NSU Florida
NOVA SOUTHEASTERN UNIVERSITY

Nova Southeastern University
NSUWorks

CEC Theses and Dissertations

College of Engineering and Computing

2016

Empirical Analysis of Socio-Cognitive Factors Affecting Security Behaviors and Practices of Smartphone Users

Joseph P. Simpson
Nova Southeastern University, js3185@nova.edu

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

Part of the Databases and Information Systems Commons, Information Security Commons, Science and Technology Studies Commons, and the Social Media Commons

Share Feedback About This Item

NSUWorks Citation

Joseph P. Simpson. 2016. *Empirical Analysis of Socio-Cognitive Factors Affecting Security Behaviors and Practices of Smartphone Users.* Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (951) https://nsuworks.nova.edu/gscis_etd/951.

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.

Empirical Analysis of Socio-Cognitive Factors Affecting Security Behaviors and Practices of Smartphone Users

by

Joseph P. Simpson

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

2016

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

_____ _____

Maxine S. Cohen, Ph.D. Date
Chairperson of Dissertation Committee

_____ _____

Yair Levy, Ph.D. Date
Dissertation Committee Member

_____ _____

Ling Wang, Ph.D. Date
Dissertation Committee Member

Approved:

_____ _____

Amon B. Seagull, Ph.D. Date
Interim Dean, College of Engineering and Computing

SIGNED ORIGINAL ON FILE AT NSU

College of Engineering and Computing
Nova Southeastern University

2016

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial

Fulfillment of the Requirements for the Degree of Doctor of Philosophy

An Empirical Analysis of Socio-Cognitive Factors Affecting Security Behaviors of Smartphone Users

by
Joseph P. Simpson

March 2016

The overall security posture of information systems (IS) depends on the behaviors of the IS users. Several studies have shown that users are the greatest vulnerability to IS security. The proliferation of smartphones is introducing an entirely new set of risks, threats, and vulnerabilities. Smartphone devices amplify this data exposure problem by enabling instantaneous transmission and storage of personally identifiable information (PII) by smartphone users, which is becoming a major security risk. Moreover, companies are also capitalizing on the availability and powerful computing capabilities of these smartphone devices and developing a bring-your-own-device (BYOD) program, which makes companies susceptible to divulgence of organizational proprietary information and sensitive customer information. In addition to users being the greatest risk to IS security, several studies have shown that many people do not implement even the most basic security countermeasures on their smartphones. The lack of security countermeasures implementation, risky user behavior, and the amount of sensitive information stored and transmitted on smartphones is becoming an ever-increasing problem.

A literature review revealed a significant gap in literature pertaining to smartphone security. This study identified six socio-cognitive factors from the domain of traditional computer security which have shown to have an impact on user security behaviors and practices. The six factors this study identified and analyzed are mobile information security self-efficacy, institutional trust, party trust, and awareness of smartphone risks, threats, and vulnerabilities and their influence on smartphone security practices and behaviors. The analysis done in this research was confirmatory factor analysis (CFA) – structural equation modeling (SEM). The goal of this study was to cross-validate previously validated factors within the context of traditional computer security and assess their applicability in the context of smartphone security. Additionally, this study assessed the influential significance of these factors on the security behaviors and practices of smartphone users.

This study used a Web-based survey and was distributed to approximately 539 users through Facebook® and LinkedIn® social media outlets which resulted in 275 responses for a 51% response rate. After pre-analysis data screening was completed, there were a total of 19 responses that had to be eliminated due to unengaged responses and outliers leaving 256 responses left to analyze. The results of the analysis found that vulnerability awareness, threat awareness, and risk awareness are interrelated to one another which all in turn had significance in predicting self-efficacy, security practices, and behaviors. This intricate relationship revealed in this study indicates that a user has to have an increased awareness in all three categories of awareness before they can fully understand how to protect themselves. Having an increased awareness in one category does not impact the overall security posture of the user and that risk, threat, and vulnerability awareness all work together. Another interesting find was that as risk awareness increased the less the smartphone users protected themselves. This finding warrants additional research to investigate why the user is more averse to risk, and willing to accept the risk, despite their increased awareness. Finally, institutional trust and party trust was found not to have any significance on any of the factors.

These findings should give smartphone users and organizations insight into specific areas to focus on in minimizing inappropriate security behaviors and practices of smartphone users. More specifically, users and organizations need to focus on educating users on all three factors of threats, risks, and vulnerabilities in order for there to have any impact on increasing self-efficacy and reducing inappropriate security behaviors and practices.

Acknowledgements

This dissertation journey could not have been possible without the help, love, and sacrifices of my loving family. First, I would like to thank my lovely and beautiful wife Julie for not only the encouragement, but for the sacrifices you made in picking up the slack while I pursued my dream. I would also like to thank you for the countless hours you devoted to proof reading and editing all the papers I had to do. Without you, none of this would have been possible.

I would also like to say thank you to my three beautiful children, Isabelle, Hunter, and Colton. Thank you for your understanding and patience while daddy did his homework. I hope I have instilled in you that hard work and dedication will pay off in the end. I have a lot of time to make up to you three, so now it is time to have fun!

I would also like to thank my committee chair, Dr. Maxine Cohen. Your patience, guidance, and unwavering support were instrumental in keeping me on track. You were always there with answers to my sometimes outlandish thoughts and questions. Thank you for your mentorship.

I would also like to thank my dissertation committee members, Drs. Yair Levy and Ling Wang, for their constructive criticism, valuable suggestions, and insightful recommendations. Dr. Levy, thank you for the extra attention you have given me in my ramblings about the statistical analysis. Your statistical analysis guidance was paramount in me completing this research. This would not have been a successful endeavor if I had not had such a great committee.

Table of Contents

Approval Signature Page ii
Abstract iii
Acknowledgments iv
List of Figures ix
List of Tables x

Chapters

Introduction 1
- Background 1
- Problem Statement 2
- Dissertation Goal 4
- Research Question 5
- Relevance and Significance 6
- Barriers and Issues 8
- Assumptions, Limitations, and Delimitations 9
  - Assumptions 9
  - Limitations 10
  - Delimitations 11
- Definition of Terms 11
- Summary 13

Review of the Literature 14
- Introduction 14
- Background 14
- Self-Efficacy 19
- Awareness of Risks, Threats, and Vulnerabilities 23
- Trust 31
- Security Practices and Behaviors 36
- Summary 40

Methodology 42
- Introduction 42
- Approach 42
- Propositions 43
- Instrument Development 44
  - Mobile Infosec Self-efficacy 44
  - Vulnerability, Threat, and Risk Awareness 44
  - Institutional and Party Trust 44
  - Security Practices and Behaviors 45

Expert Panel 45
Reliability 46
Validity 47
Internal Validity 47
External validity 47
Instrument validity 47
Population and Sample 48
Pre-Analysis Data Screening 49
Data Analysis 49
Resources 50
Summary 50

Results 51
Introduction 51
Survey Analysis 51
Expert Panel 52
Survey Responses 52
Preliminary Analyses 52
Missing Data 53
Response Set 53
Outliers 53
Normality 54
Multicollinearity 54
Descriptives 57
Confirmatory Factor Analysis 59
Reliability and Validity 61
Model Respecification 62
Structural Equation Modeling 64
Proposition Testing 68
Summary 70

Conclusions, Implications, Recommendations, and Summary 72
Introduction 72
Conclusions 72
Limitations 77
Implications 78
Recommendations 82
Summary 83

Appendix

A. Preliminary Survey Instrument 87
B. Email to expert panel 91
C. Final Survey Instrument 92
D. Participant Recruitment Post 98
E. IRB Approval 99
F. Initial CFA Model with Estimation 100

G. Modified CFA Model with Estimation 101
H. Initial SEM Model with Estimation 102
I. Direct Effect SEM Model with Estimation 103
J. Final SEM Model with Estimation 104

References 105

List of Figures

Figures

1. Conceptual Model for Factors Affecting Smartphone User Security 5
2. Theoretical Framework 43
3. Research model 43
4. Initial SEM Results 66
5. Final SEM Results 68

List of Tables

Tables

1. Pearson Coefficient 55
2. Mobile InfoSec Self-Efficacy VIF 55
3. Risk Awareness VIF 56
4. Threat Awareness VIF 56
5. Vulnerability Awareness VIF 56
6. Descriptives Table 57
7. Security Practices and Behaviors Descriptive Statistics 58
8. Overall Fit Indices for Initial CFA Model 61
9. Reliability and Validity Thresholds 61
10. Reliability and Validity Table with Square Root AVE on Diagonal 62
11. Overall Fit Indices for Modified CFA Model 63
12. Initial SEM Goodness of Fit Indices 65
13. Initial SEM Regression Weights and Path Coefficients (β) 65
14. Final SEM Goodness-of-Fit Indices 67
15. Final SEM Regression Weights and Path Coefficients (β) 67
16. Summary Proposition Outcome 70

Chapter 1

Introduction

Background

Security risks are inherently present in all information systems (IS). Every Internet user is susceptible to IS risks. Moreover, users have a tendency to exhibit poor Internet security practices which puts their IS at risk of compromise (Anderson, Durbin, & Salinger, 2008; Ramim & Levy, 2006; Stanton, Stram, Mastrangelo, & Jolton, 2005). One of the most significant risky behaviors by Internet users is not implementing appropriate security measures to protect themselves from cyber attacks which could result in divulging of personally identifiable information (PII) or other potentially embarrassing personal information. Many users lack the awareness and understanding that sensitive information exposure has a devastating impact (Blackmon, Kitajima, & Polson, 2003). Since many users store PII and other sensitive information on their computing devices, their devices are prime targets for cyber attacks, and users can unknowingly divulge PII due to lack of protection.

The proliferation of smartphone devices amplifies the data exposure problem by enabling instantaneous transmission and storage of PII by smartphone users, which is becoming a major security risk. As Van Bruggen et al. (2013) stated, “Unfortunately, the expanding availability and usage of mobile devices brings an increased security risk” (p. 1). However, smartphone security risks are not limited to exposure of PII.

Many organizations are trying to capitalize on the popularity of smartphone devices by adopting a bring-your-own-device (BYOD) concept. This BYOD concept is perpetuating the problem of sensitive data exposure by allowing employees to use their personally owned, often unprotected, smartphones to perform work-related transactions. As the lines between personal and business use continue to become increasingly blurred, the transmission and storage of organizational proprietary information is also at risk (Landman, 2012). Several studies have indicated that smartphone devices are leading to significant organizational and personal IS risks, which can result in divulgence of both PII and organizational proprietary information (hereinafter, collectively referred to as sensitive information) (Distefano, Grillo, Lentini, & Italiano, 2010; Zhou, Zhang, Jiang, & Freeh, 2011).

Problem Statement

The research problem that this study addressed is inappropriate security behaviors and practices by smartphone users are leading to the exposure and compromise of sensitive information (Dorflinger, Voth, Kramer, & Fromm, 2010; Shaw, Chen, Harris, & Huang, 2009). The proliferation of smartphone devices is introducing new IS risks, which if not properly mitigated through appropriate security practices and behaviors, can result in the exposure of sensitive data (Anderson et al., 2008; Chin, Felt, Sekar, & Wagner, 2012; Furnell, Tsaganidi, & Phippen, 2008; Jones & Heinrichs, 2012; Landman, 2010; Van Bruggen et al., 2013).

Although many users are fully aware of the threats to IS security, such as viruses and malware, smartphones introduce unique risks and vulnerabilities that can be exploited by threats specific to smartphones (Husted, Saïdi, & Gehani, 2011; Jeon, Kim,

Lee, & Won, 2011). Moreover, traditional computer security mechanisms are generally not available, nor applicable, to smartphones (Landman, 2010). These unique risks, threats, and vulnerabilities make smartphones ideal targets for exploitation which can result in release of sensitive information (Botha, Furnell, & Clarke, 2009; Jeon et al., 2011).

Prior research on IS security behaviors has mainly focused on the analysis of the specific behavior (Stanton et al., 2005). However, very few studies have been conducted that focused on the socio-cognitive behaviors that affect IS user security practices and security behaviors (Huang, Rau, & Salvendy, 2010). Moreover, although an abundance of IS security focused literature exists; the literature is mainly rooted in the domain of traditional computing devices (see Albrechtsen, 2007; Botha et al., 2009; Furnell, 2008; Huang, Rau, & Salvendy, 2010; Kruger & Kearney, 2006; Rhee et al., 2009; Stanton et al., 2005).

Several traditional computing studies have shown that there are specific factors that have influenced the lack of security tool adoption and overall security behaviors of computer users. For example, Crossler and Belanger (2006) determined that self-efficacy was highly correlated to the adoption rate of security applications. Rhee, Kim, and Ryu (2009), later reaffirmed that self-efficacy had a significant influence on not only security practices, but also on overall security behaviors. Additionally, Huang et al. (2010) determined that awareness of threats, risks, and vulnerabilities are significant in determining the level of self-reported self-efficacy. Chin et al. (2012) and Furnell et al. (2008) discovered that trust in security applications was a significant factor in the adoption rate of the security applications. Finally, Allam, Flowerday, and Flowerday

(2014) noted a dichotomous view between computer users and organizations on exactly whose responsibility it was to secure the computing devices. Furnell et al. (2008) discovered that computer users believe it is the responsibility of the software manufactures to secure the computer devices. In other words, the users surveyed in the Furnell et al. (2008) study believed the operating system and software programs should be developed vulnerability free. Therefore, the user feels they should not have to take any precautions in protecting their data.

A literature review has revealed a gap in the literature between traditional computer and smartphone security. Most of the available literature about smartphone security primarily focused on specific malware and hardware attacks and how these attacks exploit specific smartphone security architectures (Mylonas et al., 2013). Very little research was found that focuses on smartphone user security behaviors and practices, which is considered relatively new in the field of research (Mylonas et al., 2013; Park & Chen, 2007). Therefore, this study began to address this gap and examined the factors that have shown to have an influence on security behaviors and practices in the traditional computing domain, and tested their applicability and validity in the domain of smartphones through confirmatory factor analysis (CFA)-structural equation modeling (SEM).

Dissertation Goal

The main goal of this study was to explore the validity and reliability for measures of the following constructs: mobile information security (InfoSec) self-efficacy (MISE), vulnerability awareness (VA), threat awareness (TA), risk awareness (RA), party trust (PT), institutional trust (IT), security practices (SP), and security behaviors (SB).

Users ultimately determine the overall security posture of an IS (Jones & Heinrichs, 2012; Rhee et al., 2009; Tsohou, Kokolakis, Karyda, & Kiountouzis, 2014). Furthermore, Furnell et al. (2008) stated, "users have significant issues with their online behaviors, carrying out risky online practices" (p. 235). Therefore, this study investigated socio-cognitive factors that influence smartphone users' security practices. Figure 1 depicts the proposed conceptual framework for this study. The intended result of this study was to empirically assess the validity and reliability of previously validated factors embedded within the traditional computing domain. These factors may be used by researchers and practitioners to determine specific areas that require increased attention in order to improve the positive security practices and behaviors of smartphone users.

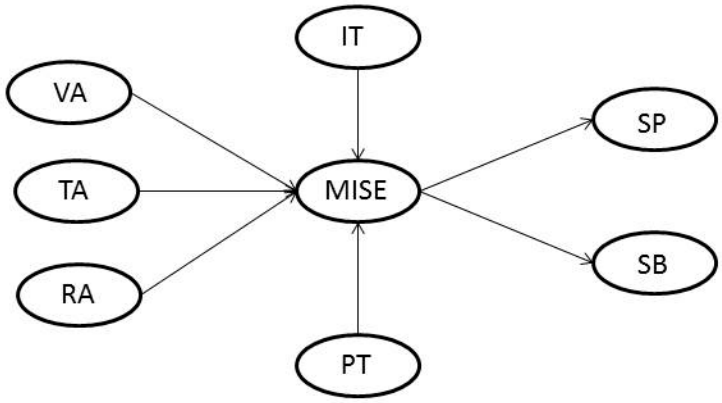


Figure 1: Conceptual Model for Factors Affecting Smartphone User Security

Research Question

This study examined socio-cognitive factors that are believed to affect the overall security practices and behaviors by smartphone users. This study is grounded in social-cognitive theory (SCT) (Bandura, 1977; Compeau & Higgins, 1995) and IS literature (Ben-Asher et al., 2011; Botha et al., 2009; Chin et al., 2012; Crossler & Bélanger, 2006; Furnell, 2008; Huang et al., 2010; Rhee et al., 2009; Shaw et al., 2009). The main

research question this study addressed was: Do the factors of Mobile InfoSec self-efficacy, vulnerability awareness, threat awareness, risk awareness, institutional trust, and party trust demonstrate high reliability and validity in determining smartphone users' security practices and security behaviors? The purpose of this study was to conduct confirmatory factor analysis (CFA) to test the validity, reliability, and model fit of these factors as well as conduct structural equation modeling (SEM) analysis to analyze the relationships between the factors within the domain of smartphone security.

Relevance and Significance

Computer security has been around for decades and has been studied since as early as the 1970s (Saltzer & Schroeder, 1975). However, as new innovative computing products come to market, research on these devices typically lags behind (Park & Chen, 2007). A literature review on smartphone security revealed very little literature available on the subject, especially concerning user behaviors as it pertains to smartphone user security behaviors and practices. This can be attributed to the fact that smartphone security is still considered a relatively new subject in the field of IS security (Mylonas et al., 2013). The few studies that were discovered during literature review usually focused on a single, isolated factor such as perceived risk or were focused on hardware/software exploits. Multiple factors need to be considered when investigating the causes of user behaviors (Huang et al., 2010). Therefore, this study attempted to bridge this apparent gap in smartphone security literature.

