motivation by an individual is based on the perceived vulnerability to the threat. Dang-Pham and Pittayachawan (2015), argued that users are motivated to protect themselves if they perceive susceptibility to threats. Posey et al. (2015) considered threat susceptibility to be a “major component in the threat appraisal process and overall formation of insiders’ protection motivation” (p. 14). According to Workman et al. (2008), the perception of being vulnerable to threat leads to an assessment of coping appraisals that motivates users to protect themselves. This assertion was supported by Gutteling, Terpstra, and Kerstholt (2017) that when users perceive high threat susceptibility, they are motivated to undertake adaptive responses they are confident will protect them from the threat. Johnston and Warkentin (2010) in an earlier study pointed out that adaptive response is motivation or desire to undertake behavior that will positively protect one from threat. Vance et al. (2012) also emphasized that adaptive response towards threat is considered positive. With this background it can be deduced that there is a positive association between threat susceptibility and protection motivation. Based on this argument, the below hypothesis was proposed:

***H2: The higher the perceived threat susceptibility of data breaches, the higher the protection motivation of mobile device users.***

Posey et al. (2015) explained response cost as the perceived drawbacks such as expenses, disruptions, difficulties, and likely negative effects that users could incur if they undertake protective actions. In an earlier study, Herath and Rao (2009) noted that high

response cost negatively influences protection motivation. Herath and Rao (2009) added that it had been cited by employees for their lack of desire to adapt security practices as it restricts and impedes the routine flow of operational processes. Palardy, Greening, Ott, Dolderby, and Atchinson (1998) had also revealed earlier that response costs have a negative impact on protection motivation. Crossler and Bélanger (2014) posited that as “response cost goes up, the likelihood of performing the adaptive coping response goes down” (p. 7). Response cost drives users towards maladaptive responses, and as noted by Posey et al. (2015), it reduces the desire of users to perform adaptive response measures. Maladaptive responses according to Vance et al. (2012), is the negative response appraised from the cognitively mediating process in individuals when they perceive a threat. Bolkan and Goodboy (2016), noted that even if an individual believes there exists a strong ability to cope, a high response cost drives that individual away from adaptive responses. Based on this argument and the noted negative association between response cost and protection motivation, the below hypothesis was proposed:

***H3: The higher the perceived response cost to mitigate data breaches, the lower the protection motivation of mobile device users.***

Rogers (1975) in the seminal study that birthed the PMT described response efficacy as the degree to which a person is convinced that a proposed response will effectively prevent a threat. Johnston and Warkentin (2010) also posited that response efficacy is the level to which a person perceives the effectiveness of a response in mitigating a threat. Davis, Bagozzi, and Warshaw (1989) posited that the most influential predictor of protection motivation is response efficacy. Similarly, Posey et al. (2015) also asserted that response efficacy plays a more significant role in forming protection motivation than the threat

appraisal constructs. According to Johnston and Warkentin (2010), “moderate to high levels of response efficacy are associated with positive inclinations of threat mitigation whereby a recommended response is enacted” (p. 553). Posey et al. (2015) in their study on insider’s motivation to protection information assets found that response efficacy has a strong positive relationship with protection motivation. Based on this argument and the noted positive association between response efficacy and protection motivation, the below hypothesis was proposed:

***H4: The higher the response efficacy to mitigate data breaches, the higher the protection motivation of mobile device users.***

Bandura (1986) posited that self-efficacy is founded in social cognitive theory and it is “people’s judgments of their capabilities to organize and execute courses of action required to attain designated types of performances” (p. 391). Keith, Babb, Lowry, Furner, and Abdullat (2015) pointed out that self-efficacy was researched earlier on within the area of computer use and contextualized as computer self-efficacy (CSE). Hardin, Chang, and Fuller (2008) citing Marakas, Yi, and Johnson (1998) emphasized that self-efficacy as a construct must be developed to reflect the computing context within which it is used. Thus, contextualization of the self-efficacy construct into an ‘internet self-efficacy’ construct in a study on electronic service acceptance (Hsu & Chiu, 2004). Wang, Lin, and Luarn (2006) also stressed that self-efficacy is applicable in the context of mobile computing. Keith et al. (2015) added that adopting a mobile self-efficacy construct presents a more rigorous approach to understanding the protection behavior of mobile device users. In the case of mobile computing, it can be deduced from Chan et al. (2006) that mobile self-efficacy will lead mobile device users to develop an intention to protect their devices. Posey et al. (2015)

posited that self-efficacy is a high significant predictor of protection motivation in numerous and different contexts. Protection motivation was found to be the best measure of intent (Posey et al., 2015). Johnston and Warkentin (2010) in the study on fear appeals determined that self-efficacy is a direct determinant of intent. Self-efficacy was found to have a significant positive impact on intent (Johnston & Warkentin, 2010). Based on this argument and the noted positive association between mobile self-efficacy and protection motivation, the below hypothesis was proposed:

***H5: The higher the mobile self-efficacy to mitigate data breaches, the higher the protection motivation of mobile device users.***

Protection motivation is the “intervening variable that has the typical characteristics of a motive: it arouses, sustains and directs activity” (Rogers, 1975, p. 98). In a further explanation of protection motivation, Rogers (1983) posited that protection motivation is the variable that drives change in behavior. Pahnla, Siponen, and Mahmood (2007) found that the stronger the intent to comply with security policies, the higher the likelihood of actual compliance. Based on Palardy et al. (1998), Herath and Rao (2009) noted that behavior has also been considered as an extension or dependent variable of protection motivation. Johnston and Warkentin (2010) citing Rogers (1983) asserted that when threat appraisals and coping appraisals are at moderate-to-high levels, an individual’s protection motivation is equally increased, thereby significantly influencing actual behavior. Furthermore, Posey et al. (2015) pointed out that protection motivation is a very significant predictor of adaptive behavior. It can be deduced from the assertion by Posey et. al (2015) that the impact of protection motivation on behavior is not only significant but positively so. Based on this

argument and the noted positive association between protection motivation and mobile device security usage, the below hypothesis was proposed:

***H6: The higher the protection motivation of mobile device users, the more likely their mobile device security usage.***

### **Relevance and Significance**

This research focused on how understanding the information security behavior of mobile device users can help bring some clarity to data compromise, and also determine ways to better manage and protect data on mobile devices. The research drew on insights from information systems theories, credible and valid data that was critically analyzed quantitatively to shed light on trends. The findings were expected to help answer key questions for both academia and practice. Hence its significance was further stated as follows:

First, highlights the growing need for IS researchers to understand how the personalization and mobility of emerging and trending technologies brings with it, perceived threats such as data breach. Some researchers have argued that developments such as the use of personal mobile devices in some work places are the pervasive risks to data privacy (Junglas, Johnson, & Spitzmüller 2008). Since this study focused on mobile devices and data breach, it provides the foundation for an alternative explanation to how users of mobile devices should behave to ensure the security of their data.

Also, it is important for IS researchers to understand that protecting data would still be at the mercy of individual users regardless of the numerous data protection tools deployed on devices. As argued by Johnston and Warkentin (2010), “technology and related procedures are not sufficient in achieving the required sense of security: people must be

motivated to utilize the available security technology and consistently perform the necessary procedures” (p. 2010). Thus, the more personalized data carrying assets become through the utilization of mobile devices for a wider array of activities, the more dependent data protection would be on user behavior. This study brings further understanding to what motivates mobile device users to protect data assets from threats such as data breach. In doing so, this study highlights the psychological process that leads to mobile device usage with regard to information security.

Furthermore, while several studies have argued for the use of persuasion and motivation in the promotion of safe security practices, it is still a challenge to identify what exactly will get users to really observe and practice them (Johnston, Warkentin, & Siponen, 2015). The use of protection motivation theory (PMT) in this study to develop a proposed research model that looks into mobile device security usage brings additional insight to past studies. This study also contributes knowledge to a key area in user information security behavior and one of ongoing debate: what motivates users to take protective initiatives over data assets to prevent data breach. This study’s aim was to highlight and inform whether the perceptions of threat when enhanced, spurs secure behaviors.

There has also been the discussion of user autonomy in some research studies. Warkentin and Willison (2009) pointed out that the vulnerability of systems is more significant when the user wields greater decision making. This study therefore adds to previous studies as it explored actual usage of security by mobile device users to protect data, whereby users mostly have autonomy over data assets which are their personal mobile devices. Mobile device users are struggling with how to properly and effectively manage the growing sophisticated security risks to their information assets. Ögütçü and Testik (2016)



argued that the behavior of humans in securing information assets goes beyond deploying technology and as such, the need for steps that take into consideration conscious elements such as user behavior. Alhogail et al. (2015) also posited that “while information security management activities comprise processes and procedures, it seems that there are a number of critical human factors that ensure a secure environment is developed and maintained” (p. 201).

Finally, this study’s proposed research model which was based on a critical review of theoretical literature and constructs in itself adds to literature that can be relied upon by other future research.

### **Barriers and Issues**

The determination of a mobile device user’s information security behavior will have to be based on a definition of what user information security behavior is, and an approach developed to measure it. The complex nature of human behavior itself can make this difficult since people exhibit different behaviors based on multiple factors and as such are unpredictable. For example, a mobile device user from a corporate environment may find the idea of data breach more catastrophic than a student mobile device user. Although data breach remains a concern for both users, the severity level each one of them places on data breach may be different therefore leading to different information security behaviors.

The ability to reach a sizeable number of participants for a survey can be a challenging task. This study leveraged a web-based survey, specifically Google Forms to reach the participants. There are several benefits of conducting a web-based survey over the traditional method. For the purpose of this study, it enabled the participation of mobile device users in different locations in the United States of America who in a traditional method

would have been difficult to reach, and it also made the data collection easy and less time consuming (Wright, 2005).

### **Assumptions**

Assumption according to Ellis and Levy (2009) is “what the researcher accepts as true without a concrete proof” (p. 331). The assumptions of this study were that: 1) the participants included in the survey would be sincere and forthright when responding to the survey questions; and 2) each participant in the survey has used mobile devices for a considerable period of time.

### **Limitations**

This study leveraged an online survey, also known as web-based survey. Rea and Parker (2014) pointed out that web-based surveys have a limitation of self-selection bias. Prospective respondents who feel they can appropriately complete a web-based survey and have knowledge of the subject matter may be the only ones who complete it. This impacts the generalization of the research in terms of the general population.

### **Delimitations**

Measuring variables is not an easy exercise and as such the survey for this study kept the questions in scope and not complicated to make participants reluctant from taking the survey (Rea & Parker, 2014). The use of convenience sampling as the sample design further helped to achieve this. The scope of this research was also restrictive to information security behavior as it relates to mobile device users. Houston and Tran (2001) pointed out that “the problem facing researchers is how to encourage participants to respond, and then to provide a truthful response in surveys” (p. 70). Thus, the survey instrument developed for this study was simple and could be completed under fifteen minutes (Rea & Parker, 2014).

## Summary

Following the background given on the area of the research, the introductory chapter centered on a research worthy problem within the field of information systems, and to be specific, the information security usage behavior of mobile device users in the context of data breach. The problem statement identified and elaborated on the specific problem to be investigated, why it is a problem, the way this problem has transformed overtime, and also pertinent occurrences preceding this problem. The problem statement was followed by the identification of the clear goal of this study. There was the presentation of a research question that gives an indication of the areas in the literature that was relied upon in this study. Based on the research question there were hypotheses and a proposed research model. The proposed research model was based on the PMT constructs of perceived threat severity, perceived threat susceptibility, perceived response costs, response efficacy, mobile self-efficacy, as determinants of protection motivation which leads to mobile device security usage. The relevance and significance of this study was presented to further elaborate on the need to investigate the identified problem, previous attempts made at resolving the problem, and the significant difference in contribution this study will make towards the resolution of the problem. Also, barriers and issues that were faced in this study's attempt at proposing a solution to the problem identified were presented. Finally, assumptions, limitations and delimitations of the research were highlighted to show the scope of this study.

## Chapter 2

### Review of the Literature

#### Overview

Information security has over the years been addressed from perspectives such as the technical design of security mechanisms, and often times as well, the socio-technical treatments of the topic. Research on user information security behavior is growing in demand because of the growth in security breaches involving both deliberate and accidental human behavior (Willison & Warkentin, 2013). User behavior in information security however, is a complex area of research because it is not easy pointing to one standard definition of what constitutes intended system user behavior. Alhogail et al. (2015) pointed out that intended user behavior cannot easily be predicted and is complex to manage.

The literature review in this study focused on synthesizing literature from other research works and sources that have attempted to examine the user behavior aspect of information security. The literature review in examining previous studies for their constructs, theories, contributions, limitations, and gaps, also analyzed the research methodologies used. The chapter aimed to understand data breach and also the factors at play in the information security behavior of mobile device users.

#### Theoretical Foundation

The PMT was first developed by Rogers (1975) as a framework to provide clarity to the understanding of fear-appeals. It was later revised by Rogers (1983) to provide a more general perspective of the impact of persuasion communication with emphasis on the cognitive processes that mediate behavior change. 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 the individual” (p. 409). PMT shows that individuals’ protection motivation is based on perceived threats to themselves and their surroundings, and individuals cope with threats based on two processes: appraising the threat, and a coping appraisal in which the options to reduce or mitigate the threats are assessed (Herath & Rao, 2009).

The rationale for leveraging the PMT is its potential to predict users desire to protect themselves, with emphasis on the cognitive processes that mediate change in behavior (Rogers, 1983). According to Almuhimedi et al. (2015), the information security behavior and decisions of mobile device users are based on cognitive and decision heuristics (p. 1). Tsohou, Karyda, and Kokolakis (2015) noted that cognitive factors affect the information security behavior of system users, and that it influences their compliance or noncompliance decisions. Boss et al. (2015) and Posey et al. (2015), posited that PMT is based on threat appraisal and coping appraisal, and how these two components influence the creation security related behaviors.

This study was a survey-based research and as such there were constructs identified based on the foundational theory. The PMT constructs leveraged for the purposes of this study were: perceived threat severity, perceived threat susceptibility, perceived response costs, response efficacy, mobile self-efficacy, protection motivation, and mobile device security usage. Furthermore, to point out the rationale for the scope of literature reviewed for this study, each of the constructs used have been separately defined and elaborated upon below:

**Perceived threat severity:** Johnston and Warkentin (2010) defined threat severity simply as the level of seriousness of the threat. Herath and Rao (2009), also defined threat

severity as the “degree of harm associated with the threat” (p. 111). Both definitions are 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). According to Coa, Chen and Wang (2014) users’ perceived threat severity is the expected outcome of the risks they encounter and their belief of the seriousness such changes could cause. According to Junglas, Johnson, and Spitzmüller (2008) the perceived threat severity by users which come with it the motivation for protection is cognitive, basically reliant on the personal psychological makeup of users. A major tenet of PMT is that the individual must perceive a certain level of threat to respond (Rogers, 1983).

**Perceived threat susceptibility:** threat susceptibility is defined by Witte and Allen (2000) as the “degree to which one feels at risk for experiencing the threat” (p. 592). According to Herath and Rao (2009), threat susceptibility is the “probability of the threat occurring” (p. 111). Johnston and Warkentin (2010) defined it as the probability of an individual personally encountering a threat. Cao, Chen and Wang (2014) posited that perceived threat susceptibility is the amount of vulnerabilities that the users feel exists and the likelihood of exposure their systems are to threats. The construct motivates users to protect themselves and this is an essential human characteristic and part of our psychological makeup, which even leads some research to claim that the urgency to protect ourselves is biologically motivated (Junglas, Johnson, & Spitzmüller, 2008).

**Perceived response costs:** according to Fry and Prentice-Dunn (2005), perceived response cost is the “social, physical and monetary expenses of performing the recommended response” (p. 288). It is further explained by Herath and Rao (2009) as the beliefs regarding the cost that comes with performing the recommended response. In terms of information

security, this would be the cost incurred by the user complying with security policies. Crossler and Bélanger (2014) citing Lee, Fan, Miller, Stolfo, and Zadok (2002) posited that security countermeasures are avoided when the cost involved is more than the severity of the threat. Herath and Rao (2009) pointed out that response cost negatively affects user attitude towards policies and especially in information security, users find security practices to be hindrances to their routine. Also, Post and Kagan (2007) in their study on access controls revealed that users did not embrace certain strong information security measures as they found them to be response cost which are detrimental to organizational creativity and restricts the flexibility of routine operations. Rogers (1975) in the seminal study that birthed PMT, posited that the costs of performing a certain behavior, such as time lost or heightened burden if high would hinder the performance of adaptive responses.

**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). Crossler and Belanger (2014) in a study on individual security behaviors described response efficacy as “an individual’s confidence that a recommended behavior will prevent or mitigate the threatening security event” (p. 8). The construct varies in terms of the level of adaptability, from maladaptive to adaptive. Adaptive response is defined by Johnston and Warkentin (2010) as the outcome of some degree of fear arousal (threat) that induces a “motivation for behavior consistent with alleviating the threat” (p. 551). 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. Vance et al. (2012) further noted that employee compliance with information security policies is a representation

of adaptive response. Adaptive response generates positive outcomes for users. Shillair et al. (2015) posited that adaptive response is perceived to protect users from threats.

Maladaptive response according to Rippetoe and Rogers (1987) is when users perceive threats due to the unavailability of a useful coping response and undertake activities that minimizes the fear the threat poses without necessarily tackling the risk fundamentally. The definition of maladaptive responses is considered by Vance et al. (2012) as the negative response appraised from the cognitively mediating process in individuals when they perceive a threat. Vance et al. (2012) posited that employee non-compliance with information security policies is a representation of maladaptive responses. In addition, Shillair et al. (2015) noted that maladaptive response drives users to take no action or when they do, leads to higher levels of threats. Warkentin, Johnston, Walden, and Straub (2016) in a recent research about fear appeals posited that “maladaptive responses serve to neutralize fear by rejecting the fear appeal” (p. 196).

**Mobile self-efficacy:** according to Bandura (1986), self-efficacy is founded in social cognitive theory and it is “people’s judgments of their capabilities to organize and execute courses of action required to attain designated types of performances” (p. 391). Similarly, Huffman, Whetten, and Huffman (2013) posited that self-efficacy is the perception people have of themselves to be able to execute certain actions satisfactorily. An earlier definition of self-efficacy by Bandura (1982) is more appreciated as it includes ‘behavior’, a variable that underlines the security usage of mobile device users. Bandura (1982) defined self-efficacy as “generative capability in which cognitive, social and behavioral sub-skills must be organized into integrated courses of action to serve innumerable purpose” (p. 142). The value of the definition by Bandura (1982) for this study is elaborated upon by Keith et al. (2015) as they



noted that self-efficacy has an effect on behavioral change. Bandura (2012) noted in a more current study that actual behavior was found to be influenced by self-efficacy.

**Protection motivation:** protection motivation is the result of the two processes of threat appraisal and coping appraisal, and it is defined by Rogers (1975) as an “intervening variable that has the typical characteristics of a motive: it arouses, sustains and directs activity” (p. 98). Rogers (1983) further explained protection motivation as the single mediating construct between adaptive response and threat appraisal, and coping appraisal. According to Witte et al. (1996), protection motivation is the main purpose of PMT but the process does not end there as it predicts behavior. Protection motivation is the result of the cognitive appraisal of threat appraisal and coping appraisal (Herath & Rao, 2009). Posey et al. (2015) asserted that the “PMT appraisal processes is a motivational force termed protection motivation” (p. 7).

**Mobile device security usage:** as the dependent variable that was used in this study, the actual use of mobile device security features and components was the measurement for this construct. It was ascertained utilizing questions, and survey items to assess whether mobile device users employ adequate security features not limited to anti-virus, anti-malware, backup, firewall, checks for and implementation of software and operating system updates, and strong authentication (Claar & Johnson, 2012).

### **Past Literature and Identification of Gaps**

Previous behavioral information security research mostly lack an explicit inclusion of actual security use as the dependent construct in their models. Its minimal use in previous information systems research focusing on user information security behavior has created a gap in the literature and a lack of understanding. In exploring the use of mobile device

security usage as a dependent construct in this study to explain mobile device user information security behavior, the options of including perceived threat severity, perceived threat susceptibility, perceived response costs, response efficacy, mobile self-efficacy, and protection motivation were considered.

Threat severity, fear, and response costs were utilized by Posey, Roberts, and Lowry (2015) in their study on the impact of organizational commitment on insiders' security behavior. Posey et al. (2015) found that threat severity, fear, and response costs became more significantly related with protection motivation when organizational commitment was at high levels, and not just in the general sense. Based on this finding, Posey et al. (2015) concluded that the PMT constructs is beneficial when used to give meaning to the cognitive, motivational, and past sequence of behavior of users with high organizational commitment rather than low commitment.

Crossler and Bélanger (2014) adapted threat severity, threat vulnerability, and response costs in their study to develop a unified security practices (USP) instrument. The development of the USP was based on the opinion that measuring multiple security behaviors rather than one, better reflects the measures users should take to protect their information assets. Crossler and Bélanger (2014) noted that perceived threat severity influenced the USP positively, whilst perceived threat vulnerability was negative, and response cost had no strong relation with the USP. It is worth pointing out that these findings were impacted by the reliance of Crossler and Bélanger (2014) on actual behaviors for the USP and non-technical individuals working in non-technically intensive fields as survey participants. Past findings by Woon, Tan, and Low (2005), Kumar, Park, and Subramaniam (2008) and Herath and Rao (2009b) have shown that when the information security knowledge and technical

level of users work industry is low, perceived vulnerability does not significantly influence their security behavior. These findings therefore suggest that a person's security knowledge plays a major role in their perceptions of security towards protection from data breach. Nevertheless, the study by Crossler and Bélanger (2014) to determine individual security behaviors leveraging PMT and a unified security practices (USP) instrument (USP) does not consider actual user security behavior towards the rapidly changing technological landscape, and information security risks. However, from a security perspective, changes in risks determines actual security performance eventually (Johnston & Warkentin, 2010).

The constructs that were leveraged by Claar and Johnson (2012) in their study on adoption behavior are severity and threat vulnerability. Contrary to the findings in the study by Crossler and Bélanger (2014), Claar and Johnson (2012) in an earlier study found that threat severity did not have a significant influence on user security behavior prior to the threat happening, rather it was found to be impactful after incident occurrence. Also, Claar and Johnson (2012) noted that threat vulnerability significantly influenced user security behavior. It is worth noting that moderating variables of gender, age, education, and prior experience with security incidents were used in the study to arrive at the findings. The study by Claar and Johnson (2012) noted that fear had a major influence on behavior, and this was missing in previous security adoption models.

The fear appeals model (FAM) developed by Johnston and Warkentin (2010) in their study on fear appeals and information security behavior, used the PMT constructs of threat severity, threat susceptibility, and behavioral intent. The new dimension the study presented to the literature on behavioral security is its use of social influence as a construct. According to Johnston and Warkentin (2010), its inclusion as a construct of FAM, expands previous

constructs and theories such as social factors (Thompson, Higgins, & Howell, 1991), image (Moore & Benbasat, 1991), and social norm which has been significant in past research attempts at understanding user behavior from the lenses of the theory of reasoned action (Fishbein & Ajzen, 1975), and the theory of planned behavior (Venkatesh & Davis, 2000). Johnston and Warkentin (2010) used the development of FAM to highlight the importance of behavioral intent but did not go further in testing actual use thereby leaving a gap for further research. Also, in an earlier study on how internet users can take more responsibility for their security behavior online, LaRose, Rifon, and Enbody (2008) leveraged the PMT constructs of threat severity and threat susceptibility to develop a framework for promoting safe online behavior.

Harris, Furnell, and Patten (2014) in a study which compared the security behavior of IT and non-IT college students, and predominately non-security-focused IT professionals 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 existence of such a situation is far from reality. Contrary to Harris et al. (2014), it was noted by Tu et al. (2015) in their study on mobile user behavior in coping with the risk of loss or theft that users do not naturally exhibit responsible security behaviors but tend to leverage technical countermeasures. In a study to evaluate what influences changes in user smartphone security behavior, van Bruggen (2013) posited that users make tradeoffs when weighing different security behaviors. However, complacency and disregard for responsible security behavior were noted as behaviors exhibited by most mobile device users (Mylonas, Kastania, & Gritzalis, 2013).

It is evident that there are gaps in the research on mobile device user security behavior. Wang, Duon, and Chen (2016) pointed out that further research is needed on user behavior and its applicability in securing the privacy of information on mobile devices. Crossler et al. (2013) posited that efforts to understand user information security behavior should consider behavior and shift the focus of research from technical issues. Additionally, Kokolakis (2017) noted that there is the need for more research into the elements that can be leveraged to influence the human factor in information security and privacy. 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 in user security behavior, and also studies related to mobile device that were reviewed for the purpose of this research used a varying array of research methods and designs. Quantitative research methods including surveys, and experimental designs have been leveraged, and qualitative research methods such as case studies, narratives and interviews have also been used in some instances. From the prior studies reviewed, it was not evident that mixed research methods are widely used in behavioral information security research. Survey research and experiment was evidently the most utilized research method for the prior studies reviewed for the purposes of this study. Posey, Roberts, and Lowry (2015) in their study on the impact of organizational commitment on insiders' security behavior used a survey completed by 380 survey participants. In their study to develop a unified security practices (USP) instrument, Crossler and Bélanger (2014) conducted an online and paper-based survey with 324 participants involved. Claar and Johnson (2012) in

their study on security adoption behavior used an internet-based survey to collect data from 311 participants.

Construct, content, and discriminant validity was established in almost each of the studies reviewed. Few studies also conducted a partial least square (PLS) analysis to test their structural models, the convergent and discriminant validity, and associated hypotheses. Descriptive statistics, hence a determination of the mean, mode and median, as well as inferential statistics was used in most of the studies. They also included tests such as Cronbach's alpha, good-fit, and regression analysis to further strengthen the validity and reliability of their results. Most of the studies used the cross-sectional method instead of longitudinal signifying that there was no need of collecting data at different points in time.

### **Mobile Device Data Breach**

Lowry, Posey, Bennet, and Roberts (2015) pointed out that data breach can be a result of deliberate user actions, negligence or accidental incidents. 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 of sensitive information by an external entity to the organization. An earlier, and widely used explanation of data breach by Culnan and Williams (2009) held that data breaches occur when personal information is accessed by unapproved or unauthorized persons as a result of security vulnerabilities exploited by hackers, lost mobile devices, unauthorized third parties and inappropriate information disposal processes by organizations.

Data breach occurrences from mobile devices according to Romer (2014), could be a non-issue if users control what applications they load on their devices. Similarly, Steiner (2014) also proposed that leveraging authentication tokens could be a data breach solution

for mobile devices. However, O'Neill (2014) argued that the security challenges of mobile devices are more complex and the simple reason that they get lost and are stolen more often than conventional computers makes the effort needed to protect them from data breach more challenging. Li and Clark (2013) in a study on mobile security noted that mobile devices have become more vulnerable to data breach as users rely more on mobile applications that exposes them to malicious activities as they load them on inadequately insecure devices.

### **Synthesis of the Literature**

The foundational theory that this study was based on is the PMT which was initially developed as a fear-appeals framework by Rogers (1975) and later extended by Rogers (1983) to include an understanding of cognitive factors that affect change in behavior. "The purpose of PMT research is usually to persuade people to follow the communicator's recommendations; so, intentions indicate the effectiveness of the attempted persuasion" (Floyd et al. 2000, p. 411). The PMT's main independent constructs constitute two components of the theory which are the threat appraisal and coping appraisal (Boss et al., 2015). The theory's dependent construct is best conceptualized by Floyd et al. (2000) as protection motivation. Floyd et al. (2000) posited that "the protection motivation concept involves any threat for which there is an effective recommended response that can be carried out by the individual" (p. 409). This study did not only use the existing constructs from the PMT theory but extended it by adding new constructs related to mobile device: mobile self-efficacy and mobile device security usage.

As the IS literature shows, there have been previous studies conducted on user security behavior, but there is not a published research found that focused on mobile device security usage of users by determining the effects of perceived threat severity, perceived

threat susceptibility, perceived response costs, response efficacy, mobile self-efficacy, and protection motivation. Continuous effort must be made to understand the information security behavior of mobile device users to be able to adopt approaches that will direct them in their efforts to protect data (Posey, Roberts, & Lowry, 2015). While the foundation for this study was based on previous work in the area of user security behavior, it intended to extend their findings by modifying them to investigate mobile device security usage behavior.

### **Summary**

The literature review in this study highlighted and synthesized literature from other previous research studies and sources that examined user security behavior. The literature review delved into the foundational theory of this study which is the protection motivation theory (PMT). It also attempted through the theory development to understand how the constructs used in this study: perceived threat severity, perceived threat susceptibility, perceived response costs, response efficacy, mobile self-efficacy, act as determinants of protection motivation, which leads to mobile device security usage. In so doing, prior studies that have leveraged the same constructs or adapted similar versions, were reviewed for their findings, contributions and gaps. Also, the research methodology used by these previous studies were reviewed in this chapter to highlight their validity and reliability for this study. The overall aim of the review of literature was to bring new insights to the existing body of knowledge as it attempts to understand the factors at play in the information security behavior of mobile device users.



## Chapter 3

### Methodology

#### **Overview of Research Methodology/Design**

Survey research was the research strategy used for this empirical study to assess how the independent variables - perceived threat severity, perceived threat susceptibility, perceived response costs, response efficacy, and mobile self-efficacy determines protection motivation which influences the dependent variable - mobile device security usage. This strategy was used because it allowed for the collection of quantitative data which was statistically analyzed to test the hypotheses involving the above-mentioned variables.

The research strategy was based on a positivism philosophy or orientation because the hypotheses could be tested based on facts through the appropriate use of theories and models by previous researchers. Saunders, Lewis, and Thornhill (2003) explained that a positivism approach will mean a very structured methodology so that the study can be reproduced by another researcher and it will also mean the application of quantitative observations that permits data to be analyzed statistically. Positivism philosophy when adopted gives findings that are based on firmer grounds than just mere opinions or intuition (Burns, 2000). This study in a broad perspective aimed at revealing mobile device users' security behavior in the context of data breach. Putting it another way, it sought to establish not only a relationship but predict the impact as well between the presented constructs.

#### **Research Method**

The primary data collection method used for this study was quantitative and to be precise, a survey. For the purpose of this study, a web-based survey was designed. This method of data collection was chosen because of its numerous benefits, making it appropriate

for this study. Also, a large number of peoples' views was needed, which made this method ideal due to its ability to collect highly standardized information with the absence of bias since the same questions are answered by all respondents.

Prior to conducting the survey for the main data collection, a Delphi study was conducted. According to Skulmoski, Hartman, and Krahn (2007), a Delphi study is an "iterative process to collect and distill the anonymous judgments of experts using a series of data collection and analysis techniques interspersed with feedback" (p. 1). The rationale of first conducting a Delphi study was to further validate the constructs used in the research by seeking expert feedback and validation of the meanings and operationalizations of the variables. According to Okoli and Pawlowski (2004), "the Delphi method can employ further construct validation by asking experts to validate the researcher's interpretation and categorization of the variables" (p. 19). Okoli and Pawlowski (2004) pointed out four benefits of using a Delphi method in IS research: 1) it helps researchers determine relevant variables and develop hypotheses, 2) it helps reinforce the establishment of theory and increase its generalizability, 3) it aids with comprehending the causal associations between elements which is important in theory development, and 4) it adds to construct validity. The Delphi study involved 11 subject matter experts (SMEs) familiar with mobile device security use. The experts were tasked with reviewing and validating the content of each item. The experts were also requested to recommend adjustments to the items. Gray and Hovav (2014) explained that SMEs are usually qualified professionals knowledgeable in a particular discipline and have adequate experience to speak with authority on matters of that discipline. Sumsion (1998) posited that in a Delphi study, an agreement between 70% or more of the

SMEs is considered a consensus. The issue of SMEs remaining anonymous as part of this process was addressed.

The survey was in a non-contrived setting with minimal extent of interference since the surveying of the selected mobile device users will happen in their natural environment. The target population studied was individual mobile device users. The use of the individual unit of analysis was ideal because of the overall goal of this study, which is to establish the mobile device security usage of mobile device users. Sekaran and Bougie (2013) defined the individual unit of analysis as “treating each employee’s response as an individual data source” (p. 104). The cross-sectional method was appropriate for this study because there was no need of collecting data at different points in time to be able to answer the research question.

### **Instrument Development and Validation**

The survey instrument for this study was a combination of adopting and adapting some existing items and developing some of its own items for this study. Saunders et al. (2003) suggested that adopting or adapting items is more efficient than developing items yourself only if it enables you to gather the appropriate data needed to meet the demands of the study. The items were structured in the simplest of language for easy understanding. This gave respondents the ease and encouraged them to answer the questions. In the designing of the survey, care was taken since it is not necessarily a scientific task where a rigid format has to be followed, instead the target respondents would have to be highly considered and factored into its design.

Interval scale was the level of measurement used to measure each of the following variables in the survey items. Although the survey employed the Likert scale, which leans

more towards an ordinal level of measurement, the actual level of measurement for this study was however treated as interval because the scale that was used gave a clear interval between them. The use of interval scale to measure each variable of survey items ensured that the responses are easily quantifiable and can be readily analyzed quantitatively using statistical tools. Also, this level of measurement ensured that the survey respondents were not coerced into taking a position. Rather, it provided a level of agreement, disagreement or even neutrality and indecisiveness.

The Likert-style rating scale, to be precise, a 7-point rating scale was used on all survey items. Instrument reliability was tested because it is important that this study was based on reliable data that is free from bias. Therefore, the Cronbach alpha test was conducted to test the reliability of the items. Gay et al. (2009) suggested that when a study's survey instrument uses Likert scale, the Cronbach's alpha is a more useful option for assessing the internal consistency reliability. The reliability processing result is considered an acceptable significant level of reliability if the various variables each return a Cronbach's alpha of 0.7 or more. According to Gefen, Straub, and Boudreau (2000), 0.70 at least should be achieved as it is the lower limit for Cronbach's alpha internal consistency reliability in confirmatory research. Rovai, Baker, and Ponton (2013) further explained that a factor loading below 0.5 is regarded as a low Cronbach's alpha coefficient, average for a coefficient between 0.5 and 0.7, and above 0.7 is considered high.

The survey included the six major constructs identified for the purposes of this study: 1) perceived threat severity, 2) perceived threat susceptibility, 3) perceived response costs, 4) response efficacy, 5) mobile self-efficacy, 6) protection motivation, and 7) mobile device security usage. The items for measuring perceived threat severity and perceived threat

susceptibility were adapted from Claar and Johnson (2012). The items for both constructs “assess the degree to which individuals feel that it is likely they will experience the scenario and assesses the impact to them were it to happen” (Boss, 2007, p. 75). The items for perceived threat severity were measured on a 7-point Likert scale ranging from “1” = Very-Low Impact to “7” = Very-High Impact. The items for perceived threat susceptibility were measured on a 7-point Likert scale ranging from “1” = Highly-Unlikely to “7” = Highly-Likely. The reliability test for the adapted items had a Cronbach’s alpha of 0.91 for perceived threat severity and 0.92. for perceived threat susceptibility (Claar & Johnson, 2012). To measure perceived response cost, a scale was adapted from Boss et. al (2015); Woon et al. (2005). The items for perceived response cost was measured on a 7-point Likert scale ranging from “1” = Strongly Disagree to “7” = Strongly Agree. The reliability measure for the adapted items showed a 0.84 Cronbach’s alpha (Boss et al., 2015; Woon et al., 2005). The response efficacy scale was adapted from Boss et al. (2015); 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). The items for response efficacy was measured on a 7-point Likert scale ranging from “1” = Strongly Disagree to “7” = Strongly Agree. To measure mobile self-efficacy, a scale was adapted from Claar and Johnson (2012). The items for mobile self-efficacy was measured on a 7-point Likert scale ranging from “1” = Strongly Disagree to “7” = Strongly Agree. The measure of reliability of the adapted items was a Cronbach’s alpha of 0.94 (Claar & Johnson, 2012). The items for protection motivation was adapted from Posey et al. (2015). The items for protection motivation was measured on a 7-point Likert scale ranging from “1” = Strongly Disagree to “7” = Strongly Agree. The reliability measure of the adapted items was a Cronbach’s alpha 0.64. Posey et al. (2015)

pointed out that an alpha below 0.70 for protection motivation meets the requirements from past studies and a lower alpha is usually the case when an instrument has fewer items.

Mobile device security usage was measured by adapting a scale from Claar and Johnson (2012) and also self-developed items. The items for mobile device security usage was measured on a 7-point Likert scale ranging from “1” = Never to “7” = Always. The reliability measure of the adapted items was a 0.90 Cronbach’s alpha (Claar & Johnson, 2012).

The survey conducted for the purpose of this study was highly relevant in resolving the hypotheses because it provided primary information on the various variables that make up the hypotheses. Straub (1989) noted that for a research model to adequately test its hypothesized relationships, the constructs must be properly operationalized. Also, it was important to establish the reliability and validity of the items used in the constructs. The items that were used for each construct can be found in Table 1.

Table 1

*Constructs Items and Instrument Source*

Constructs/Items	Description	Source
<b>Perceived Threat Severity</b>	Please indicate the impact that each of these scenarios would have on you if it would occur.	
PTSE1	My mobile device becoming corrupted by a virus.	Claar and Johnson (2012)
PTSE2	My mobile device being taken over by a hacker.	Claar and Johnson (2012)
PTSE3	My sensitive personal data (bank account, social security, etc..) being stolen from my mobile device.	Claar and Johnson (2012)
PTSE4	My data being lost due to a virus on my mobile device.	Claar and Johnson (2012)

Constructs/Items	Description	Source
PTSE5	My mobile device downloading a virus or bug infected application.	Claar and Johnson (2012)
<b>Perceived Threat Susceptibility</b>	Please indicate how likely you feel each scenario will occur with your mobile device.	
PTSU1	My mobile device becoming corrupted by a virus.	Claar and Johnson (2012)
PTSU2	My mobile device being taken over by a hacker.	Claar and Johnson (2012)
PTSU3	My sensitive personal data (bank account, social security, etc..) being stolen from my mobile device.	Claar and Johnson (2012)
PTSU4	My data being lost due to a virus on my mobile device.	Claar and Johnson (2012)
PTSU5	My mobile device downloading a virus or bug infected application.	Claar and Johnson (2012)
<b>Perceived Response Cost</b>	Please indicate the degree to which you agree or disagree with the following statements.	
PC1	Using an anti-virus software on my mobile device decreases the device's convenience.	Boss et al. (2015); Woon et al. (2005)
PC2	Using an anti-malware software on my mobile device decreases the device's convenience	Boss et al. (2015); Woon et al. (2005)
PC3	Using an anti-virus software on my mobile device involves too much work.	Boss et al. (2015); Woon et al. (2005)
PC4	Using an anti-malware software on my mobile device involves too much work.	Boss et al. (2015); Woon et al. (2005)
PC5	Using an anti-virus software on my mobile device requires considerable investment.	Boss et al. (2015); Woon et al. (2005)
PC6	Using an anti-malware software on my mobile device requires considerable investment.	Boss et al. (2015); Woon et al. (2005)
PC7	Using an anti-virus software on my mobile device is time consuming.	Boss et al. (2015); Woon et al. (2005)

Construct/Items	Description	Sources
PC8	Using an anti-malware software on my mobile device is time consuming.	Boss et al. (2015); Woon et al. (2005)
<b>Response Efficacy</b>	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)
RE 3	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)
<b>Mobile Self-Efficacy</b>	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)



Constructs/Items	Description	Source
<b>Protection motivation</b>	Please indicate the degree to which you agree or disagree with the following statements.	
PM1	I am motivated to protect my mobile device from threats of data breach.	Posey et al. (2015)
PM2	I am motivated to prevent threats of data breach to my mobile device from being successful.	Posey et al. (2015)
PM3	I am motivated to engage in activities that protect my mobile device from threats of data breach.	Posey et al. (2015)
<b>Mobile Device Security Usage</b>	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...).	Self-developed
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.	Self-developed
MDSU6	I use biometric protection on my mobile device.	Self-developed
MDSU7	I use software updates on my mobile device whenever they are available.	Self-developed
MDSU8	I use operating system updates on my mobile device whenever they are available.	Self-developed

To test the validity of the data used in this study, content validity was employed by relying on expert judges such as information security professionals to attest that the measures

and items used in the survey, are appropriately and adequately testing the concept. Gay, Mills, and Airasian (2009) defined content validity as "the degree to which a test measures an intended content area" (p. 155). Diamantopoulos and Winklhofer (2001) noted that content validity is important because it eliminates items from measured variables relying on understandable phenomena and does not lower the rigor of the instrument.