The need for this work is demonstrated by Furnell (2008), Furnell et al. (2008), Huang et al. (2010), Jones and Heinrichs (2012), Landman (2010), and Rhee et al. (2009). Jones and Heinrichs argued that the proliferation of smartphones is increasing the

overall risk of data breaches. Landman noted that as organizations continue to increase their reliance on smartphones, the storage and transmission rate of sensitive data will also continue to increase. Furnell et al. argued that rapid technological advancements of devices are far outpacing the available security, thereby increasing the risks of sensitive data exposure. Furthermore, Furnell stated "although a new generation of 'digital natives' is emerging that are more IT-literate, this by no means implies that they will be more naturally security-aware" (p. 9). Rhee et al. argued that there are social-cognitive factors, such as self-efficacy, security consciousness, and a person's cognitive ability to control threats and risks all play a significant role in the adoption of security applications and behaviors and requires further investigation. Finally, Huang et al. noted that studying risk by itself is not sufficient in trying to determine the security practices of users and that other factors need to be investigated.

This study sought to gain a deeper understanding into the factors that influence smartphone user security practices and security behaviors. As previously described, the bulk of IS security research has been mainly conducted in the traditional computing domain. Unfortunately, information security and protection of sensitive data continues to be a problem (Shaw et al., 2009), and several studies noted that users are typically the problem in IS security (Chin et al., 2012; Furnell, 2008; Furnell et al., 2007, 2008; Kruger & Kearney, 2006; Ramim & Levy, 2006; Rhee et al., 2009; Van Bruggen et al., 2013). As information security and protection of data continue to be a problem, coupled with the fact that users continue to be the main problem, smartphones are only compounding this problem.

This study is significant because it will advance smartphone security research and facilitate an increase in the body of knowledge regarding the factors that influence smartphone user security behaviors and practices. Understanding user behaviors is critical in IS security (Hazari, Hargrave, & Clenney, 2008). As previously noted, current research has typically only studied perceived risks and has failed to explore other factors that influence IS security behaviors, such as perceived threats and perceived vulnerabilities and has typically focused on traditional computing (Huang et al., 2010). Thus, to address this gap, this study explored additional factors that influence smartphone user behaviors and practices.

This study also has practical implications for organizations that allow BYOD. The study statistically assessed factors identified in traditional IS security literature review and tested them for reliability and validity in the context of smartphones. Now completed, organizations may use the results to assess their smartphone information security plans and identify areas of improvement or non-applicability.

Barriers and Issues

The goal of this research was to determine the impacts of Vulnerability Awareness (VA), Risk Awareness (RA), Threat Awareness (TA), Mobile InfoSec Self-Efficacy (MISE), Institutional Trust (IT), and Party Trust (PT) on smartphone user's Security Practices (SP) and Security Behaviors (SB). One potential barrier that existed was the number of survey responses required to ensure a sufficient statistical sample to conduct CFA-SEM. A literature review has revealed that there is not a hard and steadfast rule concerning the minimum number of responses in order to conduct CFA-SEM. However, nearly all literature has agreed that N>200 is a sufficient number of minimum

responses to conduct the statistical analysis. The results of the data collection effort netted 275 total responses.

Another potential issue was that users may not be completely honest in their answers due to fear of lack of anonymity. To mitigate this, a disclaimer was posted at the top of the survey to inform the respondents that all users would remain anonymous, their participation was voluntary, and they could have exited the survey at any time. Furthermore, the survey was devoid of any questions that may result in traceability back to the respondent.

Finally, another possible barrier was the length of the survey. Long surveys have shown to lead to non-response issue and early exit from the survey by the respondent (Bogen, 1996; Galesic & Bosnjak, 2009; Herzog & Bachman, 1981). Although most of the constructs were previously validated in prior literature, an expert panel was created to ensure the questions were properly worded, not redundant, and applicable to the study to help mitigate this issue. The results of the data collection showed potential survey length issues since 13 response sets had to be eliminated from the analysis portion in order to avoid skewing the results. The estimated length of the survey was 10 minutes.

Assumptions, Limitations, and Delimitations

Assumptions

1) It was assumed that participants were honest in their responses;
2) It was assumed that the participants either presently used or have previously used a smartphone device;
3) It was assumed that the participants made a valiant effort to complete the survey in its entirety with accurate reflections of their behaviors and/or beliefs.

Limitations

One limitation of this study was that the survey was disseminated through the author's social media outlets (e.g., Facebook® & LinkedIn®). This participant recruitment medium was selected due to the demographic diversity and the amount of potential respondents. Studies have shown that social media sites are an excellent tool for recruiting survey participants (Ramo & Prochaska, 2012; Ta, Forgasz, Leder, & McLeod, 2012). In an unpublished article by Simpson, Nilsen, Levy, and Cohen (2013), Facebook® was used to recruit participants to engage in a similar study which resulted in 240 responses in a little less than 30 days. Thus, using LinkedIn® in addition to Facebook® expanded the prospective participant pool. Between the two social media outlets, there were a total of 539 total available participants. Of these 539, 275 people responded for a response rate of 50.6%. However, it should be noted that some bias may have been introduced through using these social media tools based on the possible assumption of users being technologically savvy merely because they can utilize social media tools.

Additionally, this study was adapted from the domain of traditional computing to test for validity and reliability in the context of smartphones. Therefore, the constructs that were selected for this study had yet to be validated and/or used in the context of smartphones. The purpose of this study was to determine the constructs' applicability to the smartphone context. Therefore, a potential finding may have been that some of the constructs are not valid in the new context.

Delimitations

One of the delimitations of this study was that users may not have been aware of the differences between risks, vulnerabilities, and threats. To address the potential confusion between risks, vulnerabilities, and threats, precise definitions of each were provided from published literature at the beginning of that respective section of the survey.

Definition of Terms

Definitions of key terms used in this document are outlined below:

Computer security is the protection of computing systems against threats to the confidentiality, integrity, and availability of computer systems (Summers, 1997).

Information security is "the protection of personal data against accidental or intentional disclosure to unauthorized persons, or unauthorized modifications or destruction" (Udo, 2001, p. 165).

Information security awareness is "the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organization's data and networks" (Shaw et al., 2009, p. 92).

Institutional trust is the faith a user has that online application stores only distribute software that is safe for use, free from defects, and devoid of malicious code (Mui et al., 2002).

Mobile InfoSec Self-efficacy (MISE) is a person's belief in their own abilities to exercise control over events and actions related to their mobile devices.

Party trust is the faith a user has that a software developer has made the software safe for use, free from defects, and devoid of malicious code (Mui et al., 2002).

Personally identifiable information (PII) is "Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked or linkable to a specified individual" (DoN, 2012).

Proprietary data are "Documents and data that has [sic] been generated by the company to allow it to control and safeguard its competitiveness over other companies" (Proprietary Data, n.d.).

Risk awareness is the amount of awareness a person has pertaining to information security risks (Stanton et al., 2005).

Risky behaviors are defined as inappropriate and destructive behaviors that reduce the overall effectiveness of IS security posture (Stanton et al., 2005).

Security behaviors are the security conscious behaviors and actions that users demonstrate/conduct while using their mobile device (Rhee et al., 2009).

Security practices is the technological aspect that users take (i.e., installing security applications) to protect their mobile device (Rhee et al., 2009).

Self-efficacy is a person's belief in his/her own abilities to exercise control over given events (Ozer & Bandera, 1990).

Sensitive information is both PII and organizational proprietary data.

Smartphone is a high-powered, small-form-factor computing device that blends a rich, hardware-computing platform with that of a traditional specialized cellular phone (Husted et al., 2011).

Threat awareness is the amount of awareness a person has as it pertains to information security threats.

Trust is "the subjective probability which consumers believe that a particular transaction will occur in a manner consistent with their confident expectations" (Chellappa & Pavlou, 2002, p. 360).

Vulnerability awareness is the amount of awareness a person has as it relates to vulnerabilities of his/her mobile devices.

Summary

Information security is an ongoing issue pertaining to safe guarding sensitive information. Several studies have been conducted concerning InfoSec within the domain of traditional computing. However, very little of the research has focused on the socio-cognitive factors associated with the adoption of security by computer users. Moreover, very little research has been done concerning smartphone InfoSec as it relates to smartphone users' security practices and behaviors. Therefore, a model was developed consisting of previously validated constructs from traditional computing to test for applicability and validity in the context of smartphone user security practices and behaviors.

Chapter 2

Review of the Literature

Introduction

The literature review is conducted to provide the theoretical foundation for this study. The literature review revealed there is little relevant literature available on these constructs in the context of smartphones, specifically smartphone user security behaviors and practices. This can be mostly attributed to the fact that this is a relatively new field of study (Mylonas et al., 2013; Park & Chen, 2007). Reviewing and identifying relevant constructs is an imperative part of the literature review (Hart, 1998). The constructs that will be investigated in this study are outlined in the proceding sections.

Background

Computer and information security research has been studied since as early as the 1970s (Saltzer & Schroeder, 1975). However, the invention of the smartphone in the mid-2000s has created new avenues that extend threats to information security by introducing an entirely new set of risks and vulnerabilities. Moreover, these threats continue to increase because of the exponential growth in smartphone usage (Burns & Johnson, 2015; Landman, 2010). Unfortunately, computer and information security has failed to keep pace with the mobile device community, specifically smartphones (Bickford, O'Hare, Baliga, Ganapathy, & Iftode, 2010).

The smartphone is a high-powered, small-form-factor computing device that blends a rich, hardware-computing platform with that of a traditional specialized cellular phone (Husted et al., 2011). Smartphones are not only used for making phone calls, but also taking pictures, updating social media statuses, text messaging, storing contact information, sending/receiving email, banking, and browsing the Internet. These types of usage can not only lead to inadvertent disclosure of sensitive data, but can also exploit embarrassed users via criminal blackmail attempts (Muslukhov, Boshmaf, Kuo, Lester, & Beznosov, 2013).

Additionally, smartphones are relatively inexpensive and rich in application availability from their respective vendor's market place (i.e., Apple, Android, and Windows) making these smartphones highly desirable (Chin et al., 2012). Smartphone popularity has spurred tremendous growth in the development and availability of smartphone applications. Unfortunately, some of these applications are used to access and exploit personal information (Park, Lee, Kim, Cho, & Choi, 2012).

Smartphones are becoming so popular due to their computing power, portability, and relatively cheap prices that they are supplanting traditional computing devices (Chin et al., 2012; Brenner, 2013). According to comScore (2013), as of November 2013, 152.5 million people in the United States own a smartphone. This equates to 63.8 percent of the U.S. population. This increase has created a demand by smartphone users to be able to use their smartphones in the workplace. Many companies have responded to this demand and, as of 2013, it is estimated that 90% of workforce employees use their personal smartphone to conduct work-related transactions (Cisco, 2012).

Due to the computing power of these smartphone devices, many organizations are becoming more reliant on them as well. As such, many organizations have adopted a bring-your-own-device (BYOD) concept. This BYOD concept leads to new IS risks as the lines of mobile device usage between personal and business use become increasingly blurred (Landman, 2012). Studies have shown that these mobile computing devices are leading to significant IS risks to organizations, resulting in identity theft and divulgence of proprietary information (Distefano, Grillo, Lentini, & Italiano, 2010; Zhou, Zhang, Jiang, & Freeh, 2011). Van Bruggen et al. (2013) also indicated that:

> Unfortunately, the expanding availability and usage of mobile devices brings increased security risks. From an organizational perspective, the increased risk is two-fold. First, with many users personally owning a variety of capable mobile devices, considerable pressure emerges from employees to have their organizations embrace Bring Your Own Device (BYOD) policies. Second, the perceived potential for productivity gains offered by capable mobile devices is appealing to the organization but tempered by the risks of exposing sensitive data. (p. 1)

Since smartphones are small hand-held computing devices carried virtually everywhere, they are frequently lost or stolen (Ballagas, Borchers, Rohs, & Sheridan, 2006). For example, it is quite easy for a smartphone user to lay the smartphone down and walk away, leaving the phone behind. A recent survey by Consumer Reports revealed that over 1.4 million smartphones were lost and another 3.1 million stolen in 2013 (Consumer Reports, 2014). That is double the number of phones stolen in 2012. In addition, many of these smartphone devices are often left unsecured, in terms of

authentication mechanisms, and lack appropriate security protection such as anti-virus, anti-malware, and firewall protection (Ben-Asher et al., 2011; Botha, Furnell, & Clarke, 2009; Van Bruggen et al., 2013). The increased popularity and adoption of smartphones and lack of security countermeasures is creating a significant increase in smartphone IS risks. The following study by Symantec Corporation highlights the severity of the threats to information security and poor user practices.

In 2012, Symantec Corporation purposely "lost" 50 smartphones installed with remote activity monitoring software (Haley, 2012). The study found that of the 50 smartphones found by strangers, 96% of the smartphones were accessed and revealed personal and proprietary information intrusion such as pictures, text messages, social networks, and banking information. In other words, upon finding the smartphones, those strangers accessed them with the intent of finding sensitive information stored on the phone.

With the massive amount of smartphones lost each year, specific and special care is needed in securing these devices to avoid exposure, loss, and theft of sensitive data. As Van Bruggen et al. (2013) stated, "The question becomes when, not if, the mobile device will be lost…" (p. 2). This explosion of smartphone popularity is not only leading to significant information security risks, but several studies have shown that many of these risks are due to inappropriate and risky user behaviors.

Several studies have argued that users are typically the weakest link in IS security and continually put themselves at risk by exhibiting precarious Internet behaviors (Anderson, Durbin, & Salinger, 2008; Ramim & Levy, 2006; Stanton, Stram, Mastrangelo, & Jolton, 2005). Furnell et al. (2008) stated, "Users have significant issues

with their online behavior, carrying out risky online practices" (p. 235). It has also been noted that Internet users divulging PII or other sensitive data is due to their risky security practices (Anderson et al., 2008; Chin et al., 2012). Studies have also specifically noted that users not utilizing security tools, nor exhibiting security conscious behaviors, are of particular importance and are extremely risky (Furnell et al., 2007; Husted et al., 2011; Mylonas et al., 2013). Chipperfield and Furnell (2010) also noted that users are sometimes unwilling to protect themselves, for one reason or another, which ultimately makes smartphone users a prime target for attack. This could be attributable to users fearing they will make a mistake in using the tools, will cause damage to the equipment, or will prove incompetent on using security applications (Shneiderman, 1992). Users are often times not even aware of the susceptibility of attacks on their mobile devices (Furnell, Tsaganidi, & Phippen, 2008).This deficiency of security conscious behavior and absence of security application and tool usage lowers the security hurdles would-be attackers must overcome to gain access to stored data (Anderson et al., 2008; Furnell et al., 2008).

Sensitive data is easily obtainable, whether it be for legitimate or illegitimate reasons (Burns and Johnson, 2015; Nurse, Erola, Goldsmith & Creese, 2015). Okenyi and Owens (2007), as well as Luo et al. (2007), have also noted that sensitive data is not only easily obtainable, but its loss can largely be due to psychological influences by the users. Okenyi and Owens, as well as Luo et al., concluded that policies, procedures, and user education are pivotal in deterring the dissemination of sensitive data caused by psychological factors. Additionally, Workman (2007) stated that the decisions made to provide sensitive data are based on fear, authority, trust, and likeability.

Although there has been increased publicity concerning IS risks, associated threats, and the resultant security breaches, it has done very little to improve the security practices and behaviors of Internet users. The occurrence of identity theft and sensitive information exposure continues to increase at an alarming rate due to users divulging sensitive information (Anderson et al., 2008; Luo, Brody, Seazzu, & Byrd, 2011; Workman, 2007). When users divulge this sensitive information, even under the guise of increased security, or as a requirement for access such as through a Web interface, it can lead to the compromise of sensitive information (Okenyi & Owens, 2007). Moreover, smartphone devices are exacerbating these risks, due to their small-form-factor and ubiquitous nature. Since users carry their smartphone devices with them all the time, it is easy to access unsecured Websites and Wi-Fi and forget about security measures. Therefore, due to the increased risks associated with smartphones, and the lack of research pertaining to the factors that affect inappropriate security behaviors (Teer, Kruk, & Kruk, 2007), further research was warranted to investigate the factors that affect the security practices and behaviors of smartphone users.

Self-Efficacy

Self-efficacy is originally rooted within the social-cognitive theory (SCT) developed by Bandura (1977). The SCT posits that output expectations and self-efficacy are the driving forces that influence behavior (Bandura, 1977; Compeau & Higgins, 1995). Compeau and Higgins (1995) later adopted self-efficacy in the computer domain. They coined the new construct computer self-efficacy (CSE). CSE is defined as “an individual’s perception of his or her ability to use a computer in the accomplishment of a job task” (Compeau & Higgins, 1995, p. 193). CSE has been demonstrated as having

high reliability and validity in the studies of technology acceptance (Agarwal, Sambamurthy, & Stair, 2000; Park & Chen, 2007; Sheng, Pearson, & Crosby, 2003).

CSE is often studied in conjunction with the Technology Acceptance Model (TAM) (Venkatesh & Davis, 1996; Fenech, 1998). Specifically, CSE has proven to have a significant impact on the perceived usefulness and perceived ease of use constructs of the TAM (Dishaw, Strong, & Bandy, 2002). CSE and the TAM, studied together, assist in gaining insight into users' behaviors, perceptions, and attitudes (Chen, Chen, & Yen, 2011). It has been repeatedly proven that CSE is a significant predictor in the adoption of new technologies (Ball, 2008). Ball (2008) discovered that CSE was one of the most important factors in determining user behavioral intention as it related to the acceptance and usage of technology. Several prior studies have indicated that CSE should be included when studying attitude and intention (Ong, Lai, & Wang, 2004; Vijayasarathy, 2004; Yi & Hwang, 2003).