Construct validity was used to further testify the validity of the results of the survey by showing that there is a convergence between constructs that theoretically are similar and recognize a distinction from constructs that are not theoretically similar. Factor analysis was used to test the convergent validity of the items and constructs. Convergent validity is "the degree to which concepts that should be related theoretically are interrelated in reality." (Trochim & Donnelly, 2008, p.68). Peter (1981) defined construct validity as "the degree of correspondence between constructs and their measures" (p. 133). According to Trochim and Donnelly (2008), construct validity is the "degree to which inferences can legitimately be made from the operationalizations in your study to the theoretical constructs on which those operationalizations are made" (p. 56). This study also established discriminant validity. According to 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 survey was also pilot tested to ensure reliability. Arachilage and Love (2014) explained that a pilot study is the test that precedes the main study to determine its validity and correct identified errors. Based on the results from the pilot study, changes were made to the survey by correcting mistakes and wording the items more clearly. Also, the pilot study gave a general idea of how much time is needed for the completion of the survey. The pilot

study was conducted with 20 participants to ensure the survey instrument developed is reliable. Lewis-Beck and Liao (2014) suggested that conducting a pilot study supports other tests of validity by helping to notice survey items that are complex.

### **Ethical consideration**

The Institutional Review Board (IRB) at Nova Southeastern University was contacted to get approval to conduct this study. The IRB requirements and standards for the collection and handling of data were adhered to for the purpose of this study. It was made clear to participants in the survey that their participation is voluntary, all information will be held confidential, and only used for purposes of this study. Attention was paid to the ethical issue of the need to take care in the designing of the survey by avoiding the inclusion of items that seek private information such as name and job title because most participants would have been reluctant to participate since anonymity would not have been kept. Similarly, the Delphi study, that was conducted prior to the main survey for this research ensured the SMEs had full anonymity. The survey also provided maximum comfort and anonymity by making it impossible to identify who participated. “In the context of research, ethics refers to the appropriateness of your behavior in relation to the rights of those who become the subjects of your work or are affected by it” (Saunders et al., 2003, p. 129). The issue of respondents remaining anonymous was reiterated in the survey and also this study’s importance and significance made the respondents take the exercise seriously.

### **Population and Sample**

The sampling frame for the research was the individual users from the target population. The sample frame which is the representation of the elements in the population in question for this research was drawn through the web-based survey. The current data at the

time of the survey of the targeted population indicated the sample frame which was a representation of the overall number of individual mobile device users. Nonprobability sampling design was adopted since the choice subjects from the population to be studied was not based on any probabilities.

Convenience sampling was the category of nonprobability sampling design used because this study was looking to collect data from a specific target group, and in this case, mobile device users. Specifically, judgment sampling was the type of purposive sampling used as it was the ideal sampling design for reaching the subjects who voluntarily wanted to participate in the survey. Thus, the use of judgment sampling was to collect information from the individual mobile device users, who were inclined to participate in the survey study.

There were 1,310 online surveys sent to participants through email, social media platforms and messaging applications. The total of 390 responses received was in the range of the 30% to 40% anticipated response rate. There was no incentive given for participation in this study. Johnston and Warkentin (2010) in their seminal study that proposed the fear appeals model, achieved a response rate of 40% using an online survey without offering incentives.

Rogelberg and Stanton (2007) argued that “if a study does obtain a response rate well below some industry or area standard, this does not automatically signify that the data obtained from the research were biased” (p. 198). It is only through coercion that a 100% response rate can be achieved (Rogelberg & Stanton, 2007). Baruch and Holtom (2008) corroborated the argument by Rogelberg and Stanton (2007) noting that the average response rate for published academic research is significantly below 100%.

### **Pre-analysis Data Screening**

Pre-analysis data screening to check for validity is important prior to data analysis. Levy (2006), noted that “a pre-analysis data screening deals with the process of detecting irregularities or problems with the collected data” (p. 150). As pointed out by Mertler and Vannatta (2010), the rationale for pre-analysis data screening is to avoid incorrect results from data analyzed. Through the use of web-based survey as the medium of data collection, the possibility of mistakes during response transcription was avoided. Detecting and eliminating responses that are of the same value for each survey item is another reason noted by Levy (2003) for pre-analysis data screening. To address the response set-issue, this study adopted the suggestion by Ferdousi and Levy (2010) by conducting a visual inspection to eliminate items that show 100% of the responses having the same value.

The concern of losing or collecting partial data is another reason for pre-analysis data screening which will help to increase validity (Sekaran, 2003). Hair, Black, Babin, and Anderson (2010) also suggested that the effects of using incomplete data as a result of not performing pre-analysis data screening can be significant. Pre-analysis data screening is helpful for identifying multivariate outliers which can change results due to their exceptional nature (Mertler & Vannatta, 2010). Mertler and Vannatta (2001) explained that multivariate outliers are “cases with unusual combination of scores on two or more variables” (p. 27). As suggested by Levy (2008), Mahalanobis Distance was used in this study to identify and eliminate multivariate outliers. Levy (2006) explained that the Mahalanobis Distance “evaluates the distance of each case from the centroid of the remaining cases, where the centroid is created by the means of all the variables in that analysis” (p. 152).

## **Data Analysis Strategy**

Sekaran (2003), noted that “in the data analysis we have three objectives: getting a feel for the data, testing the goodness of data, and testing the hypotheses developed for the research” (p. 306). This study used descriptive statistics to get a measurement of the median, mean, mode and standard deviation of the data that was collected. The Partial Least Square Structural Equation Modeling (PLS-SEM) for data analysis was ideal for this study as it attempts to predict the impact the research model’s independent variables have on the dependent variable. The rationale behind choosing the PLS-SEM for the purposes of this study was pointed out by Byrne (2001) that, it is a valuable statistical method when conducting research with causal relationships. Hair, Ringle, and Sarstedt (2011) suggested that the PLS-SEM when compared to the Covariance based Structural Equation Modeling (CB-SEM) is better placed for work that has prediction-oriented goals, has more flexibility with sample sizes, and addresses the issue of whether constructs are formative or reflective. CB-SEM on the other hand would serve a study best “if the goal is theory testing, theory confirmation, or comparison of alternative theories” (Hair et al., 2011, p. 144). Data visualization methods not limited to graphs, scatter plots, and scree plots were leveraged to succinctly present the analysis performed to show irregular structures, and variance respectively (Mertler & Vannatta, 2013).

## **Format for Presenting Results**

The format the research results is presented in makes it easy to interpret by readers. The data collected from the survey was analyzed and presented in this dissertation report. The figures and outputs from the PLS-SEM and SPSS tools used for data analysis were presented in the results chapter of this report, and the screenshots also added in the

appendices. All validity test results such as the Cronbach's alpha were presented in table form for easy interpretation. The survey template that was used for data gathering was presented in the appendices, including the approved IRB. The relevant Nova Southeastern University Dissertation Guide for the College of Engineering and Computing Doctoral for students was followed for guidance on the presentation of the research report.

### **Resource Requirements**

Resources used for the purpose of this study include a laptop, journals, books, peer-reviewed articles and other sources of credible literature that were leveraged to support this study. The primary resource that was relied upon to access all the relevant literature and information for this study was the Alvin Sherman Library of Nova Southeastern University. Also, Google Forms was leveraged for the administering of the survey questionnaire and collection of data. The experts for the Delphi study, and participants for the pilot test were also vital resources for this study. Since this study used a survey, meaning the involvement of human subjects, a signed and approved IRB form was first secured before the data gathering exercise commenced. SPSS and Smart PLS 3.0 were used for the analysis of the data collected, interpretation and presentation of the results in an acceptable and professionally academic format.

### **Summary**

The chapter covered the research design used for this study. The research strategy considered suitable for this study was quantitative research. It was based on a survey because this study sought to establish associations and relationships between certain constructs that were used. Ensuring validity and reliability in the research was important. Therefore, content, convergent, discriminant, and construct validity were established in this study.

Nonprobability sampling design was used because this study collected data from a specific target group, and in the case of this study, mobile device users. The data analysis strategy involved the use of SPSS and PLS-SEM. The research results were presented in the relevant sections and in the appendices whilst taking guidance for the presentation of the overall report from the relevant Nova Southeastern University Dissertation Guide for the College of Engineering and Computing for doctoral students. The resources required for the research to be adequately completed were available and easily accessible.



## Chapter 4

### Results

#### **Pre-Analysis Data Screening**

This study was conducted using a quantitative approach that collected data through a web-based survey designed with a 7-Point Likert scale (see Appendix A). Prior to the main data collection, a Delphi study was conducted, followed by a pilot study. The Delphi study tasked 11 experts with the validation of the constructs used in the research. The team of 11 experts was composed of a Chief Information Security Officer (1), Information Security Analysts (3), Mobile Device Management Engineers (3), Threat and Vulnerability Manager (1), Senior Mobile Applications Developer (1), Information Technology Risk Manager (1), and an Incident Response Engineer (1). Through their expert feedback and validation of the meanings and operationalizations of the variables, the needed changes were made to the survey items.

To ensure the survey instruments reliability, a pilot study was conducted with 20 participants. The participants were composed of neighbors, work colleagues and friends. Some of the survey responses in the pilot study were missing data, and it was determined the issue was due to the researcher not marking all the survey items as 'required'. This issue was addressed by marking all the survey items as 'required' in the survey instrument. Based on the results from the pilot study, changes and adjustments were also made to the survey by correcting mistakes and wording the items more clearly. Furthermore, the pilot study gave a general idea of how much time participants needed for the completion of the survey, and also helped to identify any survey items that are complex. To ensure the issue of missing values has been fully corrected, the SPSS frequency method was also used to check.

The survey link for the main study was sent to friends, neighbors, colleagues at the researcher's current place of employment, previous employers, and patronizers of the researcher's local library after IRB approval had been obtained (see Appendix B). The cross-sectional method was leveraged in the collection of data during the months of November and December 2018. The cross-sectional method was appropriate because there was no need for the collection of data at different points in time as is prescribed by the longitudinal approach. The individual unit of analysis was used for this study. Convenience sampling was used to collect the data through the survey link sent to approximately 1,200 – 1,300 individuals. The survey link was sent to them through email, social media platforms (Facebook, LinkedIn), WhatsApp messaging and regular text messaging. There were 390 responses received thus meeting the 30% – 40% response rate that was anticipated.

The IBM SPSS tool was used to perform descriptive statistics to analyze outliers, normality, and also get a measurement of the median, mean, mode and standard deviation of the data that was collected. The Smart PLS 3.0 tool was used to perform Partial Least Square Structural Equation Modeling (PLS-SEM) for the data analysis of this study. The rationale behind performing the PLS-SEM was pointed out by Byrne (2001) that, it is a valuable statistical method when conducting research with causal relationships. Additionally, Hair, Ringle, and Sarstedt (2011) suggested that the PLS-SEM when compared to the Covariance based Structural Equation Modeling (CB-SEM) is better placed for work that has prediction-oriented goals, has more flexibility with sample sizes, and addresses the issue of whether constructs are formative or reflective.

### *Mahalanobis Distance and Box Plot*

The Mahalanobis distance was used to identify and eliminate multivariate outliers. Using SPSS analysis, there were 8 outliers identified out of which the values for the cases of 25, 388, 197, 6, and 355 were noted to be above 79.63 (Appendix C Mahalanobis Distance). The critical value of chi-square at  $p < .001$  was used for the calculation of Mahalanobis distance with degrees of freedom (df) = 38 yielding a result of 59.703 from the chi-square distribution table. 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). Two of the values were dropped for being the highest extreme values and the Mahalanobis distance was rerun (see Appendix D Rerun of Mahalanobis Distance). Mertler and Reinhart (2017) pointed out that outliers should not be automatically dropped from the analysis since they may be interesting cases and perfectly legitimate, rather than considered bad. Running the Mahalanobis distance again with 388 cases, there were now 6 outliers identified with cases 196, 6, 354, 68, and 13 showing to have extreme values.

### *Normality and Scatter Plot*

The variables in the study were aggregated into independent and dependent variables for a test of normality to be conducted. The Skewness and Kurtosis before deleting 2 of the most extreme outliers as evident in the box plot were .814 and .395 respectively (see Appendix C). The values for the Skewness and Kurtosis dropped to .718 and .069 respectively when the 2 extreme outliers were deleted. Analyzing the results from the normality test done after deleting the 2 extreme cases, the data showed normal distribution. According to Hair et al. (2017), the guideline for accepting a distribution as normal is if its

skewness and kurtosis is in the range of -1 to +1. Mertler and Reinhart (2017) suggested that that statistical options, data visualization and graphical methods not limited to skewness, kurtosis, Kolmogorv-Smirnov statistic with Lilliefors significance level, ANOVA, histogram, normal P-P plot of regression, and scatter plots should be leveraged to check data for normality, linearity and variance. The statistical outputs and normality graphs for this showed that the data distribution was normal. The cases were almost on the diagonal line for both the normality Q-Q and normality P-P regression plots, and the scatter plot also formed a rectangular shape which shows that the distribution is normal (see Appendix D Rerun of Mahalanobis Distance and Appendix E Normality and Scatter Plot).

### **Data Analysis**

Data analysis was performed using the Smart PLS 3.0 tool. The tests performed included factor loading, model fit, construct reliability and validity, discriminant validity, outer loading, path coefficients, and bootstrapping. The PLS algorithm was run and the factor loadings met the acceptable value of 0.70 with the exceptions of RE4 (0.490), RE5 (0.396), MDSU5 (0.503), MDSU6 (0.244), and MDSU7 (0.320) (see Appendix F).

#### *Construct Reliability and Validity*

Based on further analysis of the construct reliability and validity output, the average variance extracted (AVE) for RE and MDSU were 0.438 and 0.358 respectively which are not considered reliable as they do not meet the accepted value of 0.5 or higher see (see Appendix G). However, the constructs used in this study had Cronbach's alpha and a composite reliability ranging between 0.7 and 1.0, therefore indicating reliability. The reliability processing result is considered an acceptable significant level of reliability if the various variables each return a Cronbach's alpha of 0.7 or more (Gray et al., 2009). Gefen et

al (2000) also pointed out that a value of 0.70 at least should be achieved as it is the lower limit for Cronbach's alpha internal consistency reliability in confirmatory research.

The AVE for RE and MDSU improved to 0.568 and 0.513 respectively, thus meeting the accepted value of 0.5., when the latent variables RE4 (0.490), RE5 (0.396), MDSU5 (0.503), MDSU6 (0.244), and MDSU7 (0.320) were deleted and the PLS algorithm was run again. Hair et al. (2017) pointed out that an average variance extracted (AVE) of 0.5 or higher is acceptable. The findings from the Cronbach's alpha, composite reliability, and AVE show that the measurement items used in this study exhibit convergent validity (see Table 2, Appendix H and Appendix I).

Table 2

*Construct Reliability and Validity*

	<b>Cronbach's Alpha</b>	<b>rho_A</b>	<b>Composite Reliability</b>	<b>Average Variance Extracted (AVE)</b>
<b>Mobile Device Security Usage</b>	0.746	0.803	0.833	0.513
<b>Mobile Self-Efficacy</b>	0.912	0.92	0.938	0.791
<b>Perceived Response Cost</b>	0.933	0.974	0.942	0.673
<b>Perceived Threat Severity</b>	0.931	1.007	0.946	0.778
<b>Perceived Threat Susceptibility</b>	0.740	0.827	0.834	0.526
<b>Protection Motivation</b>	0.881	0.882	0.926	0.808
<b>Response Efficacy</b>	0.746	0.868	0.833	0.568

The model fit was analyzed after running the PLS algorithm. As pointed out by Hu and Bentler (1998), when it is applied in CB-SEM, an SRMR value less than 0.08 indicates a good fit. Although the relevance of the model fit in a PLS-SEM context is discussed in the literature, Hair et al. (2012) pointed out that the distinct statistical concepts of both the CB-SEM and PLS-SEM makes them more complementary as the weakness of one is the strength

of the other. The SRMR for this study's model fit was 0.066 which is less than the 0.080 value, therefore indicating a good fit (Hair et al., 2017) (see Table 3 and Appendix I). Hair et al. (2017) defined the model fit's SRMR as a "standardized root mean square residual" (p. 13).

Table 3

*Model Fit and Accepted Values*

	<b>Saturated Model</b>	<b>Estimated Model</b>
<b>SRMR</b>	0.066	0.090
<b>d_ ULS</b>	2.629	4.794
<b>d_ G</b>	0.973	1.069
<b>Chi-Square</b>	2,103.02	2,250.54
<b>NFI</b>	0.781	0.766

*Discriminant Validity*

Henseler, Ringle, and Sarstedt (2015) stated that "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). To determine discriminant validity, Chin (1998) proposed that each variable's loading to itself must be greater in value compared to its cross-loadings with other variables. Fornell and Larcker (1981) explained that discriminant validity is established when the latent variable has a higher variance in its associated variables compared to its values when cross-loaded with other constructs in the same model. The results of the discriminant validity test in this study showed that the diagonal loadings are greater than all their cross-loadings. Discriminant validity is therefore evident in the measurement items of this study (see Table 4 and Appendix I).

Table 4

*Discriminant Validity*

	Mobile Device Security Usage	Mobile Self-Efficacy	Perceived Response Cost	Perceived Threat Severity	Perceived Threat Susceptibility	Protection Motivation	Response Efficacy
<b>Mobile Device Security Usage</b>	0.717						
<b>Mobile Self- Efficacy</b>	0.622	0.890					
<b>Perceived Response Cost</b>	0.267	0.187	0.820				
<b>Perceived Threat Severity</b>	0.167	0.098	0.259	0.882			
<b>Perceived Threat Susceptibility</b>	0.132	0.080	0.193	0.685	0.725		
<b>Protection Motivation</b>	0.515	0.519	0.139	0.058	0.149	0.899	
<b>Response Efficacy</b>	0.495	0.409	0.15	0.202	0.205	0.332	0.754

**Findings**

The Smart PLS 3.0 tool was used to test the hypotheses suggested in this study.

Bootstrapping with a 500 re-sampling was performed to test the significance of the research model's paths. The bootstrapping performed produced a *t*-statistics (*t*-values) that shows the significance in the structural path (see Appendix J). The independent constructs exhibited variance towards the dependent construct with protection motivation showing 30 percent explained by perceived threat severity, perceived threat susceptibility, perceived response cost, response efficacy, and mobile self-efficacy. Mobile device security usage showed 26

percent explained by protection motivation (see Figure 2, Appendix H and Appendix I for the R-Square output).

Based on the analysis and as shown in Table 5, it is evident that protection motivation was not positively influenced by perceived threat severity ( $t=2.158$ ,  $p=0.031$ ), and positively influenced by perceived threat susceptibility ( $t=2.554$ ,  $p=0.011$ ). Protection motivation surprisingly was not influenced by perceived response cost ( $t=0.803$ ,  $p=0.422$ ). However, the remaining two coping appraisal constructs, response efficacy ( $t=2.538$ ,  $p=0.011$ ), and mobile self-efficacy ( $t=8.472$ ,  $p=0.000$ ) showed to positively influence protection motivation. Mobile device security usage shows it is positively influenced by protection motivation ( $t=11.077$ ,  $p=0.000$ ). The PLS analysis with all the data points are shown in Figure 2 below.

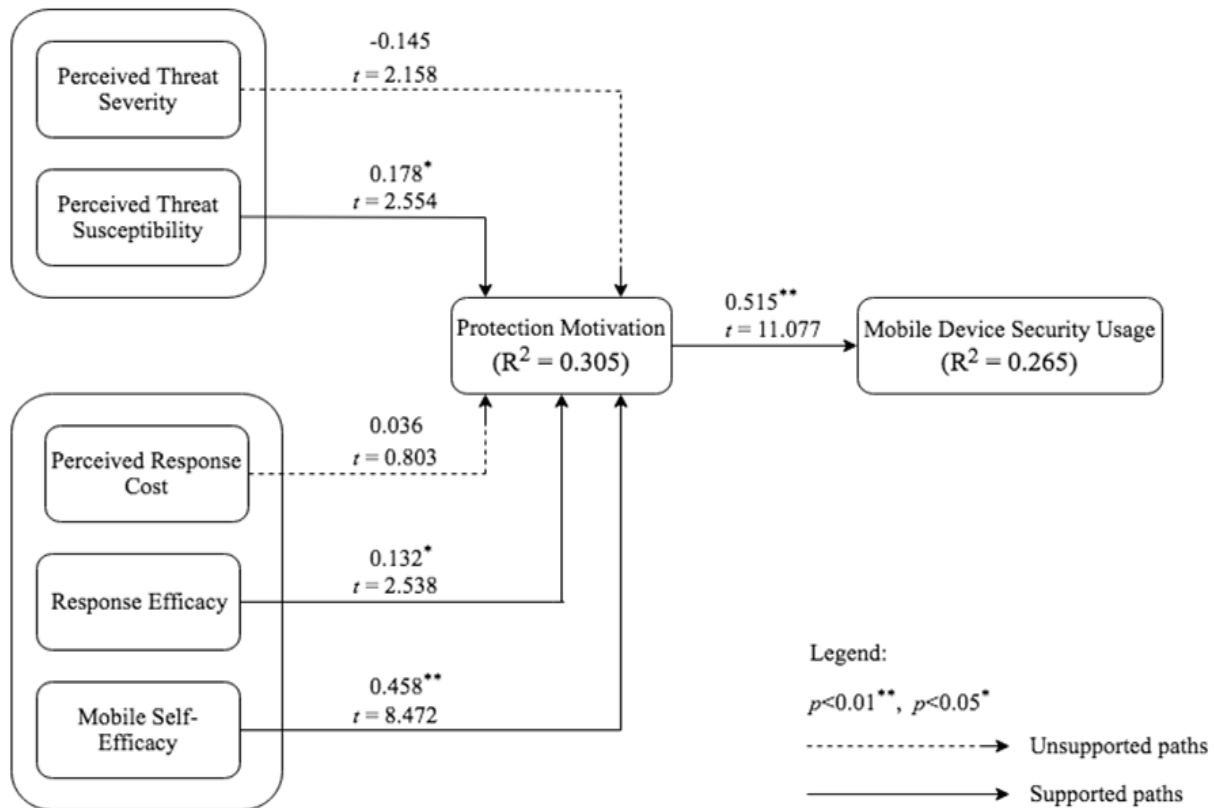


Figure 2. PLS Analysis Result for Mobile Device Security Usage



Hair et al (2011) pointed out that “the individual path coefficients of the PLS structural model can be interpreted as standardized beta coefficients of ordinary least squares regressions” (p. 147). Perceived threat severity ( $\beta=-0.145$ ,  $p<0.05$ ) surprisingly showed a negative effect on protection motivation, in contrast to the hypothesis (**H1**), and perceived threat susceptibility ( $\beta=0.178$ ,  $p<0.05$ ) showed a significant and direct positive effect on protection motivation. Thus, **H1** of the hypotheses was not supported while **H2** was supported. Also, in contrast to the hypothesis (**H3**), perceived response cost ( $\beta=0.036$ ,  $p<0.05$ ) did not show to have a significant effect on protection motivation. Nevertheless, the two other coping appraisal constructs in this study, which are response efficacy ( $\beta=0.132$ ,  $p<0.05$ ) and mobile self-efficacy ( $\beta=0.458$ ,  $p<0.01$ ) had significant and positive effects on protection motivation. Thus, **H3** was not supported, while **H4** and **H5** were supported. Protection motivation ( $\beta=0.515$ ,  $p<0.01$ ) had a significant and direct positive effect on mobile device security usage. Thus, **H6** of the hypotheses was supported (see Table 5).

Table 5

*Summary of Hypotheses Tests*

	Path Coefficient	t Value	p Value	Support
<b>Perceived Threat Severity -&gt; Protection Motivation</b>	-0.145	2.158	0.031	No
<b>Perceived Threat Susceptibility -&gt; Protection Motivation</b>	0.178	2.554	0.011	Yes
<b>Perceived Response Cost -&gt; Protection Motivation</b>	0.036	0.803	0.422	No
<b>Response Efficacy -&gt; Protection Motivation</b>	0.132	2.538	0.011	Yes
<b>Mobile Self-Efficacy -&gt; Protection Motivation</b>	0.458	8.472	0.000	Yes
<b>Protection Motivation-&gt; Mobile Device Security Usage</b>	0.515	11.077	0.000	Yes

## Chapter 5

### Conclusions

Mobile device security usage by mobile device users is critically important to protect their data from breach. From the results of the survey data analyzed and depicted in Figure 2, perceived threat severity did not have a positive effect on protection motivation as anticipated. The study by Claar and Johnson (2011) on home personal computer security adoption behavior found a negative relationship between perceived threat severity and computer security usage (dependent variable). Similarly, the study by Posey et al. (2015) on the factors that motivate employees to protect their organizations from information security threats, also showed that perceived threat severity had a negative effect on protection motivation. Thus, the finding from this study and the previous studies highlighted which also leveraged PMT, emphasize the position that the coping appraisal process is a more significant factor in increasing users' protection motivation than the threat appraisal process (Milne, Sheeran, and Orbell, 2000; Posey et al., 2015; Rippetoe & Rogers, 1987). It can be inferred from this finding that the confidence of mobile device users in the effectiveness of the available response efficacy and their mobile self-efficacy to protect their mobile devices leads them to minimize or dismiss the severity of perceived threats. It is evident that mobile device users perceive threat susceptibility as a necessary factor that leads them to want to perform security measures that will protect their devices from data breach. This finding is not surprising as it is backed by the literature. Dang-Pham and Pittayachawan (2015), argued that users are motivated to protect themselves if they perceive susceptibility to threats. Similarly, Posey et al. (2015) considered threat susceptibility to be a "major component in the threat appraisal process and overall formation of insiders' protection motivation" (p. 14). Herath

and Rao (2009) noted that the protection motivation by an individual is based on the perceived vulnerability to the threat. According to Workman et al. (2008), the perception of being vulnerable to threat leads to an assessment of coping appraisals that motivates users to protect themselves.

Furthermore, from the results, it is obvious that mobile device users consider as important, the response efficacy of the security measures available to mitigate data breach threats. This study's finding is not contrary to the literature. Posey et al. (2015) asserted that response efficacy more than the threat appraisal constructs, plays a more significant role in forming protection motivation. Johnston and Warkentin (2010) also 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, from earlier literature that corroborates this study's finding, Davis, Bagozzi, and Warshaw (1989) posited that an influential predictor of protection motivation is response efficacy.

Contrary to findings from previous studies, the results from this study did not show that the perceived response cost of security measures influences the protection motivation of mobile device users to secure their devices from data breach. The insignificant relationship shown by perceived response cost in this study can be attributed to the significant level of influence response efficacy and mobile self-efficacy have on protection motivation. According to Boss et al. (2015) and Posey et al. (2015), in the coping appraisal process of PMT, response efficacy and self-efficacy must be more than response cost for an individual to engage in protection motivation. From this study's findings, it is obvious that the response efficacy and mobile self-efficacy of mobile device users outweighed their perceived response cost to engage in protective behavior. Thus, it can be inferred from this study's findings that

when mobile device users are highly confident in their response efficacy and mobile self-efficacy against security threats, their perceived response cost does not have any significant influence on their protective security behavior.

The mobile self-efficacy of mobile device users as shown by the results, significantly influences their motivation to protect their devices from data breach. The finding is very much in conformity to the literature. Posey et al. (2015) posited that self-efficacy is a high significant predictor of protection motivation in numerous and different contexts. Keith et al. (2015) also noted that adopting a mobile self-efficacy construct presents a more rigorous approach to understanding the protection behavior of mobile device use. Self-efficacy has a significant positive impact on users' intent to protect themselves (Johnston & Warkentin, 2010). Findings from earlier research such as Chan et al. (2006), noted that mobile self-efficacy will lead mobile device users to develop an intention to protect their devices.

It is also very apparent from the results of this study that the mobile device security usage of mobile device users is significantly influenced by their motivation to protect their devices from data breach. The existing literature fully supports this finding. Posey et. al (2015) posited that the impact of protection motivation on behavior is not only significant but positively so. Johnston and Warkentin (2010) citing Rogers (1983) asserted that when threat appraisals and coping appraisals are at moderate-to-high levels, an individual's protection motivation is equally increased, thereby significantly influencing actual behavior. The stronger the intent to comply with security measures, the likelihood of actual compliance (Pahnila et al., 2007). Rogers (1983) posited that protection motivation is the variable that drives change in behavior.

## Discussion

The interpretation of the level of significance in this study follows the position by Hair et al. (1995) that a  $t$ -value above or equal to 1.96 is considered significant and acceptable for research values with a two-tailed test at a 5% significance level. Based on the PLS analysis conducted in this study and results presented in Figure 2, it was evident that protection motivation is negatively influenced by perceived threat severity, but positively influenced by perceived threat susceptibility, response efficacy, and mobile self-efficacy at 30 percent. Furthermore, the relationship between these constructs and protection motivation were significant showing perceived threat severity ( $t = 2.158$ ), perceived threat susceptibility ( $t = 2.554$ ) and response efficacy ( $t = 2.538$ ). Mobile self-efficacy particularly showed a strong relationship with protection motivation at a value of  $t = 8.472$ . This implies that the level of motivation for mobile device users to undertake positive protective measures that will secure their mobile devices is heavily driven by their assessment of the probability of being vulnerable to these threats, and the level of confidence in the mitigating controls, and in their own abilities to adequately use the mitigating controls. It is recommended that organizations, especially those that leverage mobile devices make the effort to better understand how employees handle security threats and their usage of mobile device security. Since the results of this study shows that mobile device security usage is based on personal behavior, it is also recommended that organizations focus more on the psychological aspects of user behavior through information security awareness programs, rather than solely relying on the conventional compliance approach which is based only on organizational security policies.

Mobile device security usage is explained by protection motivation at 26 percent. Protection motivation has a significantly high  $t$ -value of 11.077 which is well above the acceptable value of 1.96 recommended by Hair et al. (1995). This implies that the usage of mobile device security by mobile device users is based on their level of motivation to protect their devices from the security threats of data breach.

This study presents theoretical implications. It contributes to the literature in the IS security domain, primarily filling the existing gap in the literature by focusing on specific emerging technology trends and their associated security threats. Past studies in the IS security domain focused more broadly on computing systems and security. Also, previous research attempts around mobile devices in the IS security domain have mainly focused on areas such as information disclosure and location-based services on mobile devices (Keith et al., 2013), smartphone information security awareness (Allam et al., 2014), user attitude and mobile device usage participatory programs (Lee et al., 2016), and users perceived concerns and benefits of mobile device usage (Lebek et al., 2013). Other research attempts investigated the usage of mobile devices in unconventional ways in areas such as: learning (Martin & Ertzberger, 2013), healthcare (Boruff, & Storie, 2014), and finance (Fenu & Pau, 2015). The findings from this study contributes to the existing literature by demonstrating the effects of perceived threat severity, perceived threat susceptibility, perceived response costs, response efficacy, mobile self-efficacy, and protection motivation on the actual information security usage behavior of mobile device users in the context of data breach, a research area that had remained unexplored.

Furthermore, this study's focus on actual security usage behavior adds to the existing literature by demonstrating that mobile device users' protection of data from breach goes

beyond users' intention to users' actual behavior. Intention serves as an antecedent of behavior and there is an expectation that users carry out their intentions (Ajzen, 1985). Several past studies in the IS security domain relied on behavioral intention as the dependent variable (Anderson & Agarwal, 2010; Dinev & Hu, 2007; Johnston & Warkentin, 2010; Yoon & Kim, 2013). This study adds to those past research works and consequently the existing literature through the introduction of 'mobile device security usage' as a dependent construct that focuses on actual security behavior. Past security studies' reliance on intentions rather than actual behavior is limiting to theory development and theory validation (Crossler et al., 2013). Boss et al. (2015) also pointed out that "actual behaviors are important for ISec research because the end goal is to change security behaviors, not just security intentions" (p. 46).

Another theoretical implication of this study's findings is that it reinforces the PMT's capacity to predict user behavior based on threat and coping appraisals. Boss et al. (2015) and Posey et al. (2015), posited that the PMT is based on threat appraisal and coping appraisal, and how these two components influence protection motivation. For the purposes of this study, the PMT was extended as exhibited in Figure 1 to suggest that users can take recommended responses to threats, specifically within the context of mobile device security usage towards data breach. The use of the 'mobile device security usage' construct and the subsequent findings from this study adds to the literature by highlighting how the actual security behavior of users leveraging mobile device security features such as backup, firewall, authentication, anti-virus, anti-malware, and patching (software and system updates) helps to protect data from breach. Thus, re-emphasizing the importance of actual behavior in the IS security literature and research (Boss et al., 2015; Crossler et al., 2013).

An additional theoretical implication of this study is that it broadens the use of PMT to a relatively unexplored but relevant area in the IS security domain. Thus, an empirical assessment of mobile device users' information security behavior in the context of data breach. Given the prevalent vulnerabilities of mobile devices to data breach compared to conventional systems (Ben-Asher et al., 2011; Leavitt, 2011; Li & Clark, 2013; Oberheide & Jahanian, 2010; Tu & Yuan, 2012) and the need for users to take special measures to reduce or prevent them (Das & Khan, 2016; He et al., 2015; O'Neill, 2014; Tu and Yuan, 2012; Tu et al., 2015), this study's use of the PMT reinforces its capacity to be leveraged in different user information security behavior contexts. Herath and Rao (2009) noted that PMT can be explored and applied in a variety of information security contexts.

There are practical implications presented by this study. This study found that protection motivation influences the usage of mobile device security. There is also evidence of a high impact of mobile self-efficacy on protection motivation from this study. The practical implication is that information security training programs must be designed by practitioners to target the mobile self-efficacy of device users. Thus, a continuous improvement of users' information security skills to reflect changes in mobile device technology and enhance their abilities to leverage it on an ongoing basis. This re-emphasizes the call by Harris et al. (2014) for more frequent mobile device training due to the rapidly changing nature of mobile device technology. The security trainings practitioners provide mobile device users should include awareness on the susceptibility of users' mobile devices to data breach risks, including but not limited to virus, malware, Trojans, phishing, malicious website sites and applications (Edwards, 2015).



Another practical implication from this study is that practitioners must design mobile device management systems with processes and procedures that enables users to take practical steps at protecting their devices. Tu et al. (2015) advocated that users should be given access to countermeasures designed against the loss or theft of mobile devices. Additionally, practitioners must design programs to boost the confidence of mobile device users in their abilities to effectively work through such device management systems, processes and procedures. This practical implication complements the suggestions by Slusky and Partow-Navid (2012) and He (2013) for practitioners to design mobile device security training that targets both users' knowledge of security issues and their practical know-how of dealing with them. Such a practical approach will create an environment and culture where peer-to-peer review, collaboration and assistance on security issues is promoted among mobile device users. This will encourage mobile device users to believe in their know-how of protective security measures, thereby increasing their conformity and willingness to continuously apply them to their mobile devices (Tu et al., 2015).

### **Limitations and Future Studies**

The scope of this research was restrictive to information security behavior as it relates to mobile device users. Also, within the context of mobile device security, the scope of this study was limited to the constructs that represent the PMT core nomology. Hence the use of perceived threat severity, perceived threat susceptibility, response cost, response efficacy, self-efficacy, protection motivation, and security related behaviors. There was the exclusion of maladaptive rewards and fear from the scope of this study. The expectation is that future studies on mobile device security leveraging PMT will include maladaptive rewards and fear to represent the full nomology.

The result from this study unexpectedly shows that mobile device users' perceived response cost of security measures has no significant effect on their level of motivation to protect their devices from data breach. It is therefore proposed that future research in mobile device security pay particular attention to perceived response cost and study this construct further.

The data collected for this study was restricted to mobile device users in the United States of America. It is a recommendation of this study that future studies broaden the populations from which data is collected to include other geographic regions besides the United States of America. Additionally, future studies should consider data collection from populations sampled on the basis of culture, as a study leveraging such data criteria in this area of user information security behavior could possibly reveal some interesting findings.

Additionally, this study leveraged an online survey, also known as web-based survey for data collection. The limitation presented by web-based surveys is self-selection bias. Prospective respondents who feel they can appropriately complete a web-based survey and have knowledge of the subject matter may be the only ones who complete it. This limitation impacts the generalization of this research in terms of the general population studied.

## **Summary**

The primary premise on which this study was conducted was the identification and definition of an existing problem within the field of Information Systems. Thus, an empirical assessment of the information security usage behavior of mobile device users in the context of data breach. The introduction of this study also gave a background on the area of the research. Based on the review of previous literature, which were mentioned, this study sought to assess the effect that perceived threat severity, perceived threat susceptibility, perceived

response costs, response efficacy, and mobile self-efficacy have on shaping the protection motivation of mobile device users and determine whether that in turn leads to their usage of mobile device security. There was a presentation of a research question and based on that the development of hypotheses and a research model proposed. Also, barriers and issues that were faced in this study's attempt at proposing a solution to the problem were presented.

The literature review in this study highlighted and synthesized literature from other previous research studies and sources that examined user information security behavior. The foundational theory relied upon for this study is protection motivation theory (PMT). 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 the individual" (p. 409). Herath and Rao (2009) also noted that PMT shows individuals' protection motivation is based on perceived threats to themselves and their surroundings, and individuals cope with threats based on two processes: appraising the threat, and a coping appraisal in which the options to reduce or mitigate the threats are assessed. Overall, the literature review showed the constructs, findings, and contributions from previous literature, as well as existing gaps that needs further research.