Chen et al. (2011) conducted a study in an attempt to gain deeper insight into smartphone user perceptions about security and their application installation habits. They interviewed 60 participants and studied their willingness to perform certain actions on their smartphones such as mobile banking, online purchasing, and checking health records. They found that people were less willing to conduct those sensitive types of transactions on their smartphones as compared to their laptops. In their findings, they noted that there were misconceptions by the users concerning application security as well as the mobile network infrastructure (e.g., 3G & 4G data network). This finding raises concerns about self-efficacy and security risk awareness. They also discovered that proficiency, efficacy, and finely grained demographics may also be significant factors.

Rhee et al. (2009) stated that very little attention has been given to the socio-cognitive behaviors of users regarding information security. Therefore, Rhee et al. investigated the relationship of information security self-efficacy and the resultant effects on information security, security practices, and motivation to strengthen security posture among computer users. Consistent with other published research articles, Rhee et al. argued that the end-users ultimately determine the overall security posture of computers and associated computer networks. The results of the study found that self-efficacy does in fact play a significant role in researching and explaining information security practices from a socio-cognitive perspective. Specifically, self-efficacy was found to play a positive role in overall security posture, level of concern about security incidents, and user intention to strengthen security posture.

Moreover, Rhee et al. (2009) found that computer experience was a significant determinant in predicting information security self-efficacy. Furnell (2008) noted that inexperience poses a significant risk in security posture. He also argued that lack of awareness on specific threats, vulnerabilities, and risks were due to inexperience. Stanton et al. (2005) also noted that experience played a significant role in adopting good security practices.

Crossler and Bélanger (2006) set out to investigate and determine the effects of CSE on the adoption of security tools through various levels of instruction. Crossler and Bélanger argued that although overall information system attacks and financial losses have decreased, unauthorized access and loss of personally identifiable and proprietary information is still on the rise. They further argued that individual differences affect a person’s use of technology. Therefore, Crossler and Bélanger set out to study the level of

self-reported CSE in relation to the level of security tool adoption. Additionally, Crossler and Bélanger tested, through quasi-experimentation, different information security instruction factors, awareness, training, and education, to test their applicability in the overall adoption rate of security tools as well as their impact on CSE. Crossler and Bélanger ultimately determined that awareness, training, and education did not have a significant impact on CSE or security tool adoption rate. However, the level of self-reported CSE was highly significant in the overall adoption rate of security tool adoption.

A literature review on smartphone self-efficacy has revealed that there is presently a literature gap as compared to the traditional computing domain; more so in regards to self-efficacy pertaining to security behaviors and practices of smartphone users. The majority of the literature that was discovered on smartphone self-efficacy was mainly focused on the adoption of the smartphone device itself (for example, see Keith, Babb, Furner, & Abdullat, 2011; Lee, 2014; Park & Chen, 2007), or the installation of applications from the respective smartphone marketplace for applications.

Self-efficacy has evolved as new innovations have come to market. As previously noted, self-efficacy was discovered by Bandura (1977). Later, self-efficacy was adopted by Compeau and Higgins (1995) and applied to computers. Eastin and Rose (2000) adopted self-efficacy and applied it to the Internet, which they coined the new construct Internet self-efficacy. Therefore, it appears to be a feasible progression of using self-efficacy construct in the context of smartphones. This study adopted self-efficacy in the mobile smartphone environment and titled the construct MISE. MISE was defined as an individual’s perception of his or her ability to protect themselves from attacks pertaining

to their smartphone. This study empirically assessed MISE and its validity and reliability in predicting user security practices and behaviors specific to smartphone devices.

Awareness of Risks, Threats, and Vulnerabilities

Users' lack of information security awareness increases the risk of a malicious attack (Furnell, 2008). Information security awareness is imperative for anyone using the Internet (Shaw et al., 2009; Siponen, 2000). Yet, Bickford et al. (2010) noted users significantly lack information security awareness, specifically when using smartphones. Moreover, a December 2010 report published by the European Network and Information Security Agency (ENISA) stated the main risk to smartphones is lack of user awareness.

A literature review on information security has shown that there is a common agreement that information security awareness is an important component in the overall security posture of an information system (Kruger & Kearny, 2006; Siponen, 2001; Straub & Welke, 1998). As Siponen (2001) noted, however, it is more than just user awareness, rather users have to be aware and commit to the security objectives. Siponen's statement was later reaffirmed by Rezgui and Marks (2008) when they stated information security awareness is the "understanding of IS security and, optimally, committing to it" (p. 242).

Since smartphones are a relatively new technology, users typically lack information security threat awareness (Chin et al., 2012). Additionally, many users are not even aware of the available countermeasures to information security risks (Furnell et al., 2008). Many users, even if aware of the technical solutions available, do not have the knowledge or expertise to configure and use them properly (Furnell, 2008). Kumar, Mohan, and Holowczak (2008) also suggested that there is a relationship between the

lack of awareness of security and the lack of adoption of the technological measures available to them. Unfortunately, as Kruger and Kearny (2006) noted, effective information security "requires a combination of technical and procedural controls to manage information risk" (p. 289).

The nature of smartphone devices (i.e., ubiquitous, small form factor, & high usage) lends itself to not only the risks, threats, and vulnerabilities associated with traditional computing environments, but also those unique to smartphones (Jeon et al., 2011). Numerous studies exist about the technical risks associated with smartphones; for example, privilege escalation attacks (Park et al., 2012), hacking and malware (Landman, 2010), and rootkits, viruses, and worms (Bickford et al., 2010). Many of these same risks exist with traditional computing devices. However, as Bickford et al. noted, smartphone rootkits can access a number of unique interfaces and information that are not normally available on desktop computers, such as the GPS, battery, and voice/messaging, validating that smartphones create uniquely different security risks.

For example, Jeon et al. (2011) identified a smartphone-specific attack called a dialer-attack. A dialer-attack is when malware infects the smartphone, hijacks the dialer function, and dials costly international phone numbers without the smartphone owner's consent (Jeon et al., 2011). A similar threat exists that carries out similar actions, but uses text messaging instead of the dialer. Therefore, technical security precautions need to be implemented to mitigate these technical threats. Examples might include implementation of firewalls, antivirus software, and smartphone authentication measures. However, as Jeon et al. indicated, although there are very different and unique risks, threats, and vulnerabilities pertaining to smartphones, the user is the biggest vulnerability.

Responsibility of securing smartphone devices typically lies with the device owner. Since most smartphone devices are owned by individual users, regardless if they are used for work purposes, the responsibility to protect their sensitive data lies with the user (Allam, Flowerday, & Flowerday, 2014). However, many users do not believe it is their responsibility to protect themselves, which indicates a strong lack of awareness on the importance of users protecting themselves (Allam et al., 2014; Furnell et al., 2008).

Furnell et al. (2007) conducted a study that investigated Internet users' awareness of threats, awareness of security countermeasures, usage of those security countermeasures, and personal protection measures they practiced. They studied 20 Internet users and found that many of the respondents had personally experienced some form of security attack and were aware of the existence of threats. However, many still failed to implement security countermeasures. Their findings also indicated that although many users claimed to be aware of security threats they were often associated with specific activities such as online banking rather than the actual threat, such as phishing, viruses, and malware.

Many users turn to family or friends for assistance, as their ability to find suitable sources of information security protection are limited (Furnell et al., 2008). Furnell et al., (2008) examined Internet users' source of knowledge as it pertains to Internet risks and associated barriers to protection. The study was qualitative in nature and was conducted using interviews of 20 novice Internet users. Novice users were specifically selected for this study as Furnell et al. conducted a previous study in which novice users were underrepresented. The results of the study found that users implement risky online practices, have significant online behavioral issues, and obtain their knowledge from less

than ideal sources. In addition to these results, key findings of this study were that users lack an understanding of specific threats and the available and appropriate safeguards, believe it is not their responsibility to protect themselves, and tend to exhibit a certain level of trust in software providers to provide the protection. Furnell et al. contended that a potential solution is to completely remove the protection decisions from users or to force the users into taking formal responsibility for their own protection. This suggests that the level of self-efficacy is low and may have a correlation to inadequate awareness of information security threats.

Allam et al., (2014) set out to explore the factors that influence the fluctuating levels of information security awareness within business organizations. Allam et al. point out that many organizations are continually adapting a BYOD concept that is perpetuating smartphone information security risks. They argue that this perpetuation is attributable to the constant growth of smartphone usage and acceptance by organizations coupled with the lack of user knowledge or motivation to secure their smartphone. Allam et al. adapted Rasmussen's (1997) awareness model and applied it to the smartphone information security domain. What Allam et al. found was that the managers, employees, and security professionals are competing against each other. Security professionals want the phone completely locked down. Managers want the least of amount of hurdles to increase productivity. Users want to reduce their workload by the maximum amount possible. Therefore, Allam et al. proposed a model that identifies an 'optimized state' of smartphone operation that equally balances the needs of security professionals, managers, and the employees. Allam et al. contend that if smartphone use is operated within this

area of ‘optimized state’, information security awareness will increase, which in turn will lead to more positive information security behaviors.

Muslukhov et al., (2013) investigated smartphone users’ perceived risks of unauthorized access of smartphone devices. Specifically, Muslukhov et al. studied perceived risks of unauthorized access by insider threats, such as friends and family, rather than outsider threats as has been the focus of other studies. The study found that users are more concerned with insider threats than outsider threats. Although not addressed in the paper, it can be surmised that this increased fear of insider threats could be attributable to the effects of long term “embarrassment.” The article studied the specific risks that smartphone users feared the most and found that unauthorized access to personal photos and videos was most feared. Consistent with other studies, this study found that only 52% of the respondents used a locking mechanism to deter unauthorized access to the device. Interestingly, Muslukhov et al. found that of those 52% of users that did employ a locking mechanism, 99% of them used a four-digit PIN or the draw-a-secret method. Several studies have shown that these are the two weakest forms of authentication and are subjected to several attacks such as shoulder surfing, eavesdropping, and smudge attacks. The users stated that they chose those authentication methods due to convenience. Muslukhov et al. suggest that smartphones need to integrate a logging system in order for the device owner to detect unauthorized access. It should be noted that the respondents were between the ages of 19-30 and over 90% were from the U.K. so generalization of the results is limited.

Mylonas, Gritzalis, Tsoumas, and Apostolopoulos (2012) addressed specific security awareness differences between smartphone users that have information security

(IS) backgrounds versus users that do not. Unsurprisingly, Mylonas et al. found that users with IS backgrounds are more aware of security risks pertaining to smartphones. Moreover, Mylonas et al. also found that users with IS backgrounds thoroughly read and analyze End User License Agreements (EULA) and permission prompts compared to users without IS backgrounds. Where the behaviors between the two groups are similar is that both groups were found to be unaware if distributed applications were scrutinized for legitimacy or if the application was malware. Also, many users from both groups were found to have basic security features disabled on their phone such as a screen locking mechanism. Mylonas et al. found that smartphone security awareness was significantly lacking as well as research specifically tailored to smartphone security behaviors. They contended future research in smartphone security behaviors is warranted to raise awareness and to assist users with the challenges of smartphone security.

In Furnell's (2008) article, he described the need for increased information security and privacy awareness. Furnell argued that the proliferation of Internet applications, Websites, and computing devices has far outpaced the embracement of security practices and awareness. In other words, adoption of security practices has not kept pace with increased security risks. Furnell stated, "Users often know the threats are there, but fail to reflect this in their behavior" (p. 6). Additionally, he argued that security awareness is not reflective of the users' online behaviors regarding sharing personal and sensitive information. The article also pointed out that this type of behavior is not only risky to organizations, but also from a personal perspective. Furnell also argued that it is more than just a lack of security awareness, but also the users' inability to understand the technicalities involved, such as how to keep anti-virus software current. Users' lack of

technical aptitude presents significant challenges in protecting themselves from sensitive information disclosure. The main premise of this article was that reckless user behavior, lack of security awareness, and technological inexperience poses significant risks to both organizations and the user.

Huang, Rau, and Salvendy (2010) set out to explore specific factors that affect the overall perception of information security (IS) among Internet users. Huang et al. argued that the human factor is significant in overall IS posture and that users view risks differently and, therefore, respond to threats differently. Moreover, Huang et al. noted that very little research has been conducted investigating the socio-cognitive behaviors behind IS behaviors. Huang et al. evaluated the responses to 21 common threats and their related outcomes. Huang et al. then conducted exploratory factor analysis (EFA), which resulted in a six factor structure: Knowledge, impact, severity, controllability, possibility, and awareness. It should be noted, however, that some factors had only 'fair' loadings of <0.5 but >0.4 and one factor loaded on more than one component. Among the most important results indicated are that computer experience played a significant role in IS perception, IS perception was related to the type of loss the threats brought, and that users showed little concern for personal information loss.

Kruger and Kearney (2006) developed and tested a prototype for assessing InfoSec awareness in an organizational environment. The article stressed the importance of measuring IS awareness as a means of governance to assess the effectiveness of organizational IS programs. Kruger and Kearney noted that the increased reliance on information technology for conducting daily business operations makes it imperative for organizations to have effective IS programs. Lack of IS awareness can put an

organization at risk of information breaches. The key purpose of these programs is to ensure employees are keenly aware of the current state of risks. However, Kruger and Kearney argued that simply developing an organizational IS program is not enough. They contended that active governance and measurement of the program is necessary, specifically because end users are typically at the heart of IS program failures. Kruger and Kearney's model measured three user components: knowledge, attitude, and behavior across five risk focus areas: company policy adherence, secret passwords, email/Internet caution, mobile equipment, and incident reporting. The results of the assessment showed promise in assessing overall organizational awareness, to include identifying specific areas for improvement. Particular to this case study, Kruger and Kearney found two risk focus areas scored poorly, adherence to policies and actions/consequences, which could be reassessed and modified to increase security awareness in those two categories.

Albrectsen (2007) explored information technology (IT) users' experiences and roles in overall information security (IS) within their organization. Consistent with the majority of published literature, Albrectsen states that users play a significant role in the overall effectiveness of IS programs. The results of this specific study found that users believed in the overall importance of IS programs. However, since the users had limited involvement, they did not feel like an important piece of the IS puzzle. Consequently, the users had little to no knowledge of current IS risks or mitigating techniques. Interestingly, although the IS program was fully documented and established within the organization, overall awareness was significantly lacking. This finding negates many other published research articles that claim documented and emphasized IS programs are key to increasing IS awareness. Through interviews, Albrectsen found a preference for a user-

involved approach to the IS program to help the users grasp the gravity of IS risks and mitigation tools. As Albrectsen noted in his analysis, “mass media awareness campaigns had a low degree of influence on users” (p. 288). The results of this study cannot be generalized due to the small sample size chosen (N=19), as Albrectsen explained that the goal was to “not generalize but to interpret some users’ experience of information security” (p. 278).

According to Rezgui and Marks (2008), the number of studies that undertake an in-depth look at IS awareness is limited. The majority of IS awareness is grounded within the computer domain. Siponen (2000) also noted the lack of studies in researching user behaviors and the determinants that result in decreased security practices. Moreover, Huang et al. (2010) stated that not only has very little research been conducted pertaining to the socio-cognitive behaviors behind IS security practices, but many studies only study a single factor. Huang et al. (2010) argued that several factors need to be investigated in order to gain a deeper understanding of the behaviors that drive the security practices of users. Additional factors they studied were threats and vulnerabilities in addition to risk. Huang et al. found that experience led to a greater awareness of threats, vulnerabilities, and risks, which all had significance in predicting user security practices.

Trust

Smartphones have dramatically changed the technological landscape. This dramatic change has led to unique ways for business to deliver their products, namely software applications. Wang and Emurian (2005) wrote that rapid advancements in technology would require businesses to seek new and alternative ways to deliver their products. As such, each individual smartphone platform (i.e., Android, iOS, Windows)

has developed its own “marketplace” for users to download software products from various manufacturers. These marketplaces are only applicable to handheld mobile devices such as smartphones and tablets and are specific to the operating system of the mobile device. Apple® devices, such as iPhone® and iPad®, use the iTunes® application market for downloads and purchasing. Whereas, the marketplace for application downloads and purchases for Android® based mobile devices is called the Play Store®. Unfortunately, some of the applications available in the marketplace are used to access and exploit personal information (Park et al., 2012). Since it may be difficult to obtain information regarding a vendor’s reputation outside of user reviews, the consumer may be forced to develop a certain level of trust (Mui, Mohtashemi, & Halberstadt, 2002).

Trust has been studied in various disciplines such as psychology, management, sociology, and marketing to name a few. Trust is also an important research topic in an online context (Tan & Sutherland, 2004; Wang & Emurian, 2005). Studies of trust and perceived risk have been conducted in an attempt to gain a deeper understanding of consumer purchasing habits (Pavlou & Gefen, 2004). Trust and reputation are at the root of every transaction and are important research topics in many fields (Mui et al., 2002). For example, the probability is low of someone purchasing a vehicle from an auto dealer that has a notorious reputation for selling lemons. However, that same consumer may consider purchasing the vehicle from that dealer if they have trust in the brand of the vehicle they are buying. The same holds true when it comes to trust and reputation regarding electronic transactions. A consumer is unlikely to download or purchase a software application that has a reputation for buggy software and lack of customer service.

However, electronic marketplaces present new problems in consumer-seller relationship trust as compared to traditional brick-and-mortar marketplaces (Verhagen, Meents, & Tan, 2006). Therefore, consumers must depend solely on their perceptions of the marketplace in order to develop a certain level of trust (Verhagen et al., 2006). In addition to trusting the marketplace, the consumer must also trust the seller.