The research design used for this study was captured in the Research Method chapter. The research strategy that was considered suitable for this study was the quantitative survey approach. The survey instrument, its reliability and validity, sample data, and data collection techniques were discussed. Nonprobability sampling design was used because data was collected from a specific target group, and in the case of this study, mobile device users. To ensure the reliability and validity of the instruments used in this research, a Delphi study was conducted using 11 subject matter experts. Additionally, a pilot study with 20 participants

was conducted before the main survey. Data analysis was done using SPSS and Smart PLS 3.0. Statistical tests conducted included Mahalanobis distance, normality, factor analysis, construct reliability and validity, PLS algorithm and bootstrapping. The interpretation of the various results from the statistical tests performed in this study have been presented in chapter 4 and in the appendices. The rejection or support of the hypotheses in this study were based on the analysis of the statistical results. The concluding chapter of this study presented implications of the findings, recommendations, limitations and suggestions for future research.

Terrel (2016) pointed out that a research problem investigated must have theoretical or practical significance. The focus and findings of this study is believed to have brought some clarity on mobile device users' information security behavior in the context of data compromise or breach. It deepened the understanding of elements that motivates mobile device users to protect data assets from data breach. Thus, it highlighted the psychological process that leads to the actual usage of mobile security by mobile device users. Furthermore, the use of PMT in this study to develop a research model within the context of mobile device security usage, brings additional insight to the existing literature. Also, there have been discussions on user autonomy in previous studies of which Warkentin and Willinson (2009) noted that systems' vulnerability, are more significant when users wield greater security decision making. The findings from this study sheds light on this ongoing discussion as it highlights how mobile device users, who wield autonomy in their security decision making behave to secure their mobile devices from data threats. Finally, the research model developed in this study will serve as an insightful premise for future research looking to extend the PMT constructs in an area of study in mobile device security

## Appendices

### Appendix A

#### *Survey Questionnaire*



NOVA SOUTHEASTERN UNIVERSITY  
College of Engineering and Computing

Participant Letter for Anonymous Surveys  
NSU Consent to be in a Research Study Entitled

*Empirical Assessment of Mobile Device Users' Information Security Behavior towards Data Breach: Leveraging Protection Motivation Theory.*

I am Anthony Duke Giwah and a doctoral student at the College of Engineering and Computing at Nova Southeastern University. I am currently working under the supervision of Dr. Ling Wang.

For the purpose of my doctoral dissertation, I am conducting a research that seeks your anonymous input to a survey. The survey is to understand the factors that contribute to the information security usage of mobile device users in the context of data breach.

Mobile device in this survey refers to a mobile phone, tablet, or laptop.

You will be taking a one-time, anonymous survey. The survey will take approximately 15 minutes or less to complete.

There are no foreseeable risks linked with your participation in this study.

You may choose to stop participating in the survey at any point in time by closing the web page that is showing the survey.

There is no cost for participation in this study. Participation is voluntary and no payment will be provided.

If you have read the above information and voluntarily wish to participate in this research study, please click on the "Next" button below on this page.

All responses to the survey are completely anonymous and the researcher will not be able to associate you with any information provided. Also, no personal identifiable data is being collected or stored from this survey.

If you have questions, you can contact Anthony Duke Giwah at +1 646-404-0449.

If you have questions about the study but want to talk to someone else who is not a part of the study, you can call the Nova Southeastern University Institutional Review Board (IRB) at (954) 262-5369 or toll free at 1-866-499-0790 or email at [IRB@nova.edu](mailto:IRB@nova.edu).

\* Required

### Perceived Threat Severity

Please indicate the impact that each of these scenarios would have on you if it would occur.

 **PTSE 1. My mobile device becoming corrupted by a virus.** ★

1	2	3	4	5	6	7
Very Low Impact	Low Impact	Medium Low Impact	Medium Impact	Medium High Impact	High Impact	Very High Impact

**PTSE 2. My mobile device being taken over by a hacker. \***

1	2	3	4	5	6	7
Very Low Impact	Low Impact	Medium Low Impact	Medium Impact	Medium High Impact	High Impact	Very High Impact

**PTSE 3. My mobile device being attacked for sensitive personal data (bank account, social security, etc). \***

1	2	3	4	5	6	7
Very Low Impact	Low Impact	Medium Low Impact	Medium Impact	Medium High Impact	High Impact	Very High Impact
○	○	○	○	○	○	○

**PTSE 4. My mobile device losing data due to a virus. \***

1	2	3	4	5	6	7
Very Low Impact	Low Impact	Medium Low Impact	Medium Impact	Medium High Impact	High Impact	Very High Impact

**PTSE 5. My mobile device downloading a virus or bug infected application. \***

1	2	3	4	5	6	7
Very Low Impact	Low Impact	Medium Low Impact	Medium Impact	Medium High Impact	High Impact	Very High Impact
○	○	○	○	○	○	○

### Perceived Threat Susceptibility

Please indicate how likely you feel each scenario will occur with your mobile device.

**PTSU 1. My mobile device becoming corrupted by a virus. \***

1                      2                      3                      4                      5                      6                      7  
Highly Unlikely      Unlikely              Somewhat Unlikely      Neutral              Somewhat Likely      Likely              Highly Likely  
○                      ○                      ○                      ○                      ○                      ○                      ○

**PTSU 2. My mobile device being taken over by a hacker. \***

1                      2                      3                      4                      5                      6                      7  
Highly Unlikely      Unlikely      Somewhat Unlikely      Neutral      Somewhat Likely      Likely      Highly Likely  
○                      ○                      ○                      ○                      ○                      ○                      ○

**PTSU 3. My mobile device being attacked for sensitive personal data (bank account, social security, etc.). \***

1  
Highly Unlikely

2  
Unlikely

3  
Somewhat Unlikely

4  
Neutral

5  
Somewhat Likely

6  
Likely

7  
Highly Likely

**PTSU 4. My mobile device losing data due to a virus. \***

1                      2                      3                      4                      5                      6                      7  
Highly Unlikely      Unlikely              Somewhat Unlikely      Neutral              Somewhat Likely      Likely              Highly Likely

**PTSU 5. My mobile device downloading a virus or bug infected application.\***

1                      2                      3                      4                      5                      6                      7  
Highly Unlikely      Unlikely              Somewhat Unlikely      Neutral              Somewhat Likely      Likely              Highly Likely  
○                      ○                      ○                      ○                      ○                      ○                      ○

### Perceived Response Cost

Please indicate the degree to which you agree or disagree with the following statements.

**PRC 1. Using an anti-virus software on my mobile device decreases the device's convenience. \***

1	2	3	4	5	6	7
Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree or Disagree	Somewhat Agree	Agree	Strongly Agree
○	○	○	○	○	○	○

**PRC 2. Using an anti-malware software on my mobile device decreases the device's convenience. \***

1	2	3	4	5	6	7
Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree or Disagree	Somewhat Agree	Agree	Strongly Agree
○	○	○	○	○	○	○

**PRC 3. Using an anti-virus software on my mobile device involves too much work. \***

1	2	3	4	5	6	7
Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree or Disagree	Somewhat Agree	Agree	Strongly Agree
○	○	○	○	○	○	○

**PRC 4. Using an anti-malware software on my mobile device involves too much work. \***

1	2	3	4	5	6	7
Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree or Disagree	Somewhat Agree	Agree	Strongly Agree
○	○	○	○	○	○	○

**PRC 5. Using an anti-virus software on my mobile device requires considerable investment. \***

[illegible]

**PRC 6. Using an anti-malware software on my mobile device requires considerable investment. \***

1	2	3	4	5	6	7
Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree or Disagree	Somewhat Agree	Agree	Strongly Agree
○	○	○	○	○	○	○

**PRC 7. Using an anti-virus software on my mobile device is time consuming.\***

1	2	3	4	5	6	7
Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree or Disagree	Somewhat Agree	Agree	Strongly Agree
○	○	○	○	○	○	○

**PRC 8. Using an anti-malware software on my mobile device is time consuming. \***

1	2	3	4	5	6	7
Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree or Disagree	Somewhat Agree	Agree	Strongly Agree
○	○	○	○	○	○	○

### Response Efficacy

Please indicate the degree to which you agree or disagree with the following statements.

**RE 1. Using an anti-virus software works to protect my mobile device from data breach. \***

[illegible]



[illegible]



### Protection Motivation

Please indicate the degree to which you agree or disagree with the following statements.

**PM 1. I am motivated to protect my mobile device from threats of data breach. \***

[illegible]

**PM 2. I am motivated to prevent threats of data breach to my mobile device from being successful. \***

1	2	3	4	5	6	7
Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree or Disagree	Somewhat Agree	Agree	Strongly Agree
○	○	○	○	○	○	○

**PM 3. I am motivated to engage in activities that protect my mobile device from threats of data breach. \***

1	2	3	4	5	6	7
Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree or Disagree	Somewhat Agree	Agree	Strongly Agree
○	○	○	○	○	○	○

## Mobile Device Security Usage

Please indicate the frequency you perform the following tasks.

**MDSU 1. I use a method to backup my mobile device (to PC, external hard drive, cloud, network storage, etc...). \***

1 2 3 4 5 6 7  
Never Almost Never Rarely Occasionally Sometimes Almost Every Time Every Time

**MDSU 2. I use the firewall protection on my mobile device. \***

1	2	3	4	5	6	7
Never	Almost Never	Rarely	Occasionally	Sometimes	Almost Every Time	Every Time

**MDSU 3. I use an anti-virus software on my mobile device. \***

1  
Never  
○

2  
Almost Never  
○

3  
Rarely  
○

4  
Occasionally  
○

5  
Sometimes  
○

6  
Almost Every Time  
○

7  
Every Time  
○

**MDSU 4. I use an anti-malware software on my mobile device. \***

1	2	3	4	5	6	7
Never	Almost Never	Rarely	Occasionally	Sometimes	Almost Every Time	Every Time
○	○	○	○	○	○	○

**MDSU 5. I use password protection on my mobile device. \***

1	2	3	4	5	6	7
Never	Almost Never	Rarely	Occasionally	Sometimes	Almost Every Time	Every Time
○	○	○	○	○	○	○

**MDSU 6. I use biometric protection on my mobile device. \***

1                  2                  3                  4                  5                  6                  7  
Never      Almost Never      Rarely      Occasionally      Sometimes      Almost Every Time      Every Time

**MDSU 7. I use software updates on my mobile device whenever they are available. \***

1                      2                      3                      4                      5                      6                      7  
Never            Almost Never            Rarely            Occasionally            Sometimes            Almost Every Time            Every Time

**MDSU 8. I use operating system updates on my mobile device whenever they are available. \***

1	2	3	4	5	6	7
Never	Almost Never	Rarely	Occasionally	Sometimes	Almost Every Time	Every Time

## Appendix B:

### IRB Approval



NOVA SOUTHEASTERN UNIVERSITY  
Institutional Review Board

I

#### MEMORANDUM

To: **Anthony Giwah**

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

Date: **October 2, 2018**

Re: **IRB #: 2018-486; Title, "Understanding the Information Security Behavior of Mobile Device Users towards Data Breach: Leveraging Protection Motivation Theory"**

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:

### *Mahalanobis Distance and Stem & Leaf Plot*

#### Descriptives

		Statistic	Std. Error
Mahalanobis Distance	Mean	38.9000000	.75009126
	95% Confidence Interval for Lower Bound	37.4252598	
	Mean Upper Bound	40.3747402	
	5% Trimmed Mean	38.0948167	
	Median	35.9621763	
	Variance	219.428	
	Std. Deviation	14.81311556	
	Minimum	14.67787	
	Maximum	91.15588	
	Range	76.47800	
	Interquartile Range	18.92554	
	Skewness	.814	.124
	Kurtosis	.395	.247

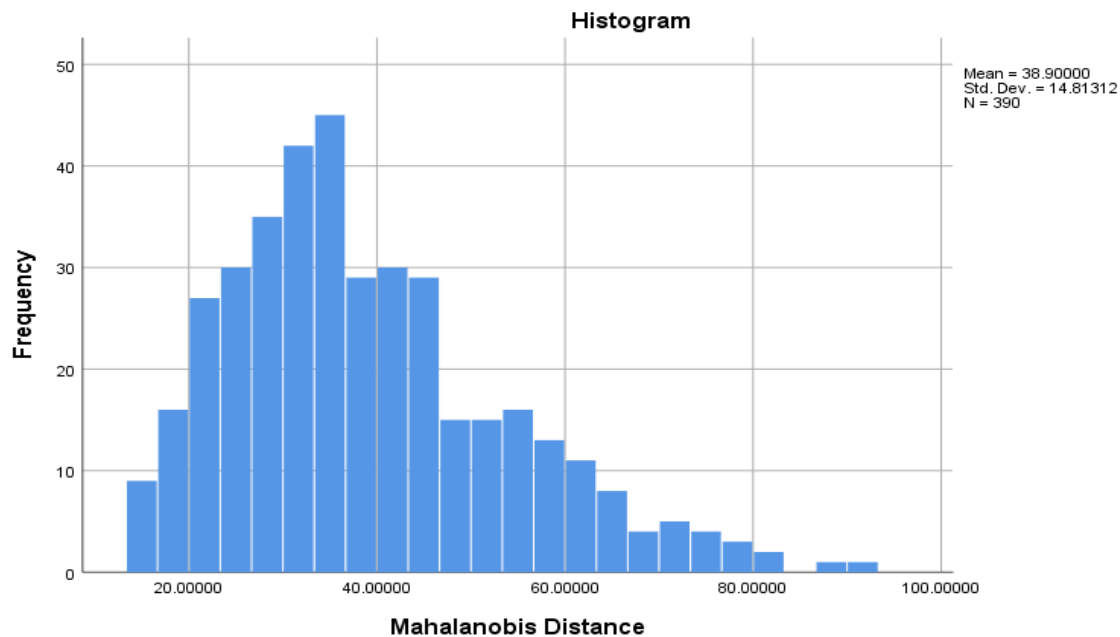
#### Extreme Values

			Case Number	Value
Mahalanobis Distance	Highest	1	25	91.15588
		2	388	88.77158
		3	197	80.71384
		4	6	80.42758
		5	355	79.63766
	Low est	1	36	14.67787
		2	78	14.82615
		3	60	14.90735
		4	51	15.19698
		5	5	15.25854

### Tests of Normality

	Kolmogorov-Smirnov <sup>a</sup>			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Mahalanobis Distance	.085	390	.000	.953	390	.000

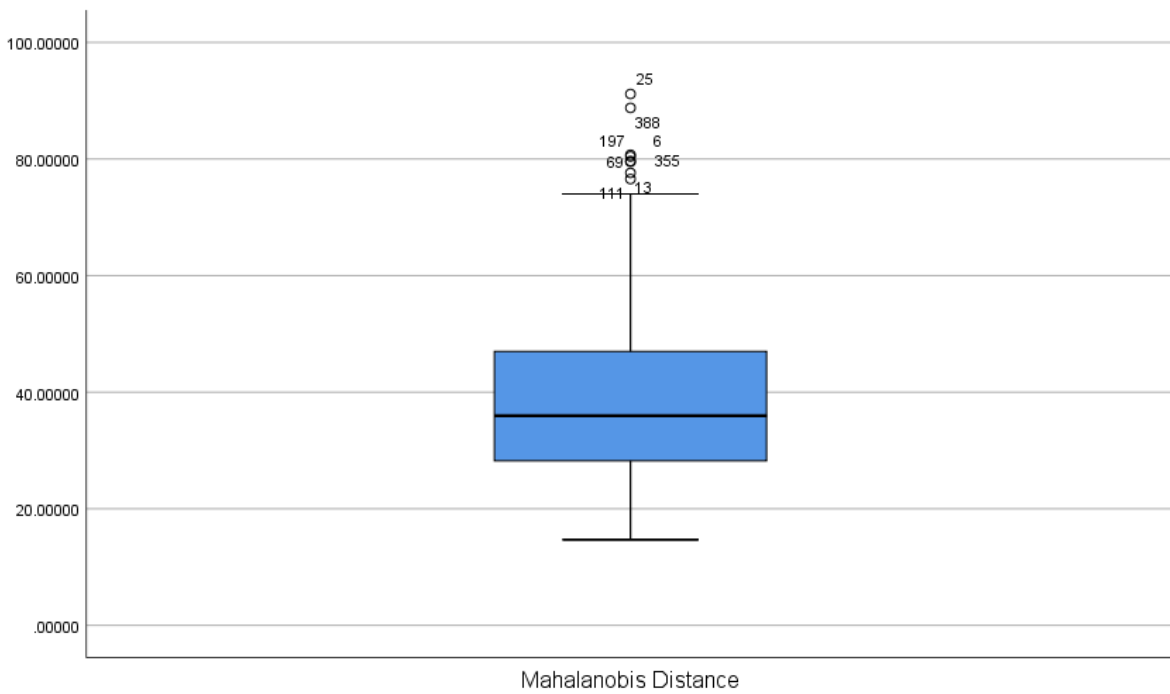
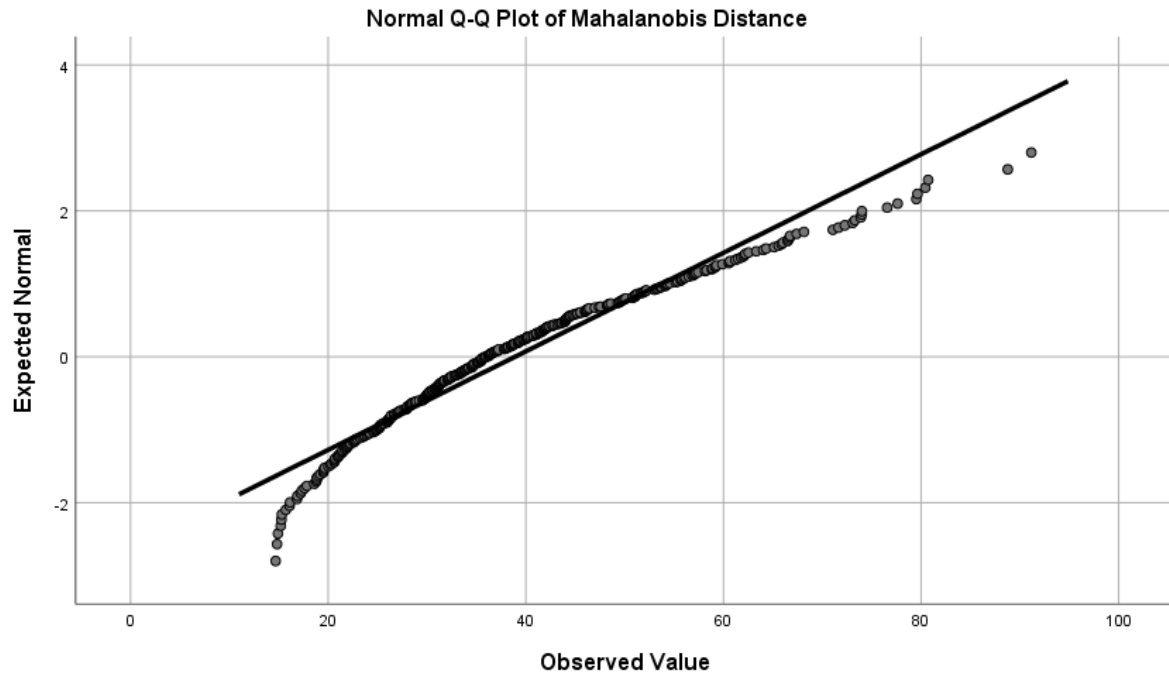
a. Lilliefors Significance Correction



Mahalanobis Distance Stem-and-Leaf Plot

Frequency	Stem &	Leaf
3.00	1 .	444
22.00	1 .	5555666677778888999999
37.00	2 .	0000000011111111222222223333344444
55.00	2 .	
55.00	2 .	55555555666666666666667777777788888888888889999999999
64.00	3 .	
00.00	3 .	00000000000001111111111111222222222222333333333334444444444
52.00	3 .	55555555555555666666666666777777788888888889999999999
48.00	4 .	00000001111111111111222222223333333444444444444
26.00	4 .	55556666666677888889999999
23.00	5 .	00011111111223333344444
21.00	5 .	555556666777788889999
13.00	6 .	0001112222344
10.00	6 .	555666678
8.00	7 .	1123334
8.00	Extremes	(>=77)