Chin et al. (2012) conducted a study that measured user confidence in smartphone security. Chin et al. hypothesized that smartphone users do not fully accept and harness the computing power of smartphone devices due to users' security and privacy concerns with smartphone devices. Chin et al. investigated smartphone users' willingness to perform certain tasks and application discovery and installation decisions. Chin et al. interviewed 60 smartphone users and found that smartphone users are less willing to conduct tasks on their smartphones than on their laptops. The respondents indicated that they are more concerned about privacy and security on their smartphones due to specific fears associated with smartphone devices. The most prominent fears included smartphone loss/damage, data loss, and application trust. A key finding of this study were the misconceptions held by users regarding application security in the application stores as well as wireless and end-to-end security of the device. Chin et al. noted in their data, although they did not investigate further, that these misconceptions might be directly related to smartphone experience and proficiency.

Ba and Pavlov (2002) stated, "Trust is a catalyst in many buyer-seller transactions…" (p. 244). Ba and Pavlov conducted a two-prong study to determine factors that may lead to an increased level of trust in order to conduct an online transaction. Ba and Pavlov developed a Webpage which mimicked eBay® for their two

studies. The first study set out to determine if positive or negative feedback from previous buyers was a determinant on purchases from a new buyer. The participant in the experiment was shown the Website with the positive and negative feedbacks, then asked to rate their level of trust with that seller. The positive and negative feedbacks were manipulated by Ba and Pavlov to determine any fluctuation in the levels of trust by the potential buyer. The second experiment was similar in nature. However, the second experiment focused on the sales price of the items. The results of the study showed that more positive feedback left by previous buyers led to an increase in overall trust by a new buyer. It also resulted in the willingness to pay a premium for the product. Suggested future work by Ba and Pavlov is a more in-depth analysis of antecedents of trust as it applies to online marketplaces. Additionally, they note that a limitation of the study was that the experiment was conducted in the context of auctions and future studies should examine different online marketplaces.

Conversely, Lacohée, Phippen, and Furnell (2006) found that trust was not a factor in whether or not an online transaction was executed. This study assessed how users establish and perceive trust in executing online transactions. Lacohée et al. contended that assurance of security by online retailers prior to engaging in online transactions was not the motivating factor behind establishing a trust relationship about the transaction. Through open focus group question-and-answer sessions, Lacohée et al. accumulated response sets from online e-commerce users. Lacohée et al. found that it is, in fact, not the claim of security assurance that is a precursor of establishing trust. Moreover, Lacohée et al. found that many users were not even sure what the technological assurances meant. The results of the focus group determined that it was

more important to specify what they will do *if and when* the security breach occurs rather than making claims that it will not occur at all. Lacohée et al. also found that many times online transactions occur regardless of the trust factor. They found if the user was able to shift the risk, was assured of restitution if something occurred, or if the benefit outweighed the risk, the transaction would still be carried out. For example, users were found to purchase from unknown online retailers if a product price was cheaper than commonly known online retailers. Additionally, users felt that purchasing by credit card shifted the risk to the credit card company, which would refund the purchase price to the credit card if something went wrong. In summary, the results of this article showed that users conduct risky online behavior, especially if they perceive they will not be the victim.

Mylonas et al. (2013) conducted interviews of 458 smartphone users. The results of the interviews found that 76% of the participants believed that the applications in the marketplace are secure. Moreover, approximately 75% of the users trusted the marketplace. However, Mylonas et al. found that users were completely unaware if applications in the application stores were scrutinized for legitimacy, despite trusting the marketplace where the applications are downloaded from. This is an indicator of possible blind trust in the application store. Moreover, Mylonas et al. found the majority of the participants believed all applications in the marketplace were secure. Their findings also suggest users who trust the application repository are typically not fully aware of smartphone security.

Shin (2010) collected 397 responses from an online survey to test the effects of trust, security and privacy in social networking sites (SNS). The results of the study

found that trust was a significant factor in determining user attitude and intention in using SNS. However, it was noted that expertise might play a significant role in determining trust as it relates to attitude and intention. Future work should also consider specific precursors to trust.

These studies indicate two possible different constructs that need further investigation: party trust and institutional trust. Sociologists believe trust stems from a social structure, which shapes the way people develop their beliefs in trust, often times referred to as institutional trust (Tan & Sutherland, 2004). A more precise definition of institutional trust as it relates to a smartphone is the trustworthiness of the intermediary operating the system (Verhagen et al., 2006).

Party trust will focus on specific applications available in the online application stores. Institutional trust will focus on trust of the application stores themselves (p. 3). Verhagen et al. (2006) define party trust as “perceptions of trust in the counterpart of the transaction” (p. 3). Fung and Lee (1999) noted that trust has shown to have high significance in uncertain environments. Theoretically, smartphones could be categorized as an uncertain environment due to their relative newness to the computing field. Therefore, based on previous research findings that both of these constructs have shown to have a direct correlation on user behavior, this study will investigate their reliability and validity specific to smartphone user’s security practices and behaviors.

Security Practices and Behaviors

Botha et al. (2009) set out to explore the differences between desktop computing security mechanisms as compared to smartphone security mechanisms. Botha et al. contended that significant differences, in user security behaviors as well as available

security tools, create a state of confusion for the users as well as lack of knowledge pertaining to smartphone security. Moreover, Botha et al. pointed out that smartphone devices create new security risks due to lack of use and availability of authentication methods, lack of physically controlled environments, and small form factor of the smartphone leading to increased loss and theft of the device. Botha et al. also noted that there are significantly different communication means that also need to be protected and manually configured by the device user, which can also lead to an increase in security vulnerabilities. Botha et al. contended that users need to be more aware of the limitations in smartphone functionality as compared to their desktop environment in order to gain a deeper understanding on how users can better protect themselves.

Ben-Asher et al. (2011) argued that the lack of authentication method implementation is largely based on smartphone users security needs, awareness of and concern for security risks, and levels of perceived sensitivity of data stored or logged on the smartphone. Moreover, Ben-Asher et al. stated that the small form factor of the device makes it inherently more susceptible to loss or theft, which can result in the risk of sensitive data compromise that is magnified by lack of awareness of available security mechanisms. In addition to lack of awareness, Ben-Asher et al. also noted that many users will simply not utilize the available security mechanisms due to the perceived inconvenience of authenticating. The results of the survey indicated that many smartphone users desired authentication methods that were more convenient but still offered substantial security adequacy. Ben-Asher et al. argued for “graded” security levels, which would be better termed “graduated” security levels, in which there are different levels of access determined by authentication type. For example, if no means of

authentication is provided, the user may be granted basic telephone privileges, but not the ability to gain access to the Internet or download and install third-party applications.

Botha, Furnell, and Clarke (2009) addressed the differences between desktop computing security mechanisms as compared to smartphone security mechanisms. Botha et al. contend that significant differences in both user security behaviors, as well as available security tools, creates a state of confusion for the users as well as lack of knowledge pertaining to smartphone security. Moreover, Botha et al. point out that smartphone devices create new security risks due to lack of authentication methods used and available, lack of physically controlled environments, and small form factor of the smartphone leading to increased loss and theft of the device. Botha et al. also noted that there are significantly different communication means that also need to be protected and manually configured by the device user, which can also lead to an increase in security vulnerabilities. Botha et al. contend that users need to become more aware of the limitations presented in smartphone devices as compared to their desktop environment in order to gain a deeper understanding on how users can better protect themselves.

In the article by Van Bruggen et al. (2013), the authors address the need for increased security conscious behavior among smartphone users. Van Bruggen et al. note that user owned smartphones are becoming more widely accepted into the workplace in order to facilitate work-related transactions, such as email while away from the office. This increased acceptance by organizations leads to organizational proprietary information being stored and transmitted on the smartphone devices and the lack of security conscious behaviors creates a significant risk. They found that many users do not even enable screen locking mechanism while the phone is not in use. Therefore, Van

Bruggen et al. tested an intervention method that focused on three different motivational angles -- deterrence, morality, and incentives -- in an attempt to increase security conscious behaviors by smartphone users; specifically, locking the phone and periodically changing their password. For those users that did lock their phone, Van Bruggen et al. found deterrence produced the most immediate results, whereas, morality produced more long term results. The results of the study found that for users who did not lock their phone, it was extremely difficult to change their behavior. Thus, it can be inferred that regardless of attempts to modify behaviors, users will still openly expose themselves and their organizations to information security risks.

Mylonas, Kastania, and Gritzalis (2012) addressed smartphone application repositories, such as Google's "Play Store" and Apple's "App Store" as breeding grounds for attackers to distribute malicious software. Mylonas et al. pointed out that the increased popularity of smartphone devices becoming more deeply entrenched in society has resulted in exponential application downloads from the official application repositories. Mylonas et al. argued that due to lack of security and privacy controls at the application repository level, the burden of security decisions has been placed on the smartphone user. Mylonas et al. explored the smartphone user's security awareness of the applications within the repositories in an attempt to build a prediction model to identify users that trust the application repositories. Mylonas et al. observed that users considered less computer savvy are more likely to download and install applications with total disregard of security and privacy implications. However, it should be noted that Mylonas et al. reported a Cronbach of only (α=.506) and the majority of their survey consisted of only two-item measures.

In the article by Furnell et al. (2007), they assessed Internet users' familiarity and knowledge of security threats and associated security protection tools. Furnell et al. argued that users' awareness concerning IT security threats and available security protection tools is a major cause for concern. The level of significance of this lack of awareness and protection can be summed up in the statement by Furnell et al., "Compromised home systems have the potential to perpetuate problems for the Internet community as a whole" (p. 410). Therefore, Furnell et al. surveyed 415 Internet users and measured their knowledge of threats, knowledge of available security tools, use of security tools, and knowledge of configuring the security tools. The results show that there is scant knowledge of the risks among the majority of respondents. However, there is a divergence between this knowledge and the knowledge of available security applications, their use, and configurations. This finding is more prevalent among novice users. Furnell et al. pointed out it is more of a concern that many users who considered themselves advanced computer users also lacked the knowledge to implement and configure the appropriate security controls. Therefore, the results showed that users do pose a significant risk to themselves and the rest of the online community through their lack of understanding and overconfidence in their abilities.

Summary

In summary, this study contended, based on prior research, that several factors have a significant impact on the overall user security practices and behaviors. Although the majority of the articles studying IS security practice behaviors and practices are grounded in the domain of traditional computing, the gap in literature between traditional computing and smartphone security is significant and requires more research. As such,

based on the works of Chen et al. (2011), Chin et al. (2012), Furnell (2008), Furnell et al. (2008), Rhee et al. (2009), and Stanton et al. (2005), this study posited that VA, RA, TA, MISE, IT, and PT all have a significant role in smartphone users' security practices (SP) and behaviors (SB).

Chapter 3

Methodology

Introduction

This chapter describes the approach and methodology that was used to conduct the study. First, the approach to the study will be discussed, followed by the specific propositions, survey development, and, finally, how the study was executed and analyzed.

Approach

This study was confirmatory in nature and employed previously validated constructs from the domain of computer security and attempted to confirm their reliability and validity in the context of smartphones. This study utilized a Web-based survey to collect and store data electronically using Google® Forms. The survey was disseminated through Facebook® and LinkedIn® social media outlets. The main research question this study proposed to address was: Do the factors of MISE, VA, TA, RA, IT and PT, demonstrate high reliability and validity in determining smartphone users' security practices and security behaviors? To address this question a theoretical model (figure 2) was developed using previously validated constructs identified during literature review pertaining to computer security. The approach to this study is depicted in figure 3.

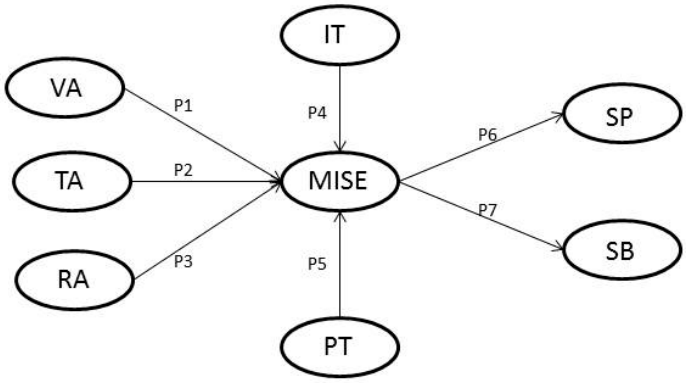


Figure 2. Theoretical Framework.

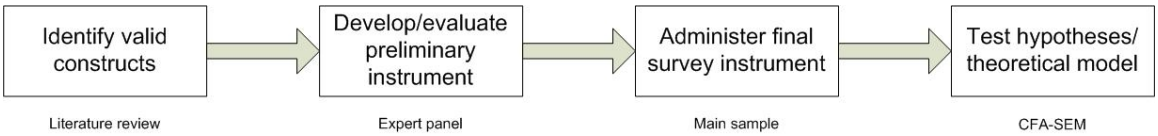


Figure 3. Research model.

Propositions

The propositions that this study analyzed were:

P1: Vulnerability awareness (VA) positively impacts mobile information security efficacy (MISE).

P2: Threat awareness (TA) positively impacts mobile information security efficacy (MISE).

P3: Risk awareness (RA) positively impacts mobile information security efficacy (MISE).

P4: Institutional trust (IT) positively impacts mobile information security efficacy (MISE).

P5: Party trust (PT) positively impacts mobile information security efficacy (MISE).

P6: Mobile information security efficacy (MISE) positively impacts security practices (SP).

P7: Mobile information security efficacy (MISE) positively impacts security behaviors (SB).

Instrument Development

Mobile Infosec Self-efficacy

This study measured user's MISE using the previously validated 11-item construct used by Rhee et al. (2010) in measuring InfoSec self-efficacy. This study adopted all 11 items and reworded them, as item number six is not applicable to smartphones. The items were tailored to smartphone-specific features. MISE was measured using a 7-point Likert scale, where 1 indicated "completely not confident" and 7 indicated "completely confident".

Vulnerability, Threat, and Risk Awareness

This study measured users' VA, TA, and RA based on the unpublished work of Simpson, Nilsen, Levy, and Cohen (2014). Simpson et al. (2014) studied factors that affected perceived information security risks of smartphone users. The study found very high reliability with strong Cronbach α values above 0.9 with all three constructs. Risk had eight items, threat had seven items, and vulnerability had nine items. All constructs were measured using a 7-point Likert scale where 1 indicated "completely unaware" and 7 indicated "completely aware."

Institutional and Party Trust

This study used the previously validated constructs of party trust and institutional trust developed by Verhagen et al. (2006). Each construct contained measurement items

that exhibited high reliability with a Cronbach α of 0.89 for institutional trust and 0.92 for party trust. The items were adapted for this study and slightly modified to put them into smartphone context. Each item was based on a 7-point Likert scale where 1 indicated "completely disagree" and 7 indicated "completely agree."

Security Practices and Behaviors

Rhee et al. (2009) studied two different types of security constructs: security practices (SP) and security behaviors (SB). This study used these two previously validated constructs. SB focused on actual behaviors of smartphone users such as online banking and willingly sharing PII. SP focused on the technical aspect of smartphone security such as the usage of anti-virus and anti-malware programs, and locking the phone when not in use. Both constructs consisted of eight measurable items. The items in the security practices construct were measured using "yes", "no", and "I don't know" answers. This study adopted five of the eight items in the SP construct and consisted of "yes" and "no" answers and was repurposed into the context of smartphones. Of the eight measurable items of the SB construct, six were adopted, again with slight variations to the wording to put them into smartphone context, and consisted of "yes" and "no" answers. Smartphone-specific features pertaining to locking the device when not in use were also added.

Expert Panel

After the literature review was completed, a preliminary survey instrument was developed. The survey instrument was then disseminated to an expert panel consisting of six members with terminal degrees in the IS field or information security backgrounds. The purpose of the expert panel was to evaluate the applicability, precision, and clarity of

the questions, known as content validity, and is consistent with the approach of Straub (1989). The goal behind the expert review was to identify any necessary adjustments to the survey instrument such as removing unnecessary items, question modifications, and or layout of survey. The preliminary survey instrument was distributed via email to the expert panel members and they were given 1 week to provide their qualitative analysis of the instrument. The feedback from all six panel members was taken into consideration. Most of the feedback was consistent between all six members. The feedback consisted of only minor issues such as removing question marks, misspellings, adding more definitions to the measurement items, and changing the wording for the responses. All the feedback was incorporated due to panel consensus. Since all six members submitted nearly identical feedback, the survey instrument was not redistributed to the expert panel.

Reliability

Establishing reliability is critical in the research process. Reliability is documenting the internal consistency of the variables, or set of variables, that they are intended to measure (Straub, Rai, & Klein, 2004). Cronbach α is the most commonly used measure to determine reliability of a survey instrument (Sekeran, 2003; Mertler & Vannatta, 2013). According to Mertler and Vannatta (2013) and Hair, Anderson, Tatham, and Black (1998), a Cronbach α value must meet or exceed 0.7 to be deemed reliable. Most of the constructs in this study are being repurposed from the traditional computing domain to the smartphone domain. The constructs were previously confirmed as reliable. However, due to the repurposing effort being undertaken in this study, Cronbach α was used to determine reliability of the constructs and are discussed in Chapter 4.

Validity

Internal Validity

According to Levy (2006), there are typically three categories of validity that need to be addressed: internal, external, and instrument. Confirming internal validity is the process of ruling out alternative explanations of dependent variables that are not explainable by the independent variables (Straub, Boudreau, & Gefen, 2004). Through extensive literature reviews, this study used previously validated constructs from existing literature that demonstrated strong causal relationships between the constructs. Moreover, an expert panel was established to review the instrument to ensure representativeness and meaningfulness of the measures. Thus, this study is considered to have high internal validity.

External validity

External validity pertains to how the results of the study can be generalized (Cook & Campbell, 1979). The targeted audience was representative of the smartphone population in terms of demographics, age, and gender. The survey was administered to 539 people. A total of 275 responses were collected for a response rate of over 50%. Thus, the results of this study are generalizable and external validity is considered high.