Stem width: 10.00000  
Each leaf: 1 case(s)



**Appendix D:**

*Rerun of Mahalanobis Distance and Stem & Leaf Plot after 2 extreme values deleted*

**Descriptives**

		Statistic	Std. Error
Mahalanobis Distance	Mean	38.8994845	.73587242
	95% Confidence Interval for Lower Bound	37.4526764	
	Mean Upper Bound	40.3462927	
	5% Trimmed Mean	38.1853458	
	Median	36.1707295	
	Variance	210.105	
	Std. Deviation	14.49500572	
	Minimum	14.70125	
	Maximum	84.17324	
	Range	69.47200	
	Interquartile Range	18.87143	
	Skew ness	.718	.124
	Kurtosis	.069	.247

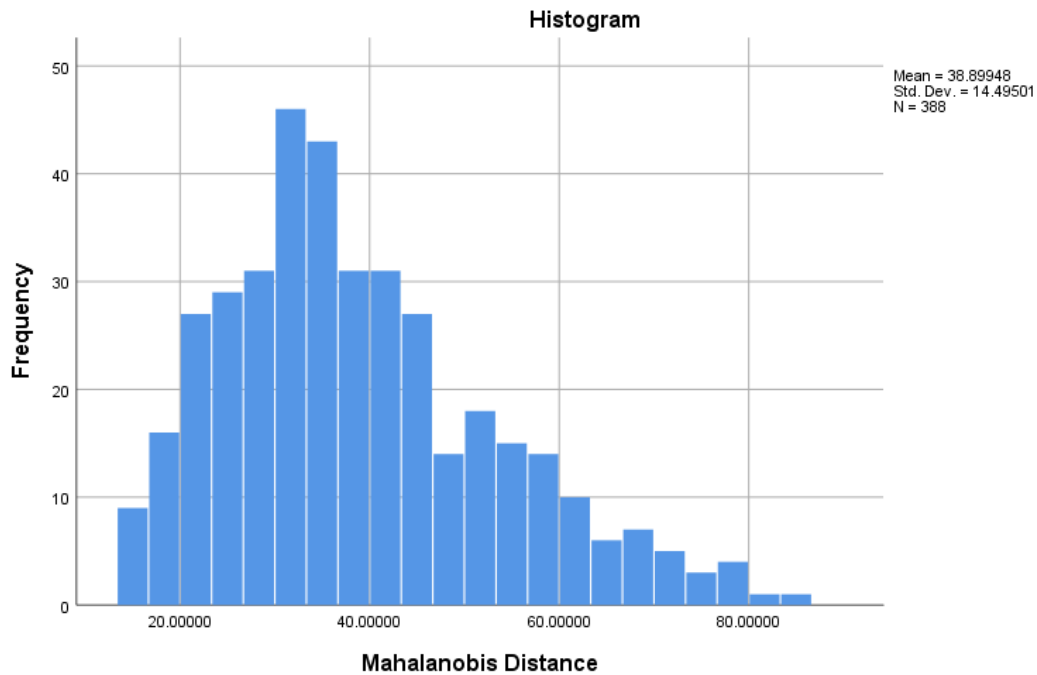
**Extreme Values**

		Case Number	Value
Mahalanobis Distance	Highest	1	196
		2	6
		3	354
		4	68
		5	13
	Low est	1	35
		2	77
		3	59
		4	50
		5	5

### Tests of Normality

	Kolmogorov-Smirnov <sup>a</sup>			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Mahalanobis Distance	.081	388	.000	.958	388	.000

a. Lilliefors Significance Correction

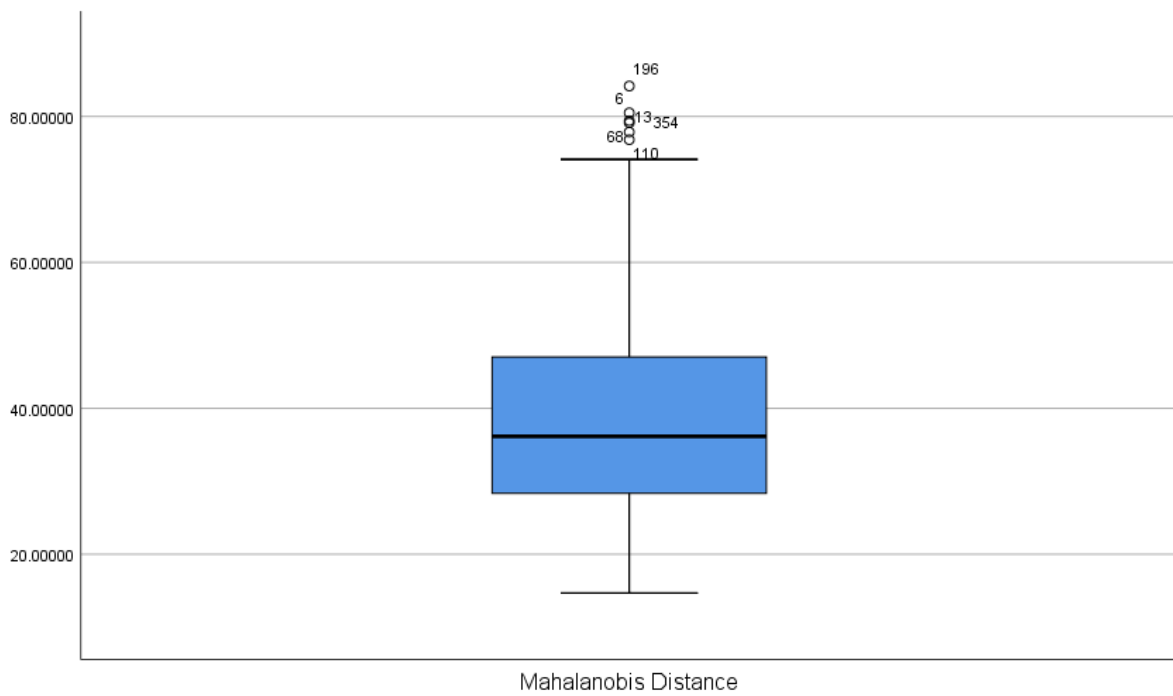
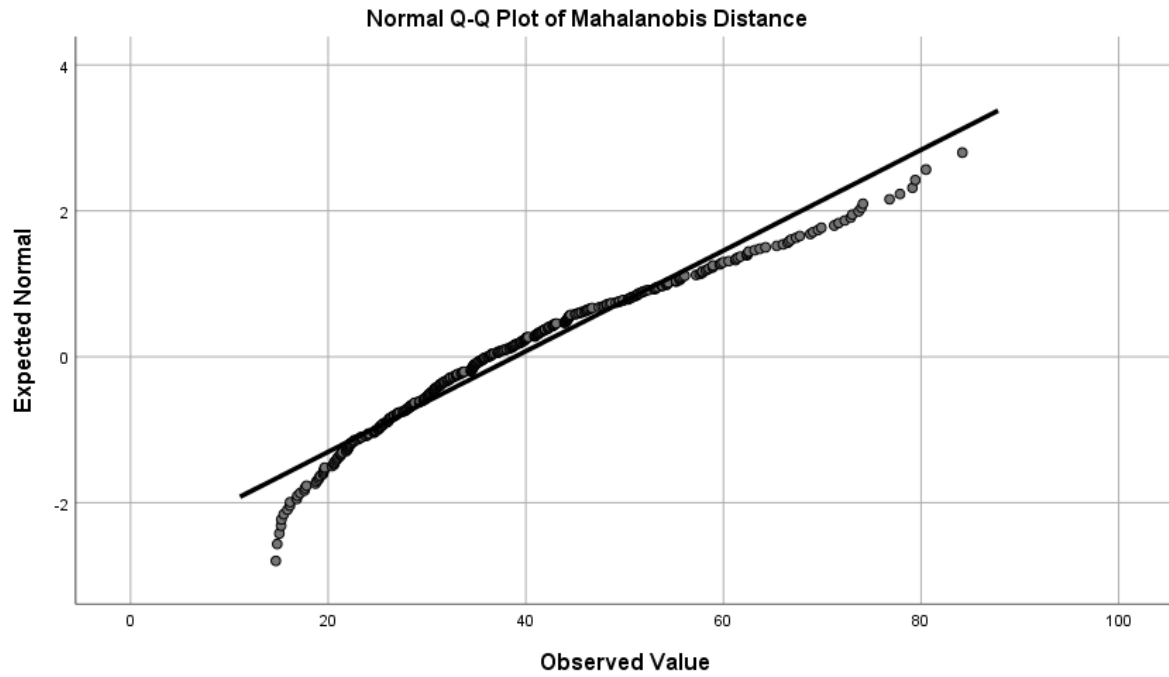


Mahalanobis Distance Stem-and-Leaf Plot

Frequency	Stem &	Leaf
2.00	1 .	44
23.00	1 .	55555666677778889999999
36.00	2 .	0000001111111122222222333344444
51.00	2 .	55555555556666666666667777777888888888999999999
68.00	3 .	
000000000000000000011111111112222222222333333334444444444444444		
52.00	3 .	555555555555666666666777777788888888889999999999999
48.00	4 .	00000001111111111122222222223333444444444444444
24.00	4 .	55555666666777888899999
25.00	5 .	000011111111223333334444
22.00	5 .	555555677777888888999
12.00	6 .	01112222334
11.00	6 .	5666778999
8.00	7 .	1122334
6.00	Extremes	(>=77)

Stem width: 10.00000

Each leaf: 1 case(s)





## Appendix E:

### Normality and Scatter Plot

**Model Summary<sup>b</sup>**

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.649 <sup>a</sup>	.421	.412	.539

a. Predictors: (Constant), PM, PTSE, PRC, RE, MSE, PTSU

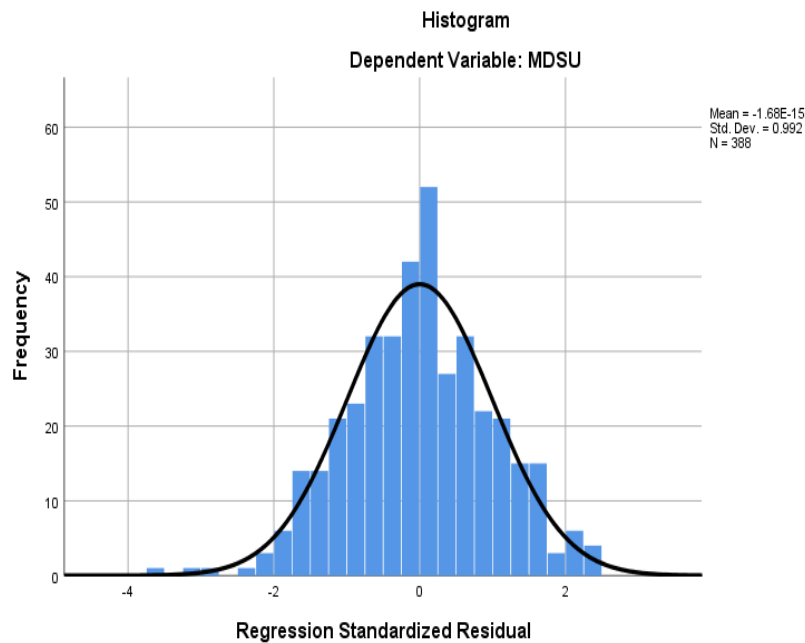
b. Dependent Variable: MDSU

**ANOVA<sup>a</sup>**

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	80.397	6	13.400	46.106	.000 <sup>b</sup>
	Residual	110.729	381	.291		
	Total	191.126	387			

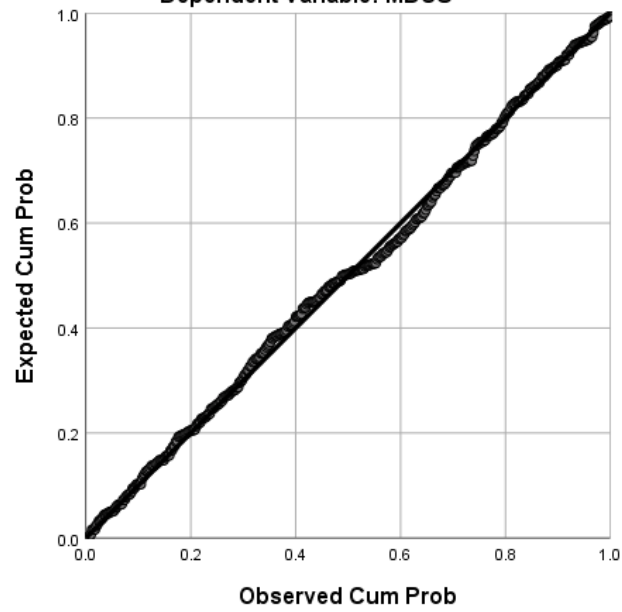
a. Dependent Variable: MDSU

b. Predictors: (Constant), PM, PTSE, PRC, RE, MSE, PTSU



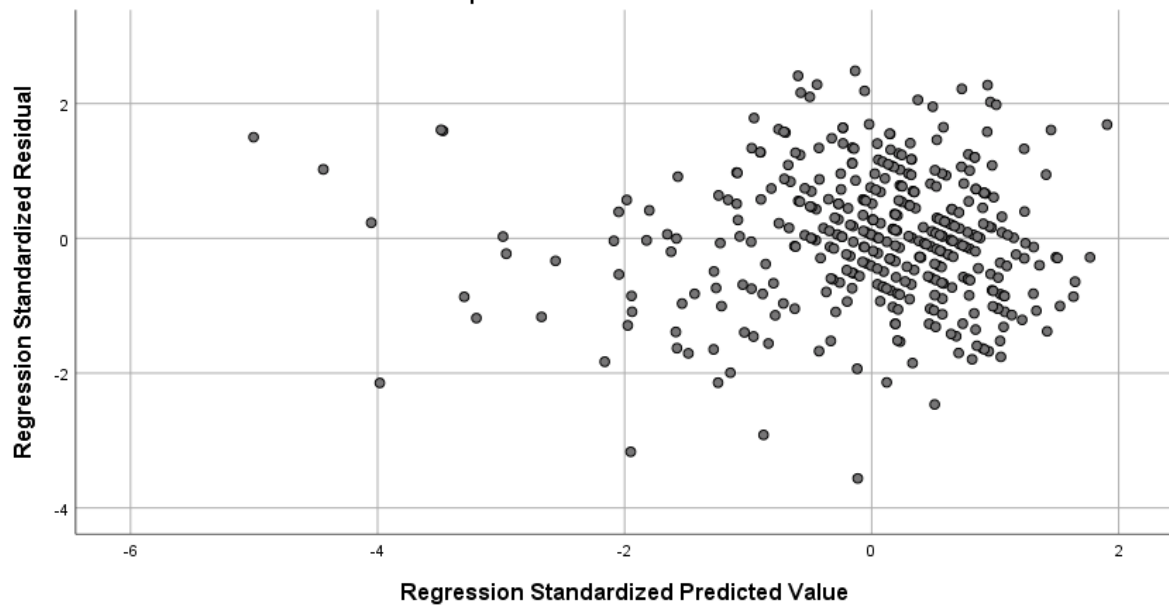
Normal P-P Plot of Regression Standardized Residual

Dependent Variable: MDSU



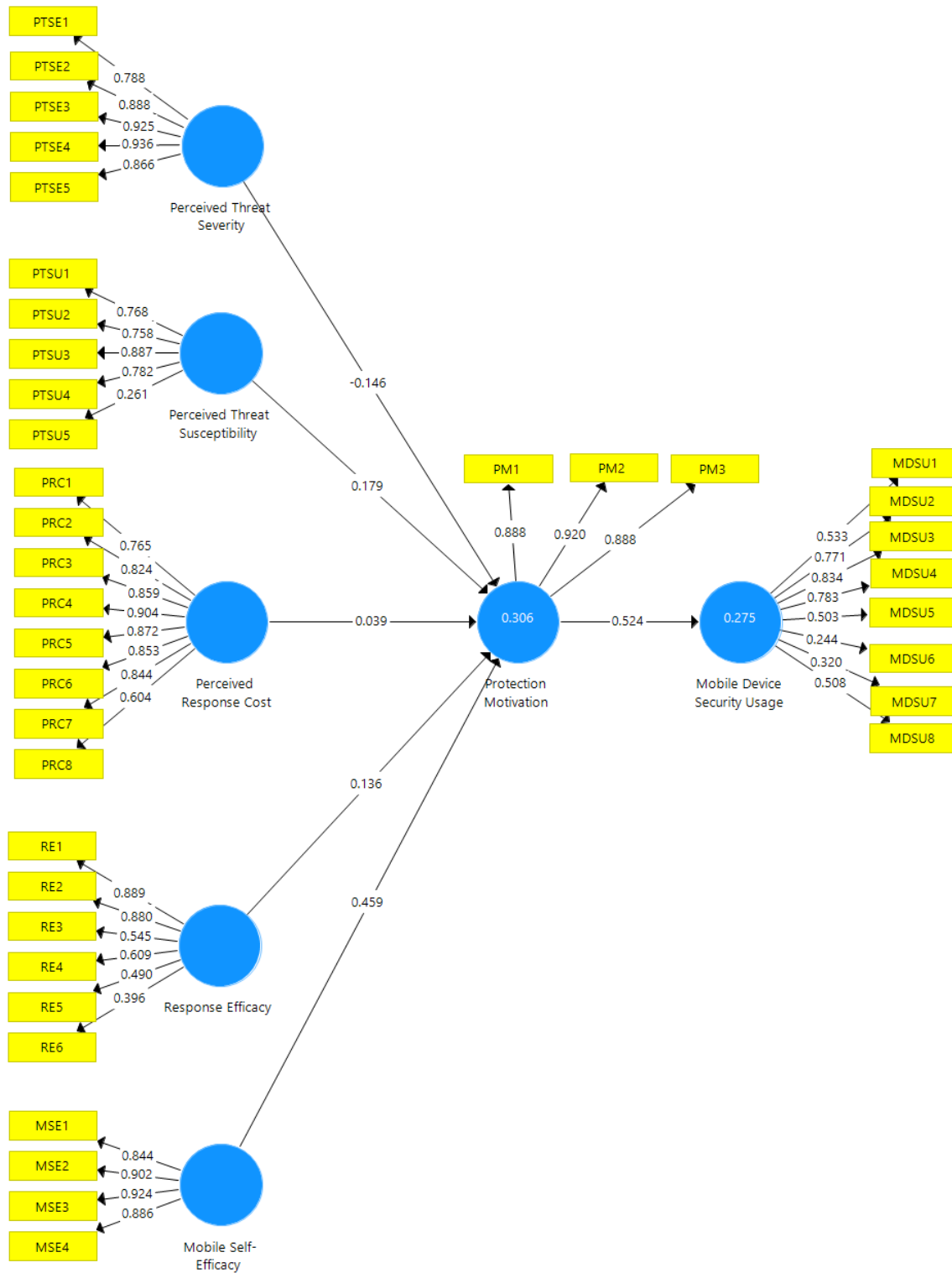
Scatterplot

Dependent Variable: MDSU



## Appendix F

### PLS Analysis with Factor Loadings



## Appendix G:

### *Model fit, Reliability, Validity, Coefficient and Outer Loading*

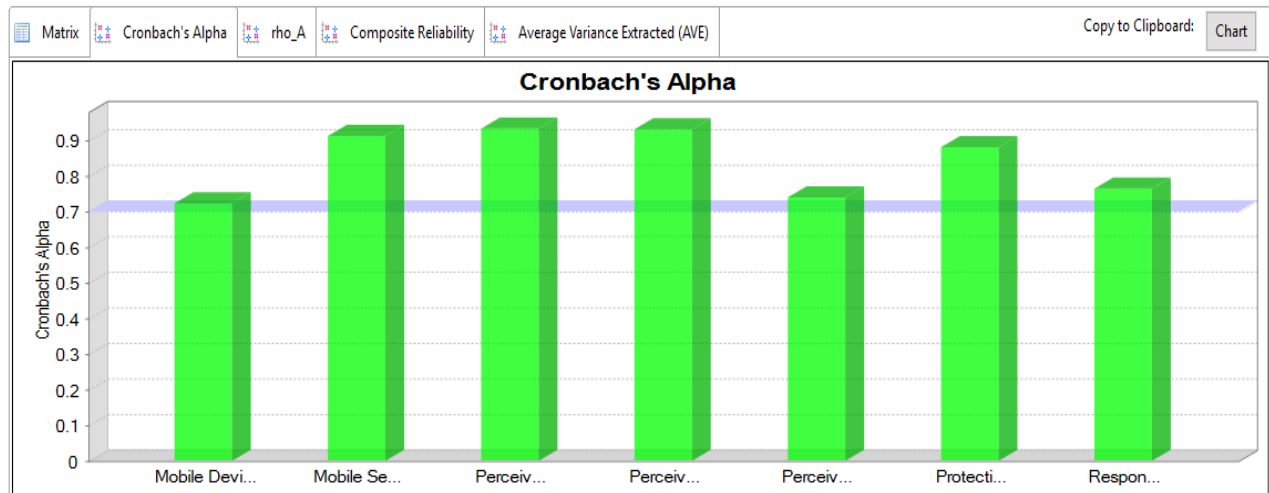
#### Model\_Fit

Fit Summary			rms Theta	
	Saturated Model	Estimated Mo...		
SRMR	0.079	0.095		
d_ULS	4.852	7.023		
d_G	1.419	1.505		
Chi-Square	2,921.225	3,051.895		
NFI	0.724	0.711		