Instrument validity

Instrument validity was addressed through both extensive literature review and an expert panel to ensure content and construct validity of the instrument. The expert panel was used to assess the content and construct related validity, helping to ensure the proposed items are appropriate to what this study intends to measure. Moreover, the expert panel was used to ensure there were not any ambiguities or redundancies and that

the instrument asks appropriate questions that are encompassing of what this study intended to measure. There were minor tweaks to the questions based on expert panel feedback. Based on expert panel feedback and extensive literature review, instrument validity is considered high.

Population and Sample

This study was disseminated through social media outlets of Facebook® and LinkedIn®. Previous work by Simpson, Nilsen, Levy, and Cohen (2014) disseminated a survey instrument through Facebook® which resulted in an approximate response rate of 30% and the respondents were representative of the population. Therefore, this study used the same means of survey distribution. The user base of this survey was distributed to 539 users. The response rate was 50.6%. Carefully crafted reminders were used to keep ongoing participant recruitment until the 250 minimum required responses to conduct the statistical analysis were met.

A review of the literature had revealed vastly different views on the minimum sample size required for CFA and SEM. For CFA, Gorsuch (1983) recommends a sample size of at least 100; whereas, Comrey and Lee (1992) recommend between 200 and 300 samples. For SEM, Weston and Gore (2006) suggest a minimum of 200 samples. Based on literature reviews to conduct CFA-SEM the response rate met the generally published guidelines of N>200 allowing for a sufficient sample of the population. The response rate also allowed for any exclusion of data that may be necessary due to missing data, response set, and outliers, while still maintaining enough responses for a valid statistical analysis.

Pre-Analysis Data Screening

Pre-analysis data screening is the process of detecting and dealing with problems with collected data (Levy, 2006). Some of these problems consist of missing data, response set, outliers, linearity, and skewness or kurtosis (non-normality). Therefore, to ensure the validity of the results, the researcher must thoroughly check the validity of the data (Mertler & Vannatta, 2013). The Web-enabled survey this study used had required responses that eliminated missing data and transcription errors. Scatter plots, discussed in Chapter 4, were used to examine linearity and normality. Mahalanobis Distance (MD), also discussed in Chapter 4, was used to determine any extreme outliers. Each case was then further scrutinized to determine the necessity of possible removal of the response case.

Data Analysis

After pre-analysis data screening, CFA was conducted. The purpose behind conducting CFA is to confirm or refute support for an *a priori* theory (Mertler & Vannatta, 2013). A hypothesized model is developed and used by the researcher in an attempt to estimate a covariance matrix of a population and compare that to the observed covariance matrix (Schrieber, Nora, Stage, Barlow, & King, 2006). Utilizing CFA has shown to be ideal for testing the validity of proposed constructs based off of previously published literature (Gallaspy, 1996). CFA is used to analyze the validity of the fitness of a proposed model. According to Shumacker and Lomax (2010) and Levy and Green (2009), the most commonly reported fitness criteria in CFA are Chi Square (CMIN/df), goodness of fit index (GFI), adjusted goodness of fit index (AGFI), root-mean-square-of-approximation (RMSEA), root mean square residual (RMR) and standardized RMR

(SRMSR). Post CFA, further data analysis was conducted using an SEM technique to test the relationships and significance between the constructs.

Resources

Google Forms was used to develop the survey and collect the data from the survey participants. The survey was distributed through Facebook® and LinkedIn®. Once the data were collected, Statistical Package for Social Sciences® (SPSS), AMOS, and Microsoft Excel were used to analyze the data.

Summary

This chapter provided an overview of the approach and methodology that this study used. This study was quantitative in nature and utilized an online survey hosted on Google Forms. The purpose of this study was to conduct CFA of previously validated constructs from existing literature in the traditional computing domain and test their applicability to smartphone security domain. The methods that were used to test the propositions and address the main research question stated in this study included a literature review, instrument development, expert panel, data collection, and analysis. The survey was disseminated though LinkedIn® and Facebook ® and resulting in 275 total responses.

Chapter 4

Results

Introduction

This chapter details the data analysis and the results of the current study. This chapter includes an analysis of the data collection process, analytical statistical methods used, and the overall results. First, the results of the expert panel will be discussed followed by the results of the pre-analysis data screening and then the results of the quantitative phase. The chapter then concludes with a summary of the results and the procedures utilized for the analysis.

Survey Analysis

Through extensive literature review of scholarly articles pertaining to computer security, a preliminary survey was developed (Appendix A). This survey was developed using Google Forms and consisted of previously validated factors from existing literature in computer security. The survey was developed in order to provide a means to collect data in order to statistically analyze the theoretical model for reliability and validity in the context of smartphones. Additionally, the data from the survey was used to test for causal relationships in the structural equation model between the factors as noted in the proposed propositions in Chapter 3. The data was also used to answer the main research question: Do the factors of mobile InfoSec self-efficacy (MISE), vulnerability awareness (VA), threat awareness (TA), risk awareness (RA), institutional trust (IT), and party trust

(PT) demonstrate high reliability and validity in determining smartphone users' security practices (SP) and security behaviors (SB)?

Expert Panel

Before disseminating the survey to the general population for data collection, the survey was sent to an expert panel to review for consistency, ambiguities, redundancies, and to ensure the questions were encompassing of the data this survey intended to collect. The survey was sent via email (Appendix B) to six people that had terminal degrees in information systems and/or had information security backgrounds and were currently working in information security positions. All six people participated in the survey review. The feedback was positive and only included minor tweaks such as rewording the answers, minor spelling mistakes, and punctuation. As a result, a final survey instrument (Appendix C) was developed and disseminated to the general population via Facebook® and LinkedIn® for data collection.

Survey Responses

The active data collection effort began on June 19th, 2015, and continued until June 27th, 2015. Study participants were able to access and complete the online survey for a total of eight days. The survey was turned off after responses were no longer being obtained. The total potential respondent base via Facebook® and LinkedIn® was 539 potential respondents. Of the 539 potential respondents, 275 total responses were collected at a collection rate of 50.6%.

Preliminary Analyses

Before testing the propositions, pre-analysis data screening was conducted in order to ensure the data was reliable, useful, and valid. The data screening process

reported below included tests for: missing data, response sets, outliers, normality, and multicollinearity.

Missing Data

As previously noted in Chapter 3, all the questions in the survey were marked as required questions. A respondent could not submit the survey unless all questions were answered. If a respondent did not answer a question, a prompt required that the missed question be answered before submitting. As such, there was no missing data in the survey.

Response Set

Response set is an unengaged respondent meaning that the respondent simply answered the same way throughout the entire survey. Response set is detected through visual inspection of the data. Through visual inspection of the data for this study, 13 response sets (cases 7, 16, 21, 41, 107, 112, 124, 130, 193, 217, 233, 239, and 247) were detected and eliminated from further data analysis. Removing these 13 responses resulted in 262 responses for further analysis.

Outliers

Next, univariate and multivariate outliers were tested. Univariate outliers are cases with extreme values on only one of the factors (standardized scores in excess of +/- 3.29), whereas cases with extreme values on two or more factors are considered multivariate outliers (Tabachnick & Fidell, 2007). The Z scores for each variable were calculated and no variable exceeded the +/-3.29 threshold. Thus, no univariate outliers were detected. To detect multivariate outliers within the data set, Mahalanobis Distance was calculated. There were six total multivariate outliers identified (cases 31, 110, 120,

151, 162, and 233) that were removed from further analysis leaving a final tally of 256 responses to analyze.

Normality

To test for normality, the data were analyzed for skewness and kurtosis. First, histograms were developed and assessed to visually determine any skewness or kurtosis issues. Reviewing the histograms did not reveal any significant non-normality issues. Second, the numeric results were also analyzed for any skewness or kurtosis issues. The numeric results showed that skewness was within acceptable levels of absolute value of 2 (Terrell, 2012). Additionally, the numeric results did not show any kurtosis issues as all values fell below the kurtosis threshold of 2.2 (Sposito et. al., 1983; Terrell, 2012). Thus, no significant non-normality issues were discovered.

Multicollinearity

Although there are several ways to detect multicollinearity, two of the most common statistical analyses to discover the potential problem are through examination of Pearson bivariate correlations and variance inflation factors (VIFs) (Mertler & Vannatta, 2014). Therefore, these two analyses were computed to determine the presence of multicollinearity. Multicollinearity is when two or more factors are highly correlated to each other ($r > .90$) because the two factors contain redundant information, thus measure the same thing (Tabachnick & Fidell, 2007). None of the factors exceeded .828 as depicted in Table 1. This is below the defined $r < .90$ threshold (Tabachnick & Fidell, 2007). None of the VIF scores (Tables 2-5) exceeded 3.20, which is well under the defined threshold of 10.00 (Hair, Anderson, Tatham, & Black, 1998). Through these two calculations it was determined that multicollinearity was not an issue.

Table 1. Pearson Coefficient (N = 256)

		COMB_SP	COMB_SB	COMB_MISE	COMB_RA	COMB_VA	COMB_TA	COMB_IT	COMB_PT
Comb_SP	Pearson Correlation	1	.225**	.276**	.243**	.373**	.357**	-0.059	-0.096
	Sig. (2-tailed)		0	0	0	0	0	0.349	0.127
Comb_SB	Pearson Correlation	.225**	1	.223**	0.093	.152*	.146*	0.067	-0.05
	Sig. (2-tailed)	0		0	0.139	0.015	0.02	0.289	0.428
COMB_MISE	Pearson Correlation	.276**	.223**	1	.689**	.794**	.752**	.230**	.352**
	Sig. (2-tailed)	0	0		0	0	0	0	0
COMB_RA	Pearson Correlation	.243**	0.093	.689**	1	.760**	.828**	0.113	.229**
	Sig. (2-tailed)	0	0.139	0		0	0	0.071	0
COMB_VA	Pearson Correlation	.373**	.152*	.794**	.760**	1	.813**	.151*	.262**
	Sig. (2-tailed)	0	0.015	0	0		0	0.016	0
COMB_TA	Pearson Correlation	.357**	.146*	.752**	.828**	.813**	1	.157*	.234**
	Sig. (2-tailed)	0	0.02	0	0	0		0.012	0
COMB_IT	Pearson Correlation	-0.059	0.067	.230**	0.113	.151*	.157*	1	.733**
	Sig. (2-tailed)	0.349	0.289	0	0.071	0.016	0.012		0
COMB_PT	Pearson Correlation	-0.096	-0.05	.352**	.229**	.262**	.234**	.733**	1
	Sig. (2-tailed)	0.127	0.428	0	0	0	0	0	
**. Correlation is significant at the 0.01 level (2-tailed).									
*. Correlation is significant at the 0.05 level (2-tailed).									

Table 2. Mobile InfoSec Self-Efficacy VIF

Coefficients[a]			
		Collinearity Statistics	
Model		Tolerance	VIF
1	COMP_VA	.338	2.962
	COMP_TA	.311	3.220
	COMP_RA	.355	2.816
a. Dependent Variable: COMP_MISE			

Table 3. Risk Awareness VIF

Coefficients[a]			
		Collinearity Statistics	
Model		Tolerance	VIF
1	COMB_MISE	.396	2.525
	COMB_VA	.309	3.237
	COMB_TA	.355	2.814
a. Dependent Variable: COMB_RA			

Table 4. Threat Awareness VIF

Coefficients[a]			
		Collinearity Statistics	
	Model	Tolerance	VIF
1	COMP_VA	.324	3.086
	COMP_MISE	.410	2.437
	COMP_RA	.421	2.375
a. Dependent Variable: COMP_TA			

Table 5. Vulnerability Awareness VIF

Coefficients[a]			
		Collinearity Statistics	
	Model	Tolerance	VIF
1	COMP_MISE	.465	2.152
	COMP_RA	.381	2.622
	COMP_TA	.338	2.962
a. Dependent Variable: COMP_VA			

Descriptives

After removing problematic responses discovered in the pre-analysis data screening, there were a total of 256 responses left for analysis. Table 6 provides a brief overview of the respondent descriptive statistics.

Table 6. Descriptives Table (N = 256)

		Frequency	**Percentage**
Gender	Male	116	45.3%
	Female	140	54.7%
		Frequency	**Percentage**
Education	High School	17	6.6%
	Some College	71	27.7%
	Associate	45	17.6%
	Bachelor	80	31.3%
	Graduate	43	16.8%
		Frequency	**Percentage**
Marital Status	Single	35	13.7%
	Married	174	68.0%
	Divorced	38	14.8%
	Widowed	3	1.2%
	Separated	6	2.3%
		Frequency	**Percentage**
IS Background	Yes	103	40.2%
	No	153	59.8%
		Frequency	**Percentage**
Operating System	Android	142	55.5%
	iPhone	106	41.4%
	Windows	3	1.2%
	Blackberry	1	0.4%
	Unknown	4	1.6%
		Frequency	**Percentage**
Age	18-24	18	7%
	25-34	61	24%
	35-44	77	30%
	45-54	54	21%
	55+	46	18%
	Min/Max	**Mean**	**Std Dev**
Years experience	1/20	7.071	4.1862

There was a fairly even distribution in gender with 55% female responses compared to 45% male responses (Table 6). Over 93% of the respondents reported having post-high school education. Sixty-eight percent of the respondents reported that they were married. The majority of the respondents (60%) reported not having an IS background. Nearly 56% of the respondents reported Android as their phone's operating system, whereas

41% reported owning the iPhone. The ages of the respondents were relatively distributed with the largest age group reporting to be between the ages of 35 to 44. The average number of years that participants reported having a smartphone was 7.07 years (*SD* = 4.19).

Additionally, descriptive statistics was also conducted on the dependent factors of security practices and security behaviors in order to obtain a deeper insight to the overall practices and behaviors of the respondents (Table 7). Security Practices is defined as the technological aspect that a user takes (i.e., installing security applications) to protect their mobile device (Rhee et al., 2009). With exception to spam filters on email clients, the majority of the respondents exhibit very poor security practices. Conversely, the majority of the respondents exhibit very good security behaviors, which is defined as the security conscious behavior and actions that users demonstrate while using their mobile device (Rhee et al., 2009).

Table 7. Security Practices and Behaviors Descriptive Statistics

Security Practices	Yes	No
1. Do you currently have antivirus software on your smartphone?	49%	51%
2. Do you currently have email spam filter installed on your smartphone?	56%	44%
3. Do you currently have antispyware on your smartphone?	47%	53%
4. Do you currently have a firewall installed on your smartphone?	30%	70%
5. Do you currently have any sort of encryption installed on your smartphone?	33%	67%
Security Behaviors		
1. Do you use file sharing software (Kazaa, EDonkey, etc.) from your smartphone?	4%	96%
2. Do you make backup copies of your files from your smartphone?	58%	42%
3. Do you have sensitive documents such as medical, financial, or banking stored on your smartphone?	20%	80%
4. Does your smartphone require some form of authentication (PIN, Password, Pattern) before getting access?	78%	22%
5. When transferring data on the Internet from your smartphone do you check to see if the site is secured?	66%	34%
6. Have you shared your smartphone with other people?	21%	79%

Confirmatory Factor Analysis

Confirmatory factor analysis (CFA) was the next step in the data analysis phase. The purpose behind conducting CFA is to confirm or disconfirm support for an *a priori* theory (Mertler & Vannatta, 2013). Steps involved in CFA are model specification, model estimation, review of the results, and sometimes model respecification. (Brown & Moore, 2015).

For model specification, an initial CFA model (Appendix F), based on the theoretical model (Figure 2) described in Chapter 3, was developed in AMOS. The diagram is depicted using latent factors (ovals), with observed, measured items (rectangles) on the latent factors, and measurement errors (circles) set on each observed item. AMOS requires that one of the regression loadings for each latent variable is set to a restrained regression weight of 1.00 in the model in order to tie the other measured items to this specific reference point (Kline, 2005). Finally, covariances between each of the latent factors were set in order to estimate the relationship between the latent factors (Brown & Moore, 2015).

Model estimation, according to Brown and Moore (2015), "is an analysis used to find a set of parameter estimates that produces a predicted variance-covariance matrix that best reproduces the input variance-covariance matrix" (p. 12). Maximum likelihood (ML) estimator was used during model estimation as this "maximizes the probability of observing the available data if the data were collected again from the same population" (Brown & Moore, 2015, p. 14). After initial computation of the CFA, all factor loadings of the observed factors on the latent factors were .70 or higher. However, the results of the model fit estimation conducted on the initial CFA model did not result in acceptable

model fit indices (Table 8). The ratio of Chi-Square (X^2) to degrees of freedom (df) (reported as CMIN/DF) is 3195.70/845 = 3.782. This exceeds the established threshold of CMIN/DF $\leq$ 3 by Schumacker and Lomax (2010) and is indicative of poor model fit. Other commonly reported model fit indices produced by the initial model, also had poor results. Goodness of fit (GFI) and adjusted goodness of fit (AGFI) at .61 and .57, respectively, came in below standard thresholds of >.9 and >.8, respectively. Root mean square of approximation (RMSEA) at 0.10 was right on the threshold of <0.10. Standard root mean residual (SRMR) at .04 indicates excellent model fit. However, caution must be exercised in reporting model fit based on specific model fit indices. Hooper, Coughlan, and Mullen (2008) noted that GFI and AGFI are sensitive to sample sizes. In large sample sizes and complex models, GFI and AGFI are almost always underestimated. This study uses a complex model with eight latent factors and has a sample size of 256. Therefore, RMSEA and SRMR are better model fit indices for a study of this complexity and sample size. Considering all indices combined, this model can only be considered a fair fit.

Table 8. Overall Fit Indices for Initial CFA Model

Goodness of Fit Measure	Recommended Value	Values from this study
Chi-square (X2)		3195.70
Degrees of freedom (df)		845
Chi-square/df (CMIN/DF)	<3.00	3.782
Goodness-of-Fit Index (GFI)	>.90	0.617
Adjusted Goodness-of-Fit Index (AGFI)	>.80	0.571
Normalized-Fit Index (NFI)*	≥.90	0.835
Tucker-Lewis Index (TLI)*	≥.90	0.864
Comparative-Fit Index (CFI)*	≥.90	0.873
Standardized Root Mean Square Residual (SRMR)	<.10	0.044
Root Mean Square of Approximation (RMSEA)	<.10	0.104
Parsimonious Goodness-of-Fit Index (PGFI)	higher the better	0.551
Parsimonious Normed-Fit Index (PNFI)	higher the better	0.781

Source: Levy and Green (2009); Schumacker and Lomax (2010)
* Values only important in SEM analysis (Hooper, Coughlan, & Mullen, 2008)

Reliability and Validity

The most commonly evaluated and reported reliability and validity indices are composite reliability (CR), average variance extracted (AVE), maximum shared variance (MSV), and average shared variance (ASV) (Hair, Black, Babin, & Anderson, 2010). CR is reported for reliability, AVE is reported for convergent validity, and MSV, ASV, and the square root of AVE are reported for discriminate validity. The thresholds for these indices are depicted in Table 9.

Table 9. Reliability and Validity Thresholds

Measure	Threshold
CR	>.70
AVE	>.50
MSV	MSV < AVE
ASV	ASV < AVE
√AVE	> inter-construct correlations

Table 10 provides the reliability and validity values for the estimated model for this study. All CR scores were greater than .9, all AVE scores were greater than .5, MSV and ASV scores were lower than AVE and the square root of AVE exceeded the scores of all inter-construct correlations. Since all scores exceeded the established thresholds, it was determined that the criteria had been met in order to determine construct reliability as well as convergent and discriminate validity (Kaartina et al., 2015).

Table 10. Reliability and Validity Table with Square Root AVE on Diagonal

	CR	AVE	MSV	ASV	VA	IT	PT	TA	RA	MISE
VA	0.939	0.795	0.659	0.389	0.892					
IT	0.981	0.928	0.576	0.134	0.130	0.963				
PT	0.981	0.929	0.576	0.172	0.248	0.759	0.964			
TA	0.971	0.871	0.659	0.363	0.812	0.120	0.197	0.934		
RA	0.968	0.882	0.613	0.343	0.783	0.096	0.222	0.766	0.939	
MISE	0.928	0.683	0.593	0.351	0.770	0.233	0.366	0.718	0.676	0.826

Model Respecification

Model respecification was conducted due to the poor model fit indices reported in the initial model evaluation. The first step in the model respecification process was to view the standardized residuals matrix. Any value over 1.96 indicates factor cross loadings of the observed items onto multiple factors (Brown & Moore, 2015). There were four observed items (MISE 1, MISE 6, VA 2, and TA 7) with values over 1.96 in the standardized residual matrix and removed from further analysis.

The second step in the model respecification process was to visually inspect the modification indices (MI) matrix for any values over 20 between the error terms within the same factor. Modification indices are computed values that reflect how much Chi-square over degrees of freedom (CMIN/DF) will decrease by covarying the error terms within the same factor (Arbuckle, 2007; Brown & Moore, 2015). This was an iterative

process until all MI were within a reasonable level of less than 20. A significant amount of time was not spent on reducing Chi-square values since Chi-square is particularly sensitive to larger sample sizes and almost always results in rejecting the hypothesis while conducting CFA (Chan, Lee, Lee, Kubota & Allen, 2007; Kline, 2005; Hox, 1997).

The model respecification resulted in a moderate increase in model fit as compared to the initial CFA model (Table 11). CMIN/DF at 1529.67/670 = 2.283 indicates acceptable model fit despite the tendency of CMIN/DF to be overestimated for model fit. All other fit indices indicate acceptable model fit with the exception of GFI and AGFI. SRMR at .03 is below the threshold of <.10. Finally, RMSEA of .07 is also below the threshold of <.10. Therefore this model (Appendix G) is considered the final CFA model and deemed acceptable.

Table 11. Overall Fit Indices for Modified CFA Model

Goodness of Fit Measure	Recommended Value	Values from this study
Chi-square (X2)		1529.67
Degrees of freedom (df)		670
Chi-square/df (CMIN/DF)	<3.00	2.283
Goodness-of-Fit Index (GFI)	>.90	0.768
Adjusted Goodness-of-Fit Index (AGFI)	>.80	0.730
Normalized-Fit Index (NFI)*	≥.90	0.913
Tucker-Lewis Index (TLI)*	≥.90	0.943
Comparative-Fit Index (CFI)*	≥.90	0.949
Standardized Root Mean Square Residual (SRMR)	<.10	0.0358
Root Mean Square of Approximation (RMSEA)	<.10	0.071
Parsimonious Goodness-of-Fit Index (PGFI)	Higher the better	0.659
Parsimonious Normed-Fit Index (PNFI)	Higher the better	0.825

Source: Levy & Green (2009) and Schumacker & Lomax (2010)
* Values only important in SEM analysis (Hooper, Coughlan, & Mullen, 2008)

Structural Equation Modeling

The following three steps were involved in SEM process for this study: Model specification, model estimation, and proposition testing. The majority of model specification was already completed in the CFA phase of this study. Only slight modification had to occur from the original model specification. First, the dependent factors of security practices (SP) and security behaviors (SB) had to be included in the SEM model. The DVs were not originally included in the CFA model, because the factors are both dichotomous and formative. Additionally, since the DVs are formative, they are considered observed factors, thus the DVs are represented as rectangles in the SEM model. After adding the dependent factors, causal paths were established between the IVs, MVs and DVs.

After specifying the SEM model (Appendix H) to mirror the proposed theoretical model, model estimation was conducted using ML. The initial fit indices (Table 12) show acceptable model fit. NFI at .90, TLI at .93, and CFI at .94 all meet or exceed ≥.90 threshold. CMIN/DF at 2.28 falls below the <.30 threshold. SRMR and RMSEA also fall within acceptable parameters of <.10.

Table 12. Initial SEM Goodness of Fit Indices

Goodness of Fit Measure	Recommended Value	Values from this study
Chi-square (X2)		1719.72
Degrees of freedom (df)		753
Chi-square/df (CMIN/DF)	<3.00	2.28
Normalized-Fit Index (NFI)*	≥.90	0.90
Tucker-Lewis Index (TLI)*	≥.90	0.93
Comparative-Fit Index (CFI)*	≥.90	0.94
Standardized Root Mean Square Residual (SRMR)	<.10	0.09
Root Mean Square of Approximation (RMSEA)	<.10	0.07
Parsimonious Goodness-of-Fit Index (PGFI)	Higher the better	0.66
Parsimonious Normed-Fit Index (PNFI)	Higher the better	0.83

Source: Levy and Green (2009); Schumacker and Lomax (2010)
* Values only important in SEM analysis (Hooper, Coughlan, & Mullen, 2008)

Initial SEM analysis also revealed good significance and relationships between most of the factors. The significant factors and relationships are: VA → MISE (β .58, p≤.001), TA →MISE (β .23, p≤.01), PT→ MISE (β .15, p≤.01), MISE → SP (β .27, p≤.001), and MISE → SB (β .21, p≤.001). Table 13 provides a summary of the regression weights and path coefficients.

Table 13. Initial SEM Regression Weights and Path Coefficients (β)

Regression Weights: (Group number 1 – Default model)							
			Estimate	**S.E.**	**C.R.**	**P**	**Path (β)**
IT	<---	MISE	-.009	0.056	-.153	.879	-.01
PT	<---	MISE	0.163	0.062	2.639	p <.01**	.15
MISE	<---	RA	.035	.055	.647	.517	.05
MISE	<---	VA	.547	0.084	6.50	p ≤.001***	.58
MISE	<---	TA	.170	0.060	2.850	p <.01**	.23
SP	<---	MISE	.338	0.080	4.234	p ≤.001***	.27
SB	<---	MISE	.165	0.050	3.302	p ≤.001***	.21
Sig. * p <.05; **p <.01; *** p <.001							

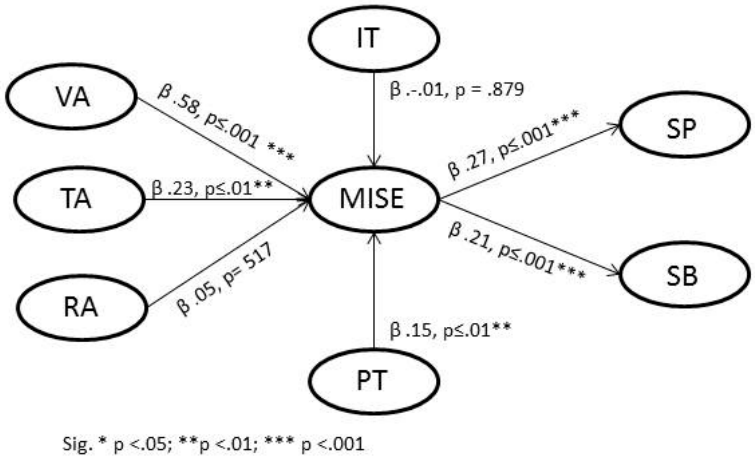


Figure 4. Initial SEM results

Despite overall acceptable model fit and significance between a majority of the factors, Schumacker and Lomax (2010) discussed the importance of testing different models by changing the interactions between the factors and comparing the different models. Although initial SEM specification indicated acceptable model fit as well as causal relationships and significance between a majority of the factors, this study undertook the recommendation of Schumacker and Lomax (2010). The purpose of conducting model respecification was to investigate whether good relationships and significance could be accomplished between all the factors, while also maintaining acceptable model fit.

Each model iteration consisted of various SEM path manipulations. The first model respecification (Appendix I) was to test direct effects, without the mediating factor of MISE, of the exogenous factors on the endogenous factors as some studies suggest (Chen et al., 2008; Furnell, 2008; Kumar et al., 2008). For the first model respecification, the MV was moved to an IV. After computation of the model without mediating effects, subsequent model respecification included MISE as a mediating factor as postulated in this study. Results of the model comparisons will be discussed in Chapter 5.

After several iterations of model respecification, a final model (Appendix J) was reached. This final model does vary from the originally proposed theoretical model (Figure 2) in Chapter 3 by the removal of IT and PT. IT and PT showed no significance or relationship with any of the other proposed factors. The new model resulted in slightly better model fit (Table 14), good relationships, and significance between all the factors (Table 15). NFI at .90, TLI at .94, and CFI at .94 all exceed the thresholds of ≥.90. Additionally, the following significance and path coefficients are the result of the final SEM model: RA → VA (β .34, p ≤.001), TA → VA (β .57, p ≤.001), VA → MISE (β .83, p ≤.001), MISE → SP (β .28, p ≤.001), and MISE → SB (β .22, p ≤.001).

Table 14. Final SEM Goodness-of-Fit Indices

Goodness of Fit Measure	Recommended Value	Values from this study
Chi-square (X2)		1732.43
Degrees of freedom (df)		756
Chi-square/df (CMIN/DF)	<3.00	2.29
Normalized-Fit Index (NFI)*	≥.90	0.90
Tucker-Lewis Index (TLI)*	≥.90	0.94
Comparative-Fit Index (CFI)*	≥.90	0.94
Standardized Root Mean Square Residual (SRMSR)	<.10	0.09
Root Mean Square of Approximation (RMSEA)	<.10	0.07
Parsimonious Goodness-of-Fit Index (PGFI)	Higher the better	0.67
Parsimonious Normed-Fit Index (PNFI)	Higher the better	0.83

Source: Levy & Green (2009) and Schumacker & Lomax (2010)
* Values only important in SEM analysis (Hooper, Coughlan, & Mullen, 2008)

Table 15. Final SEM Regression Weights and Path Coefficients (β)

Regression Weights: (Group number 1 – Default model)							
			Estimate	**S.E.**	**C.R.**	**P**	**Path (β)**
VA	<---	RA	0.276	0.050	5.519	p ≤.001***	.34
VA	<---	TA	.447	.052	8.663	p ≤.001***	.57
MISE	<---	VA	.771	0.065	11.771	p ≤.001***	.81
SP	<---	MISE	.335	0.080	4.204	p ≤.001***	.27
SB	<---	MISE	.165	0.050	3.302	p ≤.001***	.21
***Sig. p ≤.001							

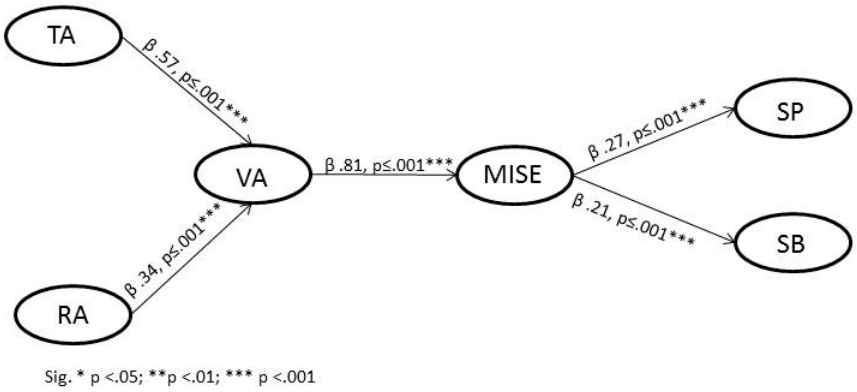


Figure 5. Final SEM results

Proposition Testing

The final step in the SEM analysis was to test the original seven propositions outlined in Chapter 3 in order to answer the original research question: Do the factors of Mobile InfoSec self-efficacy, vulnerability awareness, threat awareness, risk awareness, institutional trust, and party trust demonstrate high reliability and validity in determining smartphone users' security practices and security behaviors? In order to answer this question, those seven propositions were developed and analyzed using SEM techniques.

The first proposition (P1) was: Vulnerability awareness positively impacts mobile information security self-efficacy. SEM analysis determined that there was a correlation and significance between the two factors (β .58, $p \leq .001$). Therefore this proposition is supported.

The second proposition (P2) was: Threat awareness positively impacts mobile information security self-efficacy. SEM analysis determined that there was a correlation and significance between the two factors (β .23, $p \leq .01$). Therefore, this proposition is supported.

The third proposition (P3) was: Risk awareness positively impacts mobile information security self-efficacy. SEM analysis determined that there was a very small correlation and no significance between the two factors (β .05, p = .517). Therefore, this proposition is not supported.

The fourth proposition (P4) was: Institutional trust positively impacts mobile information security self-efficacy. SEM analysis determined that there was nearly no correlation and no significance between the two factors (β -.01, p = .879). Therefore, this proposition is not supported.

The fifth proposition (P5) was: Party trust positively impacts mobile information security self-efficacy. SEM analysis determined that there was a weak correlation, but significance between the two factors (β .15, p ≤.01). Therefore, this proposition is not supported.

The sixth proposition (P6) was: Mobile information security self-efficacy positively impacts security practices. SEM analysis determined that there was a correlation and significance between the two factors (β .27, p ≤.001). Therefore, this proposition is supported.

The seventh proposition (P7) was: Mobile information security self-efficacy positively impacts security behaviors. SEM analysis determined that there was a correlation and significance between the two factors (β .21, p ≤.001). Therefore, this proposition is supported. Table 16 provides a summary of outcomes of the propositions.

Table 16. Summary Proposition Outcome

Proposition	Significance	β	Supported
P1	P<.001***	.58	Yes
P2	P<.01**	.23	Yes
P3	p.517	.05	No
P4	p.879	-.01	No
P5	p.<01**	.15	No
P6	P<.001***	.27	Yes
P7	p.<001***	.21	Yes

Summary

This section presented the results of the data analysis of CFA-SEM. The purpose of the CFA-SEM was to test the validity, reliability, and model fit of these factors as well as conduct SEM analysis to analyze the relationships between the factors within the domain of smartphone security.

The initial CFA model did not exhibit acceptable model fit, therefore model respecification had to be conducted. In order to achieve better model fit, error terms within the same latent factors that exhibited high modification indices (above 20) were covaried. Additionally, the standardized residuals matrix was evaluated to determine if any of the measured values were greater than an absolute value of 1.96, which indicates factor cross loading. There were four items identified (MISE 1, MISE 6, TA 7, and VA 2) with values of 1.96 or greater and removed from further analysis. Once the model respecification was complete, acceptable model fit (Appendix G) was achieved.

The next step in the data analysis was SEM. The initial run of SEM analysis produced strong correlations and significance between the majority of the factors. There were four out of seven factor relationships that were correlated and significant (VA → MISE, TA → MISE, MISE→ SP, MISE → SB). Despite this finding, model respecification was conducted to determine whether strong relationships and significance could be accomplished between all the factors, while also maintaining acceptable model fit. This model respecification consisted of modifying causal paths between the factors. The model respecification was successful and resulted in acceptable model fit as well as significance and strong relationships between all the factors.

Finally, analysis of the propositions was conducted. Based on the initial SEM analysis, four of the original propositions were supported, while the remaining three were not supported. Model respecification identified potential additional propositions that will be discussed in the Recommendations section of Chapter 5.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Introduction

The goal of this study was to test previously validated factors from the traditional computer security domain and their applicability in the context of smartphone security. This chapter presents the conclusions derived from this study. Additionally, limitations and implications to smartphone security will be discussed. Finally, future research and recommendations will be discussed followed by a summary of the research.

Conclusions

This study argued that inappropriate security behaviors and practices of smartphone users are leading to the exposure and compromise of sensitive information. A review of extant literature revealed a significant gap in smartphone security, especially pertaining to smartphone users and socio-cognitive factors. As such, this study set out to find socio-cognitive factors, through literature reviews, that could potentially have an effect on security practices and behaviors of smartphone users.