#### Construct Reliability and Validity

Matrix	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Mobile Device Security Usage	0.723	0.802	0.797	0.358
Mobile Self-Efficacy	0.912	0.920	0.938	0.791
Perceived Response Cost	0.933	0.974	0.942	0.673
Perceived Threat Severity	0.931	1.006	0.946	0.778
Perceived Threat Susceptibility	0.740	0.827	0.834	0.526
Protection Motivation	0.881	0.882	0.926	0.808
Response Efficacy	0.764	0.893	0.811	0.438

### Construct Reliability and Validity



### Discriminant Validity

Fornell-Larcker Criterion Cross Loadings Heterotrait-Monotrait Ratio (HTMT) Heterotrait-Monotrait Ratio (HTMT) Copy to Clipboard: Excel Format

	Mobile Device Security Us...	Mobile Self-Effi...	Perceived Response C...	Perceived Threat Sev...	Perceived Threat Susc...	Protection Motiv...	Response Efficacy
Mobile Device Security Usage	0.598						
Mobile Self-Efficacy	0.572	0.890					
Perceived Response Cost	0.289	0.187	0.821				
Perceived Threat Severity	0.181	0.098	0.259	0.882			
Perceived Threat Susceptibility	0.142	0.080	0.193	0.685	0.725		
Protection Motivation	0.524	0.519	0.139	0.058	0.149	0.899	
Response Efficacy	0.476	0.384	0.122	0.188	0.188	0.323	0.662

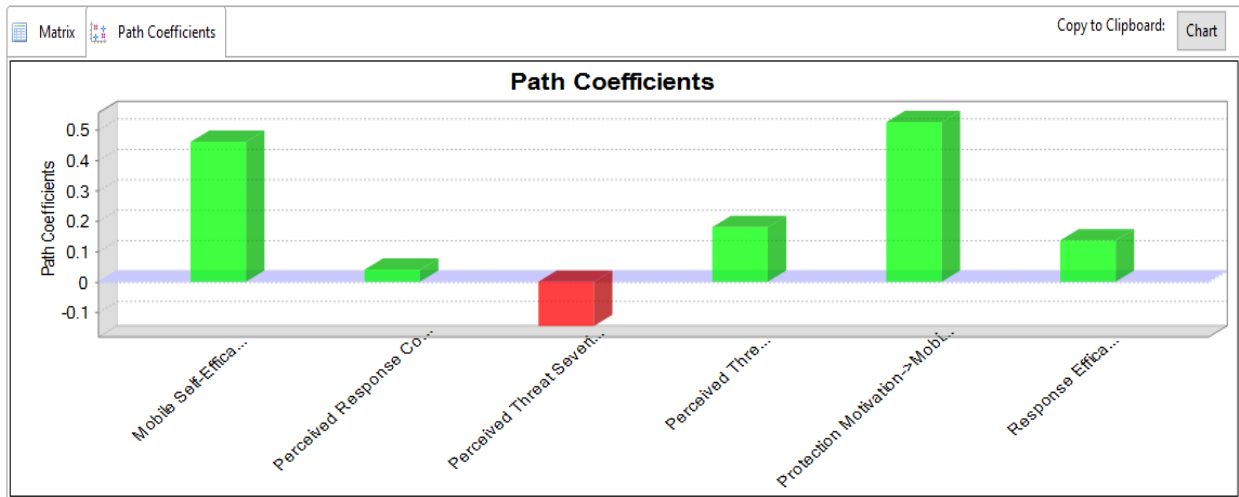
## Outer Loadings

	Mobile Device Security Usage	Mobile Self-Efficacy	Perceived Response Cost	Perceived Threat Severity	Perceived Threat Susceptibility	Protection Motivation	Response Efficacy
MDSU1	0.533						
MDSU2	0.771						
MDSU3	0.834						
MDSU4	0.783						
MDSU5	0.503						
MDSU6	0.244						
MDSU7	0.320						
MDSU8	0.508						
MSE1		0.844					
MSE2		0.902					
MSE3		0.924					
MSE4		0.886					
PM1						0.888	
PM2						0.920	
PM3						0.888	
PRC1			0.765				
PRC2			0.824				
PRC3			0.859				
PRC4			0.904				
PRC5			0.872				
PRC6			0.853				
PRC7			0.844				
PRC8			0.604				
PTSE2				0.888			
PTSE3				0.925			
PTSE4				0.936			
PTSE5				0.866			
PTSU1					0.768		
PTSU2					0.758		
PTSU3					0.887		
PTSU4					0.782		
PTSU5					0.261		
RE1							0.889
RE2							0.880
RE3							0.545
RE4							0.609
RE5							0.490
RE6							0.396
PTSE1				0.788			

### Path Coefficients

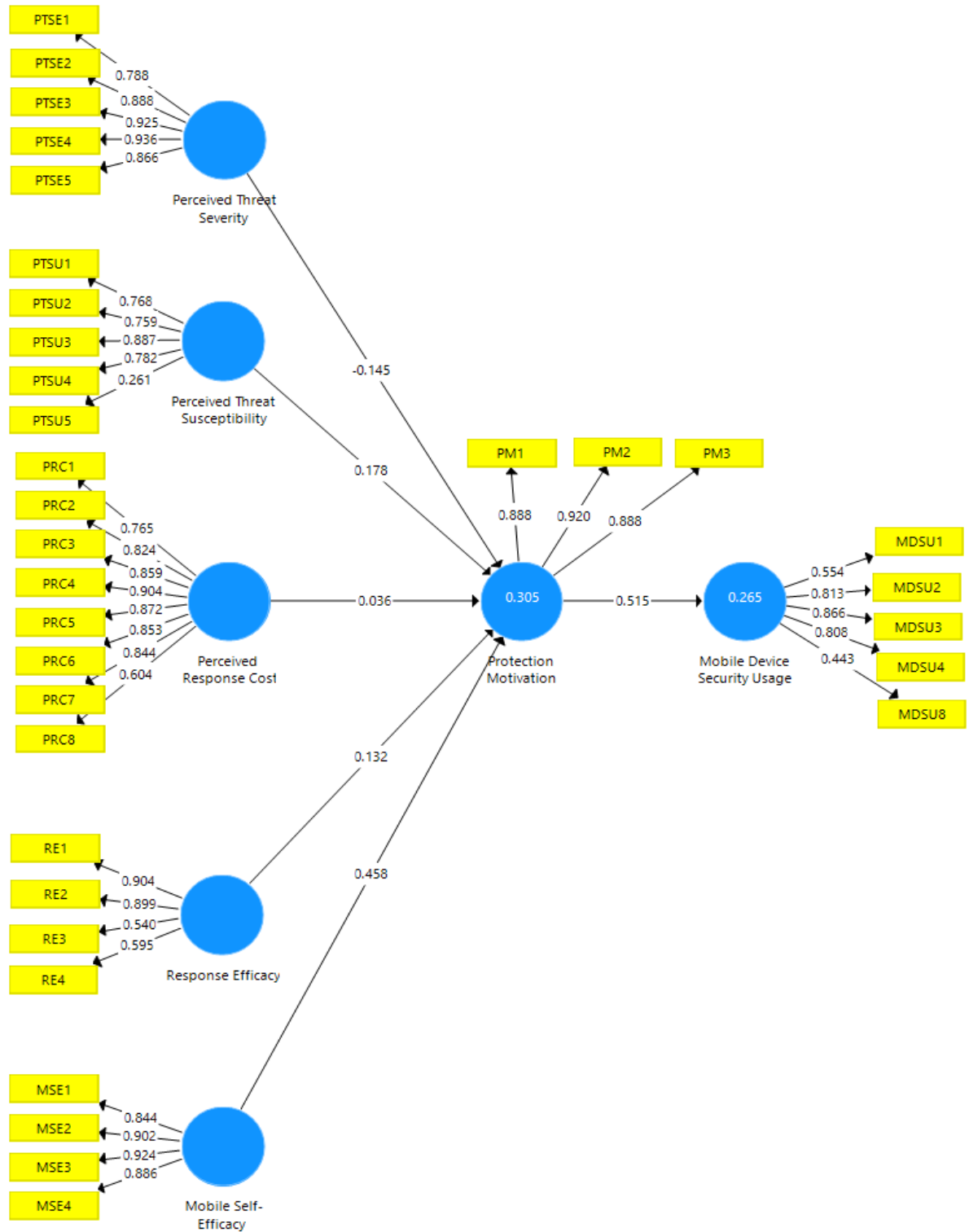
Matrix	Path Coefficients	Copy to Clipboard: <a href="#">Excel Format</a> <a href="#">R1</a>					
	Mobile Device Security Us...	Mobile Self-Effi...	Perceived Response C...	Perceived Threat Seve...	Perceived Threat Susc...	Protection Motiva...	Response Efficacy
Mobile Device Security Usage							
Mobile Self-Efficacy						0.459	
Perceived Response Cost						0.039	
Perceived Threat Severity						-0.146	
Perceived Threat Susceptibility						0.179	
Protection Motivation	0.524						
Response Efficacy						0.136	

## Path Coefficients



## Appendix H:

*PLS Analysis after deleting RE5, RE6, MDSU5, MDSU6, and MDSU 7*





## Appendix I:

### *Model fit, Reliability, Validity, Coefficient and Outer Loading*

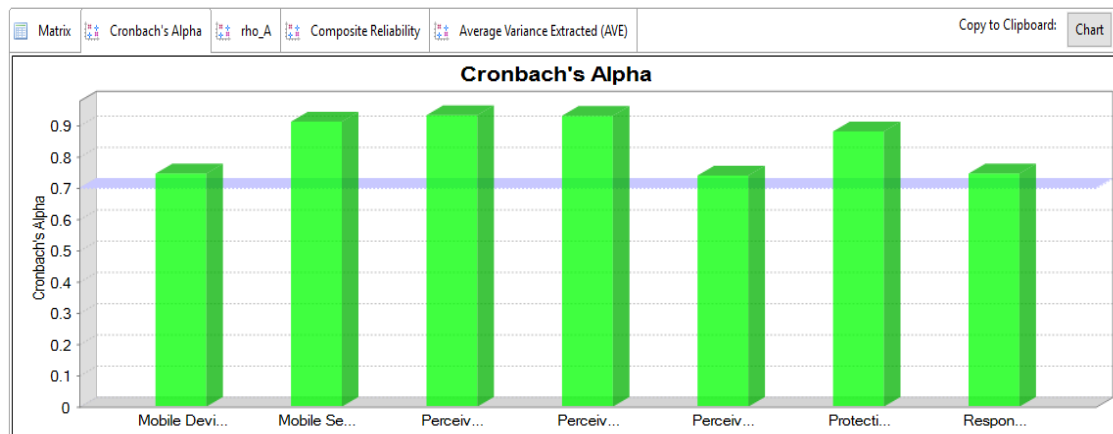
#### Model\_Fit

Fit Summary			rms Theta	
	Saturated Model	Estimated Mo...		
SRMR	0.066	0.090		
d_ULS	2.629	4.794		
d_G	0.973	1.069		
Chi-Square	2,103.022	2,250.544		
NFI	0.781	0.766		

#### Construct Reliability and Validity

Matrix	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
	Cronbach's Al...	rho_A	Composite Rel...	Average Varian...
Mobile Device Security Usage	0.746	0.803	0.833	0.513
Mobile Self-Efficacy	0.912	0.920	0.938	0.791
Perceived Response Cost	0.933	0.974	0.942	0.673
Perceived Threat Severity	0.931	1.007	0.946	0.778
Perceived Threat Susceptibility	0.740	0.827	0.834	0.526
Protection Motivation	0.881	0.882	0.926	0.808
Response Efficacy	0.746	0.868	0.833	0.568

#### Construct Reliability and Validity



## R Square

Matrix	R Square	R Square Adjusted
	R Square	R Square Adjusted
Mobile Device Security Usage	0.265	0.263
Protection Motivation	0.305	0.295

## Discriminant Validity

Fornell-Larcker Criterion	Cross Loadings	Heterotrait-Monotrait Ratio (HTMT)	Heterotrait-Monotrait Ratio (HTMT)	Copy to Clipboard: <a href="#">Excel Format</a> <a href="#">R For</a>			
	Mobile Device Security Us...	Mobile Self-Eff...	Perceived Response C...	Perceived Threat Sever...	Perceived Threat Susc...	Protection Motivation	Response Efficacy
Mobile Device Security Usage	0.717						
Mobile Self-Efficacy	0.622	0.890					
Perceived Response Cost	0.267	0.187	0.820				
Perceived Threat Severity	0.167	0.098	0.259	0.882			
Perceived Threat Susceptibility	0.132	0.080	0.193	0.685	0.725		
Protection Motivation	0.515	0.519	0.139	0.058	0.149	0.899	
Response Efficacy	0.495	0.409	0.150	0.202	0.205	0.332	0.754

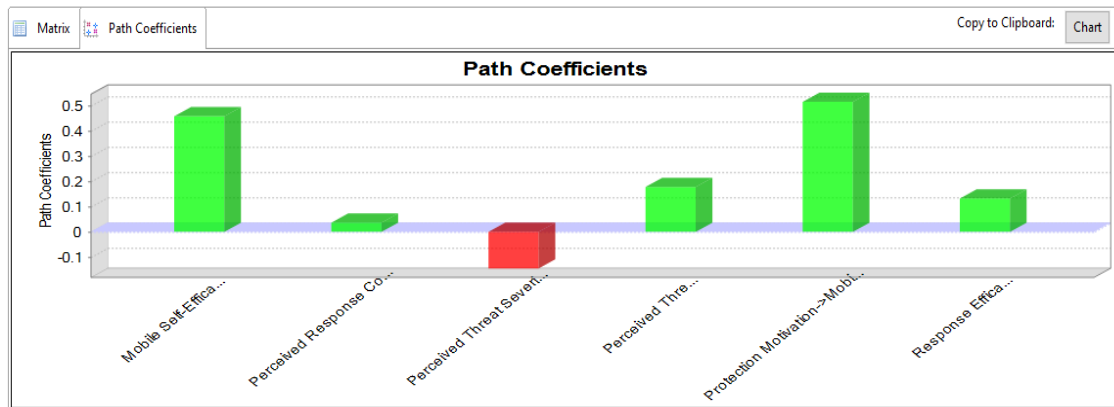
## Outer Loadings

	Mobile Device Security Usage	Mobile Self-Efficacy	Perceived Response Cost	Perceived Threat Severity	Perceived Threat Susceptibility	Protection Motivation	Response Efficacy
MDSU1	0.554						
MDSU2	0.813						
MDSU3	0.866						
MDSU4	0.808						
MDSU8	0.443						
MSE1		0.844					
MSE2		0.902					
MSE3		0.924					
MSE4		0.886					
PM1						0.888	
PM2						0.920	
PM3						0.888	
PRC1			0.765				
PRC2			0.824				
PRC3			0.859				
PRC4			0.904				
PRC5			0.872				
PRC6			0.853				
PRC7			0.844				
PRC8			0.604				
PTSE2				0.888			
PTSE3				0.925			
PTSE4				0.936			
PTSE5				0.866			
PTSU1					0.768		
PTSU2					0.758		
PTSU3					0.887		
PTSU4					0.782		
PTSU5					0.261		
RE1							0.904
RE2							0.899
RE3							0.540
RE4							0.595
PTSE1				0.788			

### Path Coefficients

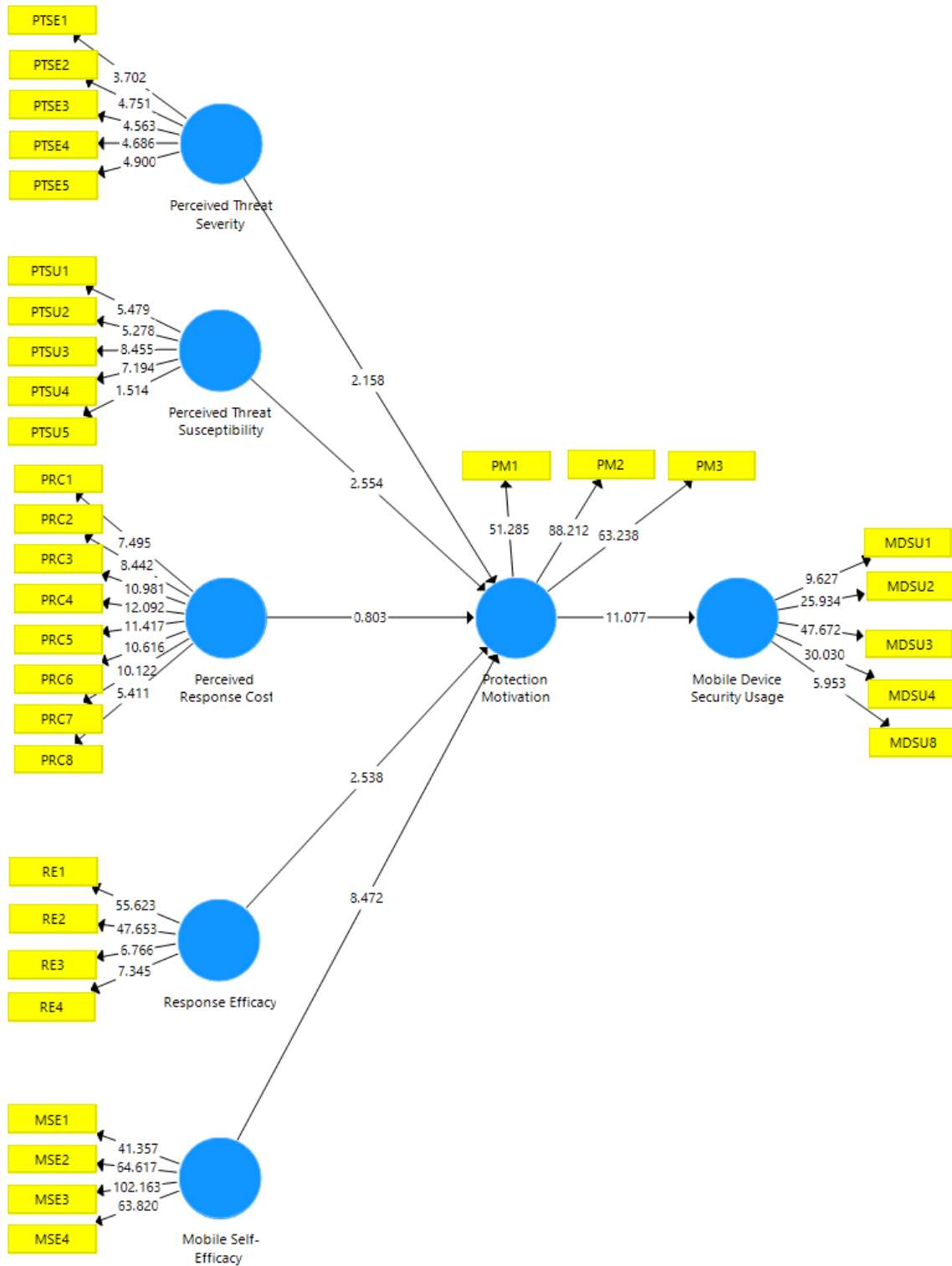
Matrix	Path Coefficients	Copy to Clipboard					
	Mobile Device ...	Mobile Self-Eff...	Perceived Resp...	Perceived Thre...	Perceived Thre...	Protection Mo...	Response Effic...
Mobile Device Security Usage							
Mobile Self-Efficacy						0.458	
Perceived Response Cost						0.036	
Perceived Threat Severity						-0.145	
Perceived Threat Susceptibility						0.178	
Protection Motivation	0.515						
Response Efficacy						0.132	