The result of this literature review revealed user awareness of threats, risks, and vulnerabilities, user trust in the smartphone application developers and smartphone application stores, as well as self-efficacy could potentially play a role in determining the security practices and behaviors of smartphone users. From this discovery, the following research question was developed: Do the factors of mobile infosec self-efficacy,

vulnerability awareness, threat awareness, risk awareness, institutional trust, and party trust demonstrate high reliability and validity in determining smartphone users' security practices and security behaviors? In order to answer this research question, seven propositions were developed and tested using CFA-SEM analysis techniques based on the data collected from 256 survey responses. The research question and propositions were derived from an extensive literature review. However, the path correlations in the theoretical model are original to this study. Some studies claimed that the specific factors were directly attributable to security practices and behaviors, while some argued the factors were significantly attributable to self-efficacy, which in turn affected security practices and behaviors. This study chose to use self-efficacy as a mediating variable.

Huang, et al. (2010) asserted that risk, trust, and vulnerability awareness all have a significant part in determining a user's security practices. Additionally, Chen et al. (2011) stated that risk awareness was significant in determining self-efficacy, security practices, and behaviors. Also, Furnell (2008) noted that users often times know the threats, but it does not reflect in their behaviors. Additionally, Furnell also noted that there is a significant correlation between awareness and self-efficacy. Conversely, Crossler and Belanger (2006) stated awareness had no impact on self-efficacy.

Lacohee et al. (2006) argued that trust is not a factor in whether or not a user conducts online transactions, such as purchasing or downloading smartphone software from the smartphone application store. Lachoee et al. further argued that despite a certain level of trust a user may have gained they will still conduct risky online behaviors. Mylonas et al. (2013) argued that the majority of smartphone users have trust in the application stores, but are not aware if the applications are safe. Chin et al. (2012), claim

trust is a factor in both self-efficacy as well as security practices. Finally, Ba and Pavlou (2002) as well as Shin (2010) also claim trust is significant factor in determining users' security practices.

The initial CFA model computation resulted in poor model fit indices but strong factor loadings. Due to the poor model fit indices, the model had to be modified. Modification included covarying the error terms (also sometimes referred to as residuals) for any modification indices over 20 and eliminating measured items over 1.96 as reported in the standardized residuals matrix. The modified model resulted in acceptable fit indices, strong factor loadings, and passed AVE tests indicating discriminate and construct reliability was not an issue. As such, the model was deemed acceptable and ready to be analyzed using SEM techniques.

The initial SEM model showed good correlations and significance between a majority of the factors. RA had very little correlation with MISE and did not indicate any significance. On the other hand, both VA (β.23, $p \leq .001$) and TA (β.58, $p \leq .01$) showed good correlations and significance to MISE. Therefore, it can be stated that VA and TA, individually, are significant predictors of MISE and therefore propositions 1 and 2 are supported. These findings fall in line with the works of Huang et al. (2010), Chen et al. (2011) and Furnell (2008). However, this is in stark contrast to Crossler and Belanger's (2006) assertions that awareness has no impact on self-efficacy.

One must understand that risk, threats, and vulnerabilities all work hand in hand. Knowing just one of them will not increase overall information security posture or knowledge. For example, one cannot simply understand that viruses exist without understanding the vulnerability the virus is going to exploit. It has been noted in

information security literature that risk is the product of threats X vulnerabilities (Cox, 2008). However, that is concerning impact factor, not from a socio-cognitive perspective. This study tested Cox's (2008) theory and found that, from a socio-cognitive perspective, vulnerability awareness is actually a product of risk and threats. As such, in the final SEM model, it was found that RA (β .34, $p \leq .001$) and TA (β .57, $p \leq .001$) had very strong correlations in determining VA, which in turn had a strong correlation and significance in determining MISE (β .83, $p \leq .001$). Therefore, risk, threats, or vulnerabilities cannot be studied in isolation to determine their significance on MISE.

IT showed very little correlation or significance on MISE. On the other hand, PT did show a weak correlation, but significance on MISE (β.15, $p \leq .01$). Thus, it can be determined that users put more emphasis in trusting the smartphone application developers than they do the smartphone application market place. The PT finding could be contributable to user reviews, peer pressure, or popularity of the application within the marketplace. Moreover, IT could also possibly not be attributable because the users have no other choice but to trust the marketplace because they cannot get the software from anywhere else; therefore there is no interest in trusting the marketplace. Thus, it can be stated that proposition 4 and 5 are not supported. The final SEM model respecification did not produce any significantly different results from the initial SEM model as it pertains to trust factors. This finding falls in line with the works of Mui et al. (2002), Mylonas et al. (2013) and Verhagen et al. (2006) which asserts that users are forced to develop a level of trust by default because they have no other options. It should be noted that very little emphasis, if any, should be placed on this PT to MISE finding due to the weak correlations between the two factors.

Finally, MISE showed strong significance and correlations to both SP (β.27, p≤.001) and SB (β.21, p≤.001). Therefore, it can be stated that MISE is a significant predictor of SP and SB and propositions 6 and 7 are supported. This finding falls in line with the works of Ball (2008), Chen et al. (2011), Crossler and Belanger (2006), and Rhee et al. (2008).

In addition to the initial and final SEM model respecification, another one was created to test the direct effects of the exogenous factors to the endogenous factors. Model fit was not analyzed in this iteration of the model respecification as the sole purpose of this specific model respecification was not to test for model fit, but to test the direct effects of the exogenous factors on the endogenous factors without any mediating effects. According to the direct effect SEM analysis it was found that RA (β-.26, p≤.05), VA (β.29, p≤.05), TA (β.38, p≤.001), all had good correlations and significance in determining security practices. IT had very little correlation to SP and there was not any significance between the two factors. Again, as with both the initial SEM model as well as the final SEM model, there was some weak correlation between PT and SP, but there was not any significance between the two factors. Therefore, it can be stated that neither of the trust factors have any significance nor correlation to security practices, security behaviors, or self-efficacy.

It is interesting to note that RA has an inverse relationship to SP. Although a user has increased RA, they still do not properly protect themselves by installing the appropriate protective measures such as anti-virus software. This could be an indicator that the users feel confident enough that they can avoid the risks associated with using their smartphone. It is also interesting to note that the users who claim to have increased

RA do not change their risky behaviors despite their lack of security protection. Therefore, even though they are aware of the risks, they still perform risky behaviors yet do not properly protect themselves (i.e. risk acceptance).

The purpose behind this research was to answer the following research question: Do the factors of mobile infosec self-efficacy, vulnerability awareness, threat awareness, risk awareness, institutional trust, and party trust demonstrate high reliability and validity in determining smartphone users' security practices and security behaviors? After conducting CFA-SEM analysis and testing the seven original propositions to answer that question it can be determined that, mobile infosec self-efficacy, vulnerability awareness, threat awareness, and risk awareness all demonstrate high reliability and validity in determining smartphone user's security practices and behaviors. Although, party trust and institutional trust demonstrated high reliability and validity, they did not have any correlation or significance in determining security practices or behaviors.

Limitations

One limitation to this study was the medium used to obtain participants. Facebook® and LinkedIn® were used as the marketing mechanism to gather the participants. This could be a limiting factor in that the respondents are not truly representative of the population. Additionally, as noted in the demographics, more women, although not significantly more, responded compared to men. There is a possibility that the results could be slight skewed one way or the other from that of the overall population.

Another potential limitation is the data collection method. There is a possibility that the data captured may not be a true representation of the respondent's beliefs. This

could possibly be attributable to the lack of comprehension of the questions or the definitions. There could have also been unengaged responses (response set) that were undetectable to the naked eye and still included in the data analysis.

Finally, another limitation to this research pertains to its generalizability. This study did not undertake any moderating effect analyses based on information security background. The number of respondents with information security backgrounds were minimal and not enough to conduct a thorough analysis. Therefore, the results of this research may not be generalizable to the entire population and may be more applicable to people without information security backgrounds.

Implications

There is currently a significant gap in smartphone security literature. This is partly due to the fact that smartphones are still a relatively new technology and literature has yet to catch up to the rapid advancement of smartphones (Mylonas et al., 2013; Park & Chen, 2007). Therefore, this research has started to address this gap and examined factors that have shown to have an influence on user's security behaviors and practices. This research is important to smartphone security literature because the proliferation of smartphone devices is rapidly increasing the risk of data exposure (Van Bruggen et al., 2013). This study enhanced the smartphone security body of knowledge by attempting to bridge the gap between traditional computer security to smartphone security. There have been some studies on smartphone security, but very few have addressed the user-focused socio-cognitive factors that drive the security practices and behaviors of smartphone users. This research addressed that gap by assessing the applicability of previously validated

constructs from the domain of traditional computer security that was found to have an impact on computer security practices and behaviors, to smartphone security.

Self-efficacy was one of the first factors identified as having a potential impact on predicting security practices and behaviors of smartphone users. Self-efficacy was first discovered by Bandura (1977). It was later adopted by Compeau and Higgins (1995) and applied to computers. Later Eastin and Rose (2000) adopted this factor and applied it to the Internet. This research empirically assessed the reliability and validity of self-efficacy in predicting user's security practices and behaviors of smartphone users.

Crossler and Belanger (2006) stated awareness had no impact in predicting computer self-efficacy. Crossler and Belanger also stated that self-efficacy was significant in determining the overall adoption rate of security tools such as anti-virus software. The results of this research revealed the awareness does in fact have an impact on determining self-efficacy, which in turn has predictive significance on security practices. Rhee et al. (2009) argued that very little attention has been given to socio-cognitive factors as it pertains to information security. Rhee et al. found that self-efficacy does play a role in determining the security posture of computers users. Chin et al. (2012) conducted a study that attempted to gain a deeper insight into smartphone user's perceptions about smartphone security. They found that users are less willing to conduct certain actions such as online banking and online shopping. Chin et al. noted that self-efficacy could be a significant factor that drives these actions and called for future research on smartphone self-efficacy. This research answered that call and empirically assessed self-efficacy and found that it is a significant factor in determining the security posture of smartphone users.

Literature reviews conducted on information security has shown that there is common agreement that awareness is an important component in how users protect themselves. There is very little literature in smartphone information security. Mylonas et al. (2012) noted that smartphone security awareness was significantly lacking and argued that studies on smartphone security awareness is needed. Huang et al. (2010) noted that most literature on information security only focuses on a single awareness factor. Huang et al. argued that more than one factor needs to be studied in order to gain a deeper understanding of security practices and behaviors. Huang et al. studied risk, threat, and vulnerability awareness and found that all three factors are important factors in determining a user's belief and ability to properly protect themselves from information security breaches. Albrectsen (2007) noted that users have very little awareness of risk. Chin et al. (2012) also state that smartphone users lack information security awareness. To address the gap in literature pertaining to smartphone security awareness, this study assessed risk, threat, and vulnerability awareness. The results of this assessment determined that vulnerability and threat awareness have predictive significance in determining self-efficacy. It was discovered that risk awareness did not have a direct impact on self-efficacy. Two possible ways this can be interpreted are: 1) Users are in fact not aware of the risks associated with smartphones as claimed by Albrectsen and Chin et al. or 2) as previously noted, risk is a product of threats X vulnerabilities and risk should only be assessed in such a manner.

Trust has been studied in an attempt to gain a deeper understanding of consumer purchasing habits (Pavlou & Gefen, 2004). Trust is at the root of every transaction and is an important topic of research in many fields (Mui et al., 2002). Smartphone applications

are delivered to consumers through what is called a marketplace. Unfortunately, users have to develop a level of blind trust of these marketplaces and trust that the marketplace will only have trustworthy applications available for download (Verhagen et al., 2006). A literature review revealed that there is also a gap in literature pertaining to trust as it relates to smartphone applications and application marketplaces. Chin et al. (2012) found that users are less willing to conduct online transactions on their smartphones which was attributable to the lack of trust in the application marketplace and smartphone applications themselves. Lacohee et al. (2006) conducted a study on how users perceive trust in executing online transactions. Lacohee et al. found that if the user could somehow shift the burden of risk, such as using a credit card and putting the risk on the credit card company, they are more likely to complete the transaction. Mylonas et al. (2013) found that users were completely unaware if applications were trustworthy. Finally, Shin (2010 conducted a study on the effects of trust in using social networking sites. Shin found that trust was a factor in determining self-efficacy. This study addressed the smartphone trust literature gap by empirically assessing both institutional trust (marketplace) and party trust (applications). The results of this research revealed that trust was not a significant predictor of self-efficacy, nor did it have any direct significance in determining security practices or behaviors. A possible interpretation of this finding is that trust is irrelevant in the context of smartphones because users can only get their smartphone software from one place. Therefore, the user has no choice but to trust the marketplace and the developers.

In summary, a total awareness of risk, threat, and vulnerabilities combined are significant predictors of self-efficacy, which in turn has predictive significance in

determining smartphone user's security practices and behaviors. Trust on the other hand, was found to have no significance in determining any of the factors in this research.

Recommendations

This study found that and increased awareness in risks and threats combined, increases awareness of the specific vulnerabilities. With that, organizations need to take a holistic approach when educating their employees. Organizations cannot focus on risk, threats, or vulnerabilities in isolation. Users need to be educated on all factors that may lead to sensitive information disclosure.

Future research in smartphone security needs to continue to be explored. As it currently stands, very little research on smartphone security exists. This study found that there is an intricate relationship between risk, threat, and vulnerability awareness and that an increased awareness in just one of these categories will not have an impact on a user's security practices and behaviors. Cox (2008) noted that risk is the product of threats X vulnerabilities X impact. However, Cox's finding is based on an impact factor. In other words, as threats become more powerful, the vulnerabilities more abundant, then the greater the risk impact will be. This study found that on a socio-cognitive level, vulnerability awareness is the product of risk and threat awareness. Future research should measure impact factor awareness and its significance in determining security practices and behaviors. Additionally, future research should focus on a baseline critical ratio of awareness factors before awareness can be deemed effective.

Another finding of this study was that risk had an inverse relationship on security practices and no impact on security behaviors. Future research should investigate why

users exhibit a certain level of risk acceptance, rather than modify their security behaviors and protect themselves with the appropriate security software such as antivirus software.

Finally, future research should also investigate moderating factors such as experience, gender, or information security backgrounds. Investigating these moderating factors may lead to new discoveries of additional factors that need to be considered when devising a smartphone security plan.

Summary

The proliferation of smartphone devices is introducing new IS risks, which if not properly mitigated through appropriate security practices and behaviors, can result in the exposure of sensitive data (Anderson et al., 2008; Chin et al., 2012; Furnell et al., 2008; Jones & Heinrichs, 2012; Landman, 2010; Van Bruggen at al., 2013). The exposure of this sensitive data can have catastrophic effects both personally and from an organizational perspective. From the personal perspective, sensitive information exposure can lead to identity theft. Organizationally, sensitive data exposure can lead to the release of trade secrets or insider information that can reduce or eliminate competitive advantage. An organizational breach can also lead to the release of consumer information which, again in turn, can lead to identity theft of an individual.

The main research question this study addressed was: Do the factors of Mobile InfoSec self-efficacy, vulnerability awareness, threat awareness, risk awareness, institutional trust, and party trust demonstrate high reliability and validity in determining smartphone users' security practices and security behaviors? The purpose of this study was to conduct confirmatory factor analysis (CFA) to test the validity, reliability, and model fit of these factors as well as conduct structural equation modeling (SEM) analysis

to analyze the relationships between the factors within the domain of smartphone security.

In order to answer this research question a survey was developed and distributed to a five-member expert panel to ensure clarity and face value validity of the constructs. After receiving feedback from the expert panel, the survey was updated to change the minor errors noted in the feedback. The minor errors noted in the expert panel feedback consisted of only spelling errors and slightly modifying the definitions to produce more clarity. The survey was then distributed to a population base of 539 people throught LinkedIn® and Facebook® with a response rate of 275 people (50.6%).

Once the survey was turned off, pre analysis data screening was conducted to search for response set (unengaged responses), missing data, normality, multicollinearity, and demographics. There were a total of 13 unengaged responses that were thrown out of further data analysis. There was not any missing data. There were not any univariate outliers. However, six multivariate outliers were identified and removed before conducting further analysis. This resulted in 256 responses available for final analysis.

The first step in the data analysis portion of this study was to test for model fit of the proposed model using CFA in order to determine if the model was acceptable. The initial CFA model did not produce acceptable goodness of fit indices. Thus, the initial model was deemed not acceptable. However, as part of the CFA technique, the researcher needs to further evaluate additional items such as modification indices and the standardized residual covariance matrix to ensure there are not any redundancies among the latent factors. After reviewing the additional indices, four measured items were removed from the latent factors as well as covarying some of the unobserved error terms

(sometimes referred to as residuals) of the latent factors. After the second iteration of CFA was conducted the model fit indices significantly improved with all model fit indices' minimums being met or exceeded. Therefore, the second model was deemed an acceptable model fit, meaning it was suitable for SEM evaluation.

The initial SEM mode analysis resulted in good model fit as well as good correlations and significance between four of the factors. These four factors were: VA → MISE (β .58, p ≤.001), TA → MISE (β .23, p ≤.01), MISE→ SP (β .27, p ≤.001), and MISE → SB (β .21, p ≤.001). Although the initial SEM (Appendix H) model exhibited good model fit indices as well as correlations and significance between four out of the seven factors, model respecification was conducted in an attempt to see if there were any other causal relationships that could be uncovered, while still maintaining good model fit.

The SEM model respecification (Appendix J) analysis discovered that risk awareness and threat awareness were antecedents to vulnerability awareness. It was found that RA (β .34, p ≤.001) and TA (β .57, p ≤.001) had very strong correlations in determining VA, which in turn had a strong correlation and significance in determining MISE (β .83, p ≤.001). This finding is an indicator that risk awareness, threat awareness, and vulnerability awareness work hand in hand and all need to be understood in order to raise awareness and self-efficacy. Some information security literature has noted that RA is a product of VA X TA and should all be analyzed together (for example Cox, 2008).