### Path Coefficients



## Appendix J:

### *Significance with Bootstrapping*



### Path Coefficients

Mean, STDEV, T-Values, P-Values	Confidence Intervals	Confidence Intervals Bias Corrected	Samples	Copy to Clipboard: Excel Fon	
	Original Sample (O)	Sample Mean (M)	Standard Deviation (S...	T Statistics ( O /STDEV)	P Values
Mobile Self-Efficacy -> Protection Motivation	0.458	0.450	0.054	8.472	0.000
Perceived Response Cost -> Protection Motivation	0.036	0.040	0.045	0.803	0.422
Perceived Threat Severity -> Protection Motivation	-0.145	-0.122	0.067	2.158	0.031
Perceived Threat Susceptibility -> Protection Motivation	0.178	0.168	0.070	2.554	0.011
Protection Motivation -> Mobile Device Security Usage	0.515	0.519	0.046	11.077	0.000
Response Efficacy -> Protection Motivation	0.132	0.135	0.052	2.538	0.011

### Total Effects

Mean, STDEV, T-Values, P-Values	Confidence Intervals	Confidence Intervals Bias Corrected	Samples	Copy to Clipboard:	
	Original Sampl...	Sample Mean (...)	Standard Devia...	T Statistics ( O...	P Values
Mobile Self-Efficacy -> Mobile Device Security Usage	0.236	0.235	0.043	5.491	0.000
Mobile Self-Efficacy -> Protection Motivation	0.458	0.450	0.054	8.472	0.000
Perceived Response Cost -> Mobile Device Security Usage	0.019	0.021	0.023	0.809	0.419
Perceived Response Cost -> Protection Motivation	0.036	0.040	0.045	0.803	0.422
Perceived Threat Severity -> Mobile Device Security Usage	-0.075	-0.063	0.035	2.152	0.032
Perceived Threat Severity -> Protection Motivation	-0.145	-0.122	0.067	2.158	0.031
Perceived Threat Susceptibility -> Mobile Device Security Usage	0.092	0.087	0.037	2.498	0.013
Perceived Threat Susceptibility -> Protection Motivation	0.178	0.168	0.070	2.554	0.011
Protection Motivation -> Mobile Device Security Usage	0.515	0.519	0.046	11.077	0.000
Response Efficacy -> Mobile Device Security Usage	0.068	0.071	0.030	2.255	0.025
Response Efficacy -> Protection Motivation	0.132	0.135	0.052	2.538	0.011

## References

- Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. *Action Control*, 11-39. Springer, Berlin, Heidelberg.
- 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.
- Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security*, 42, 56-65.
- Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., ... & Agarwal, Y. (2015, April). Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. *In Proceedings of the 33rd annual ACM conference on human factor in computing systems '15*, Seoul, Republic of South Korea, 787-796.
- Amiri, I. (2017). *The efficacy of perceived big data security, trust, perceived leadership competency, information sensitivity, privacy concern and job reward on disclosing personal security information online*. Nova University. Retrieved from ProQuest Dissertations and Theses, UMI Number: 10744475.
- Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3), 613-643.
- Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304-312.
- Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, 84(2), 191-215.
- Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist*, 37(2), 122-147.
- Bandura, A. (1986). The explanatory and predictive scope of self-efficacy theory. *Journal of Social and Clinical Psychology*, 4(3), 359-373.
- Bandura, A. (2012). On the functional properties of perceived self-efficacy revisited. *Journal of management*, 38(1), 9-44.
- Baruch, Y., & Holtom, B. C. (2008). Survey response rate levels and trends in organizational research. *Human Relations*, 61(8), 1139-1160.

- Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., & Möller, S. (2011, August). On the need for different security methods on mobile phones. *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Service '11*, Stockholm, Sweden, 465-473.
- Block, L. G., & Keller, P. A. (1995). When to accentuate the negative: The effects of perceived efficacy and message framing on intentions to perform a health-related behavior. *Journal of marketing research*, 192-203.
- Breitinger, F., & Nickel, C. (2010). User Survey on Phone Security and Usage. *BIOSIG*, 139-144.
- Byrne, B. M. (2001). *Structural equation modeling with AMOS*. Mahwah: Lawrence Erlbaum Associates.
- Bolkan, S., & Goodboy, A. K. (2016). Rhetorical dissent as an adaptive response to Classroom problems: A test of protection motivation theory. *Communication Education*, 65(1), 24-43.
- Boruff, J. T., & Storie, D. (2014). Mobile devices in medicine: a survey of how medical students, residents, and faculty use smartphones and other mobile devices to find information. *Journal of the Medical Library Association*, 102(1), 22.
- Boss, S. (2007). *Control, perceived risk and information security precautions: External and internal motivations for security behavior*. Ph.D. dissertation. Retrieved from Dissertations & Theses: Full Text. (Publication No. AAT 3284534)
- Boss, S., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4), 837-864.
- Burns, B. R., (2000). *Introduction to research methods*. 4ed. Australia: Sage Publications Limited.
- 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.
- Cao, Z. J., Chen, Y., & Wang, S. M. (2014). Health belief model-based evaluation of school health education programme for injury prevention among high school students in the community context. *BioMedical Central Public Health*, 14(26), 1-8.
- Chan, M., Woon, I., & Kankanhalli, A. (2006). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, 1, 18-41.

- Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research*, 295(2), 295-336.
- Chou, H. L., & Chou, C. (2016). An analysis of multiple factors relating to teachers' Problematic information security behavior. *Computers in Human Behavior*, 65, 334-345.
- Chou, H. L., & Sun, J. C. Y. (2017). The moderating roles of gender and social norms on the relationship between protection motivation and risky online behavior among in-service teachers. *Computers & Education*, 112, 83-96.
- Claar, C. L. (2011). *The adoption of computer security: An analysis of home personal computer user behavior using the health belief model*. Utah State University. Retrieved from ProQuest Dissertations and Theses, UMI Number: 3449480.
- Claar, C. L., & Johnson, J. (2010). Analyzing the adoption of computer security utilizing the Health Belief Model. *Issues in Information Systems*, 4(1), 286-291.
- Claar, C. L., & Johnson, J. (2012). Analyzing home PC security adoption behavior. *Journal Of Computer Information Systems*, 52(4), 20-29.
- Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database for Advances in Information Systems*, 45(4), 51-71.
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32, 90-101.
- Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the choicepoint and TJX data breaches. *MIS Quarterly*, 33(4) 673-687.
- 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.
- Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35(8), 982-1003.



- Diamantopoulos, A., & Winklhofer, H. M. (2001). Index construction with formative indicators: An alternative to scale development. *Journal of marketing research*, 38(2), 269-277.
- Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, 8(7), 23.
- Edwards, K. (2015). *Examining the security awareness, information privacy, and the security behaviors of home computer users*. Nova University. Retrieved from ProQuest Dissertations and Theses, UMI Number: 10029813.
- Ellis, T., & 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.
- Fenu, G., & Pau, P. L. (2015). An analysis of features and tendencies in mobile banking apps. *Procedia Computer Science*, 56, 26-33.
- 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.
- Flores, R. W., & Ekstedt M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers Security*, 59, 26-44.
- 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.
- Garson, G. (2016). *Partial least square: Regression and structural equation models*. Asheboro: Statistical Publishing Associates.
- 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.
- 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.

- Gefen, D., Straub, D., & Boudreau, M. (2000). Structural equation modeling techniques and regression: Guidelines for research practice. *Communications of AIS*, 7(7), 1-78.
- Gray, P., & Hovav, A. (2014). Using scenarios to understand the frontiers of IS. *Information Systems Frontiers*, 16(3), 337-345.
- 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.
- Hair J.F., Anderson R., Tatham R., & Black W. (1995). *Multivariate data analysis with readings*. Upper Saddle River: NJ, Prentice-Hall Inc.
- 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., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing theory and Practice*, 19(2), 139-152.
- Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the academy of marketing science*, 40(3), 414-433.
- Hair, J.F., Hult G.T.M., Ringle, C.M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Thousand Oaks, CA: Sage.
- Hardin, A. M., Chang, J. C.-J. & Fuller, M. A. (2008) Formative vs. reflective measurement: Comment on Marakas, Johnson, and Clay (2007). *Journal of the Association for Information Systems*, 9, 519–534.
- 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.
- He, W. (2013). A survey of security risks of mobile social media through blog mining and an extensive literature search. *Information Management & Computer Security*, 21(5), 381-400.
- He, D., Chan, S., & Guizani, M. (2015). User privacy and data trustworthiness in mobile crowd sensing. *IEEE Wireless Communications*, 22(1), 28-34.
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115-135.

- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for Security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106-125.
- Houston, J., & Tran, A. (2001). A survey of tax evasion using the randomized response technique. *Advances in Taxation*, 69-94.
- Hsu, M.-H. & Chiu, C.-m. (2004) Internet self-efficacy and electronic service acceptance. *Decision Support Systems*, 38, 369–381.
- Hu, L.T., & Bentler, P.M. (1998). Fit Indices in covariance structure modeling: Sensitivity to under parameterized model misspecification. *Psychological Methods*, 3, 424-453.
- Huffman, A. H., Whetten, J., & Huffman, W. H. (2013). Using technology in higher education: the influence of gender roles on technology self-efficacy. *Computers in Human Behavior*, 29(4), 1779–1786.
- Janis, I. L. (1967). Effects of fear arousal on attitude change: Recent developments in theory and experimental research. *Advances in Experimental Social Psychology*, 166-225.
- 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.
- Junglas, I. A., Johnson, N. A., & Spitzmüller, 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.
- 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.
- Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, 71(12), 1163-1173.
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122-134.
- Kuznekoff, J. H., & Titsworth, S. (2013). The impact of mobile phone usage on student learning. *Communication Education*, 62(3), 233-252.

- LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM*, 51(3), 71-76.
- Leavitt, N. (2011). Mobile security: Finally a serious problem? *Computer*, 44(6), 11-14.
- Lebek, B., Degirmenci, K., & Breitner, M. H. (2013, August). Investigating the influence of security, privacy, and legal concerns on employees' intention to use BYOD mobile devices. *Proceedings of the Nineteenth Americas Conference on Information Systems '13*, Chicago, Illinois, 15-17.
- Lee Jr, J., Warkentin, M., Crossler, R. E., & Otondo, R. F. (2017). Implications of monitoring mechanisms on bring your own device adoption. *Journal of Computer Information Systems*, 57(4), 309-318.
- Lee, W., Fan, W., Miller, M., Stolfo, S. J., & Zadok, E. (2002). Toward cost-sensitive modeling for intrusion detection and response. *Journal of Computer Security*, 10(1-2), 5-22.
- Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, 18(2), 177-187.
- Levy, Y. (2003). A study of learner's perceived value and satisfaction for implied effectiveness of online learning systems. *Dissertation Abstracts International*, A65(03), 1014. (UMI No. AAT 3126765).
- Levy, Y. (2006). *Assessing the value of e-learning systems*. Hershey, PA: Information Science Publishing.
- Levy, Y. (2006a). *Assessing the value of e-learning systems*. Hershey, PA: Information Science Publishing.
- Levy, Y. (2008). An empirical development of critical value factors (CVF) of online learning activities: An application of activity theory and cognitive value theory. *Computers & Education*, 51(4), 1664-1675.
- Lewis-Beck, M., & Liao, T. F. (2014). The SAGE Encyclopedia of Social Science Research Methods. *Sage Research Methods*, 156-178.
- Li, Q., & Clark, G. (2013). Mobile security: A look ahead. *IEEE Security & Privacy*, 11(1), 78-81.
- Longfellow, H. (1851). The ladder of St. Augustine. *London Journal*, 13(332), 286-286.

- 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.
- Martin, F., & Ertzberger, J. (2013). Here and now mobile learning: An experimental study on The use of mobile technology. *Computers & Education*, 68, 76-85.
- Marakas, G.M., Yi, M.Y. & Johnson, R.D. (1998) The multilevel and multifaceted character of computer self-efficacy: toward clarification of the construct and an integrative framework for research. *Information Systems Research*, 9, 126–163.
- Mertler, C. A., & Vannatta, R. A. (2001). *Advanced and multivariate statistical methods: Practical application and interpretation*. Los Angeles, CA: Pyrczak Publishing.
- Mertler, C. A., & Vannatta, R. A. (2010). *Advanced and multivariate statistical methods*. Glendale, CA: Pyrczak.
- Mertler, C., & Vannatta, R. (2013). *Advanced and multivariate statistical methods: Practical application and interpretation* (5th ed.). Glendale, CA: Pyrczak Publishing.
- Mertler, C. A., & Reinhart, R. V. (2017). *Advanced and multivariate statistical methods: Practical application and interpretation* (6th ed.). New York, NY: Routledge.
- Milne, S., Sheeran, P., and Orbell, S. (2000). Prediction and ntervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, 30(1), 106-143.
- Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, 34, 47-66.
- Neuwirth, K., Dunwoody, S., & Griffin, R. J. (2000). Protection motivation and risk Communication. *Risk Analysis*, 20(5), 721-734.
- Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). *Studying users' computer security behavior: A health belief perspective*. *Decision Support Systems*, 46(4), 815-825.
- Ögütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, 56, 83-93.
- Oberheide, J., & Jahanian, F. (2010, February). When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments. *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications '10*, Annapolis, Maryland, 43-48.

- 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.
- O'Neill, M. (2014). The Internet of things: Do more devices mean more risks? *Computer Fraud & Security*, 1, 16–17.
- Ozturk, A. B., Bilgihan, A., Nusair, K., & Okumus, F. (2016). What keeps the mobile hotel booking users loyal? Investigating the roles of self-efficacy, compatibility, perceived ease of use, and perceived convenience. *International Journal of Information Management*, 36(6), 1350-1359.
- Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security*, 31(5), 673-680.
- Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Which factors explain employees' adherence to information security policies? An empirical study. *Proceedings of Pacific Asia Conference on Information Systems (PACIS) '07*, Auckland, New Zealand.
- Palardy, N., Greening, L., Ott, J., Dolderby, A., & Atchinson J. (1998). Adolescents' health attitudes and adherence to treatment for insulin dependent diabetes mellitus. *Developmental and Behavioral Pediatrics*, 19(1), 31–37.
- Peter, J. P. (1981). Construct validity: A review of basic issues and marketing practices. *Journal of Marketing Research*, 133-145.
- 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.
- Posey, C., Roberts, T. L., Lowry, B. P., Courtney, J., & Bennett, J. R. (2011). Motivating the insider to protect organizational information assets: Evidence from protection Motivation theory and rival explanations. *Proceedings of the Dewald Roode Workshop in Information Systems Security '11*, Blacksburg, Virginia, 1–51.
- Post, G.V. and Kagan, A. (2007) Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security*, 26(3), 229–237.
- Rea, L. M & Parker, R. A. (2014). *Designing and conducting survey research: A comprehensive guide*. California: John Wiley & Sons.
- Rippetoe, P. A., & 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, 596–604.

- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, 91(1), 93-114.
- 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.
- Rogelberg, S. & Stanton, J. (2007). Understanding and dealing with organizational survey nonresponse. *Organizational Research Methods*, 10, 195–209.
- 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.
- 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*. West Sussex, United Kingdom: John Wiley & Sons Ltd.
- Sekaran, U., & Bougie, R. (2013). *Research methods for business: A skill building approach*. New Jersey: John Willey and Sons.
- Sheeran, P., & Orbell, S. (1996). How confidently can we infer health beliefs from questionnaire responses? *Psychology & Health*, 11(2), 273-290.
- Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, 48, 199-207.
- Siponen, M., Pahlila, S., & Mahmood, M. A. (2010). *Compliance with information security policies: An empirical investigation*. *Computer*, 43(2), 64-71.
- Skulmoski, G., Hartman, F., & Krahn, J. (2007). The Delphi method for graduate research. *Journal of Information Technology Education: Research*, 6(1), 1-21.
- Slusky, L., & Partow-Navid, P. (2012). Students information security practices and awareness. *Journal of Information Privacy & Security*, 8(4), 3–26.
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, 13(2), 147-169.

- Sumsion T. (1998). The Delphi technique: an adaptive research tool. *British Journal of Occupational Therapy*, 61(4), 153-156.
- Thompson, N., Ravindran, R. & Nicosia, S. (2015). Government data does not mean data governance: lessons learned from a public-sector application audit. *Government Information Quarterly*, 32, 316-322.
- Trochim, W. M. K. & Donnelly, J. P. (2008). *The research methods knowledge base* (3rd ed.). Mason, OH: Atomic Dog.
- Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, 59, 138-150.
- 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, January). Understanding user's behaviors in coping with security threat of mobile devices loss and theft. In *System Science (HICSS) Forty-Fifth Hawaii International Conference '12*, Honolulu, Hawaii, 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.
- Tyler, J. (2016). Don't be your own worst enemy: Protecting your organisation from inside threats. *Computer Fraud & Security*, 2016(8), 19-20.
- Van Bruggen, D., Liu, S., Kajzer, M., Striegel, A., Crowell, C. R., & D'Arcy, J. (2013, July). Modifying smartphone user locking behavior. In *Proceedings of the Ninth Symposium on Usable Privacy and Security '13*, Newcastle, United Kingdom, 1-14.
- 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.
- Wang, Y.-S., Lin, H.-H. & Luarn, P. (2006). Predicting consumer intention to use mobile service. *Information Systems Journal*, 16, 157-179.
- 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., Johnston, A.C., Walden, E., and Straub, D.W. (2016). Neural Correlates of Protection motivation for secure IT Behaviors: An fMRI examination. *Journal of the Association for Information Systems*, 17(3), 194.
- Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, 18(2), 101-105.
- 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.
- White, B., (2000). *Dissertation skills: For business and management students*. London: Continuum.
- Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS quarterly*, 37(1), 1-20.
- Witte, K. (1996). Predicting Risk Behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication*, 1(4), 317-342.
- Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior*, 27(5), 591-615.
- Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers In Human Behavior*, 24(6), 2799-2816.
- Wright, K. B. (2005). Researching Internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services. *Journal of Computer-Mediated Communication*, 10(3), 1034.
- Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. *Information Technology & People*, 26(4), 401-419.
- Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. *Computers & Security*, 55, 81-99.