Another SEM model respecification (Appendix I) was done to test for direct effects of RA, TA, and VA on SP and SB. According to the direct effect SEM analysis it was found that RA (β-.26, p≤.05), VA (β.29, p≤.05), TA (β.38, p≤.001), all had good correlations and significance in determining security practices.

An interesting finding is that RA has an inverse relationship to SP. Although a user has increased RA, they still do not properly protect themselves by installing the appropriate protective measures such as anti-virus software. This could be an indicator that the user feels confident enough that they can avoid the risks associated with using their smartphone. It is also interesting to note that the users who claim to have increased RA do not change their risky behaviors despite their lack of security protection. Collectively, the user is willing to accept the risk and as noted in the Future Research section, this is cause for further investigation.

Finally, the main research question can be answered that Mobile InfoSec self-efficacy, vulnerability awareness, threat awareness, and risk awareness, demonstrate high reliability and validity in determining smartphone users' security practices and security behaviors. However, vulnerability awareness, threat awareness, and risk awareness are mediated by MISE when determining security practices and behaviors. Party trust and institutional trust demonstrated no significance in determining security practices or behaviors. These findings should give smartphone users and organizations insight into specific areas of focus in minimizing inappropriate security behaviors and practices of smartphone users. More specifically, users and organizations need to focus on all three factors of threats, risks, and vulnerabilities in order for there to have any impact on reducing inappropriate security behaviors and practices. Having an increased awareness of just one of the factors, showed very little impact in effecting security practices and behaviors of smartphone users.

Appendix A

Preliminary Survey Instrument

Item	Question	Scale						
		Totally not Confident						**Totally confident**
MISE 1	I feel confident in handling viruses on my smartphone?	1	2	3	4	5	6	7
MISE 2	I feel confident in handling spyware on my smartphone?	1	2	3	4	5	6	7
MISE 3	I feel confident understanding terms/words relating to smartphone information security?	1	2	3	4	5	6	7
MISE 4	I feel confident in learning the method to protect my smartphone?	1	2	3	4	5	6	7
MISE 5	I feel confident managing information stored in my smartphone?	1	2	3	4	5	6	7
MISE 6	I feel confident using different programs on my smartphone?	1	2	3	4	5	6	7
MISE 7	I feel confident learning advanced skills to protect my information and my smartphone?	1	2	3	4	5	6	7
MISE 8	I feel confident in getting help for problems related to the security of my information and my smartphone?	1	2	3	4	5	6	7
MISE 9	I feel confident using the user's guide when help is needed to protect my information and my smartphone?	1	2	3	4	5	6	7
MISE 10	I feel confident in updating security patches to my phones operating system?	1	2	3	4	5	6	7
MISE 11	I feel confident in switching security levels of my Internet browser on my smartphone?	1	2	3	4	5	6	7
		Totally Unaware						**Totally Aware**
VA 1	I am aware of the vulnerabilities related to streaming videos on smartphones?	1	2	3	4	5	6	7
VA 2	I am aware of the vulnerabilities related to phone calls on smartphones?	1	2	3	4	5	6	7
VA 3	I am aware of the vulnerabilities related to using social media on smartphones?	1	2	3	4	5	6	7
VA 4	I am aware of the vulnerabilities related to text messaging on smartphones?	1	2	3	4	5	6	7

VA 5	I am aware of the vulnerabilities related to email on smartphones?	1	2	3	4	5	6	7
VA 6	I am aware of the vulnerabilities related to making online purchase on smartphones?	1	2	3	4	5	6	7
VA 7	I am aware of the vulnerabilities related to online banking on smartphones?	1	2	3	4	5	6	7
VA 8	I am aware of the vulnerabilities associated with pictures and videos on smartphones?	1	2	3	4	5	6	7
VA 9	I am aware of the vulnerabilities related to surfing the Internet on smartphones?	1	2	3	4	5	6	7
		Totally Unaware						**Totally Aware**
TA 1	I am aware that smartphones are susceptible to virus attacks?	1	2	3	4	5	6	7
TA 2	I am aware that smartphones are susceptible to malware attacks?	1	2	3	4	5	6	7
TA 3	I am aware that smartphones are susceptible to phishing attacks?	1	2	3	4	5	6	7
TA 4	I am aware that smartphones are susceptible to spyware attacks?	1	2	3	4	5	6	7
TA 5	I am aware that smartphones are susceptible to surveillance attacks?	1	2	3	4	5	6	7
TA 6	I am aware that smartphones are susceptible to network attacks?	1	2	3	4	5	6	7
TA 7	I am aware that smartphones are susceptible to being used for identity theft?	1	2	3	4	5	6	7
		Totally Unaware						**Totally Aware**
RA 1	I am aware that an unauthorized person could view sensitive emails on unsecured smartphones?	1	2	3	4	5	6	7
RA 2	I am aware that an unauthorized person could view pictures on unsecured smartphones?	1	2	3	4	5	6	7
RA 3	I am aware that an unauthorized person could view personal contacts on unsecured smartphones?	1	2	3	4	5	6	7
RA 4	I am aware that an unauthorized person could view text messages on unsecured smartphones?	1	2	3	4	5	6	7
RA 5	I am aware that an unauthorized person could view financial information (credit cards/banking information) on unsecured smartphones	1	2	3	4	5	6	7

RA 6	I am aware that an unauthorized person can view sensitive documents on unsecured smartphones?	1	2	3	4	5	6	7
RA 7	I am aware that an unauthorized person could view Internet browsing habits on unsecured smartphones?	1	2	3	4	5	6	7
RA 8	I am aware that an unauthorized person could place costly phone calls from unsecured smartphones?	1	2	3	4	5	6	7
		Totally Disagree						**Totally Agree**
IT 1	The online app store ensures sellers are dependable?	1	2	3	4	5	6	7
IT 2	The online app store ensures sellers are reliable?	1	2	3	4	5	6	7
IT 3	The online app store ensures sellers are honest?	1	2	3	4	5	6	7
IT 4	The online app store ensures sellers are trustworthy?	1	2	3	4	5	6	7
		Totally Disagree						**Totally Agree**
PT 1	Sellers of applications in the online app store are generally dependable?	1	2	3	4	5	6	7
PT 2	Sellers of applications in the online App store are generally reliable?	1	2	3	4	5	6	7
PT 3	Sellers of applications in the online App store are generally honest?	1	2	3	4	5	6	7
PT 4	Sellers of applications in the online app store are generally trustworthy?	1	2	3	4	5	6	7
SP 1	Do you currently have anti-virus software on your smartphone?	Yes	No					
SP2	Do you currently have anti-spyware on your smartphone?	Yes	No					
SP3	Do you currently have email spam filter installed on your smartphone?	Yes	No					
SP4	Do you currently have a firewall installed on your smartphone?	Yes	No					
SP 5	Do you currently have any sort of encryption installed on your smartphone?	Yes	No					
SB 1	Do you use file sharing software (Kazaa, E-Donkey, etc.) from your smartphone?	Yes	No					
SB 2	Do you make backup copies of your files from your smartphone?	Yes	No					

SB 3	Do you have sensitive documents such as medical, financial, or banking stored on your smartphone?	Yes	No
SB 4	Does your smartphone require some form of authentication (PIN, Password, Pattern) before getting access?	Yes	No
SB 5	When transferring data on the Internet from your smartphone do you check to see if the site is secured?	Yes	No
SB 6	Have you shared your smartphone with other people?	Yes	No

DEM 1	Gender	M	F				
DEM 2	Age	18-24	25-34	35-44	45-54	44-64	65+
DEM 3	Highest education level completed?	High School	Some College	Associate degree	Bachelor Degree	Master Degree	PhD
DEM 4	Marital Status?	Single	Married	Divorced	Widowed		
DEM 5	Number of years using computers?	Nominal					
DEM 6	Number of years using smartphones?	Less than 5	5-10 yrs	10-15 yrs	15-20 yrs		
DEM 7	Do you have an information systems security background (i.e. training, education, certification)?	Yes	no				
DEM 8	Current smartphone operating system?	iOS	Android	Windows	Blackberry	Other	unk

Appendix B

Email to expert panel

Hello, My name is Joe Simpson and I am a Ph.D. student at the Graduate School of Computer and Information Sciences, Nova Southeastern University. I am in the final stages of my Ph.D . program and currently working on my dissertation. Before I begin data collection, I am assembling a team of members to form an expert panel to review my survey before distributing it for data collection. The reason you are receiving this email is I have identified you as a potential member of my expert panel due to your information security background and/or your terminal degree in information systems.

The title of my dissertation is Empirical Analysis of Socio-Cognitive factors that affect smartphone security practices and behaviors. I am using previously validated factors from existing literature in the traditional computer security domain and testing for applicability and validity in the smartphone context.

I ask that you take 20-30 minutes of your time to review my survey, located here https://docs.google.com/forms/d/1VB0T2Vlfi5FyMfGqreA86luSdBgC0J-scT3hkX2y194/viewform, to ensure there are no ambiguities, misspellings, redundancies as well as completeness of the survey.

If you have any questions regarding this study, you may contact me at js3185@nova.edu. Thanks for your consideration and I appreciate your assistance.

Best Regards,

Joe Simpson

Appendix C

Final Survey Instrument

Smartphone Survey

Dear participants,

I am a Ph.D. Candidate at Nova Southeastern University and am conducting a survey to gain a deeper understanding of smartphone users' security behaviors and practices as partial fulfillment of my Ph.D..

By participating in this survey you agree and understand that your responses are completely anonymous and responses cannot be traced to any individual. Additionally, you may exit this survey at anytime and your responses will not be recorded. Completing this survey indicates your voluntary participation in this study. By taking this survey you certify that you are over the age of 18 years old. The data collected in this survey may be published to facilitate further research on user security behavior on smartphones.

Please answer all the questions as honestly and accurately as possible. The data collected is completely anonymous.

Mobile InfoSec Self-Efficacy

A person's belief in their own abilities to exercise control over events and actions related to their mobile devices.

	Completely not Confident			Moderately Confident			Completely Confident
1. I feel confident in removing viruses from my smartphone. *	1	2	3	4	5	6	7
2. I feel confident in removing spyware from my smartphone. *	1	2	3	4	5	6	7
3. I feel confident understanding terms relating to smartphone information security. *	1	2	3	4	5	6	7
4.I feel confident in learning how to protect my smartphone. *	1	2	3	4	5	6	7
5. I feel confident managing data stored in my smartphone. *	1	2	3	4	5	6	7
6. I feel confident using different apps on my smartphone. *	1	2	3	4	5	6	7
7. I feel confident learning advanced skills to protect my information and my smartphone. *	1	2	3	4	5	6	7

8. I feel confident in getting help for problems related to the security of my information and my smartphone. *	1	2	3	4	5	6	7
9. I feel confident using the user's guide when help is needed to protect my personal information and my smartphone. *	1	2	3	4	5	6	7
10. I feel confident in updating security patches to my smartphone's operating system. *	1	2	3	4	5	6	7
11. I feel confident in switching security levels of my Internet browser on my smartphone. *	1	2	3	4	5	6	7

Vulnerability Awareness

A vulnerability is a flaw, loophole, oversight, or error that can be exploited to violate system security policy.

	Completely Unaware			Moderately Aware			Completely Aware
1. I am aware of the vulnerabilities related to watching videos on smartphones. *	1	2	3	4	5	6	7
2. I am aware of the vulnerabilities related to phone calls on smartphones. *	1	2	3	4	5	6	7
3. I am aware of the vulnerabilities related to using social media on smartphones. *	1	2	3	4	5	6	7
4. I am aware of the vulnerabilities related to text messaging on smartphones. *	1	2	3	4	5	6	7
5. I am aware of the vulnerabilities related to email on smartphones. *	1	2	3	4	5	6	7
6. I am aware of the vulnerabilities related to making online purchase on smartphone. *	1	2	3	4	5	6	7
7. I am aware of the vulnerabilities related to online banking on smartphones. *	1	2	3	4	5	6	7
8. I am aware of the vulnerabilities associated with pictures and videos on smartphones. *	1	2	3	4	5	6	7
9. I am aware of the vulnerabilities related to surfing the Internet on smartphones. *	1	2	3	4	5	6	7

Threat Awareness

A threat is a natural or manmade event that could have some type of negative impact on the organization.

	Completely Unaware			Moderately Aware			Completely Aware
1. I am aware that smartphones are susceptible to virus attacks. *	1	2	3	4	5	6	7
2. I am aware that smartphones are susceptible to malware attacks. *	1	2	3	4	5	6	7
3. I am aware that smartphones are susceptible to phishing attacks. *	1	2	3	4	5	6	7
4. I am aware that smartphones are susceptible to spyware attacks. *	1	2	3	4	5	6	7
5. I am aware that smartphones are susceptible to surveillance attacks. *	1	2	3	4	5	6	7
6. I am aware that smartphones are susceptible to network attacks. *	1	2	3	4	5	6	7
7. I am aware that smartphones are susceptible to being used for identity theft. *	1	2	3	4	5	6	7

Risk Awareness

Risk is a situation involving exposure to danger; the possibility that something unpleasant will happen.

	Completely Unaware			Moderately Aware			Completely Aware
1. I am aware that an unauthorized person could view sensitive emails on unsecured smartphones. *	1	2	3	4	5	6	7
2. I am aware that an unauthorized person could view pictures on unsecured smartphones. *	1	2	3	4	5	6	7
3. I am aware that an unauthorized person could view personal contacts on unsecured smartphones. *	1	2	3	4	5	6	7
4. I am aware that an unauthorized person could view text messages on unsecured smartphones. *	1	2	3	4	5	6	7
5. I am aware that an unauthorized person could view financial information (credit cards/banking information) on unsecured smartphone. *	1	2	3	4	5	6	7

6. I am aware that an unauthorized person can view sensitive documents on unsecured smartphones. *	1	2	3	4	5	6	7
7. I am aware that an unauthorized person could view Internet browsing habits on unsecured smartphones. *	1	2	3	4	5	6	7
8. I am aware that an unauthorized person could place costly phone calls from unsecured smartphones. *	1	2	3	4	5	6	7

Institutional Trust

The faith a user has that online application stores only distributes software that is safe for use, free from defects, and devoid of malicious code. Online app stores are Google Play Store, iTunes, Apple App Store, etc.

	Completely Disagree			Neutral			Completely Agree
	1	2	3	4	5	6	7
1. The online app store ensures sellers are dependable. *	1	2	3	4	5	6	7
2. The online app store ensures sellers are reliable. *	1	2	3	4	5	6	7
3. The online app store ensures sellers are honest. *	1	2	3	4	5	6	7
4. The online app store ensures sellers are trustworthy. *							

Party Trust

Faith a user has that a software developer has made the software safe for use, free from defects, and devoid of malicious code.

	Completely Disagree			Neutral			Completely Agree
1. Sellers of applications in the online app store are generally dependable. *	1	2	3	4	5	6	7
2. Sellers of applications in the online app store are generally reliable. *	1	2	3	4	5	6	7
3. Sellers of applications in the online app store are generally honest.*	1	2	3	4	5	6	7
4. Sellers of applications in the online app store are generally trustworthy. *	1	2	3	4	5	6	7

Security practices

The technological aspect that a user takes (i.e. installing security applications) to protect their mobile device

1. Do you currently have antivirus software on your smartphone? *	Yes	No
2. Do you currently have email spam filter installed on your smartphone? *	Yes	No
3. Do you currently have antispyware on your smartphone? *	Yes	No
4. Do you currently have a firewall installed on your smartphone? *	Yes	No
5. Do you currently have any sort of encryption installed on your smartphone? *	Yes	No

Security Behaviors

The security conscious behavior and actions that a user demonstrates/conducts while using their mobile device.

1. Do you use file sharing software (Kazaa, EDonkey, etc.) from your smartphone? *	Yes	No
2. Do you make backup copies of your files from your smartphone? *	Yes	No
3. Do you have sensitive documents such as medical, financial, or banking stored on your smartphone? *	Yes	No
4. Does your smartphone require some form of authentication (PIN, Password, Pattern) before getting access? *	Yes	No
5. When transferring data on the Internet from your smartphone do you check to see if the site is secured? *	Yes	No
6. Have you shared your smartphone with other people? *	Yes	No

Demographics

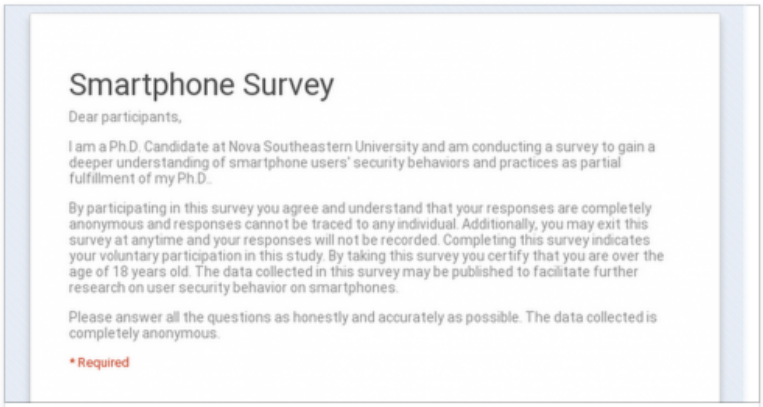
Gender *	Male	Female				
Age *	18-24	25-34	35-44	45-54	55+	
Highest level of education *	High School	Some College	Associate Degree	Bachelor Degree	Graduate Degree	
Marital Status *	Single	Married	Divorced	Widowed	Separated	
Number of years using a smartphone *	Please type an answer between 1 and 20					
Do you have an information systems security background (i.e. training, education, certification)? *	Yes	No				
What type of smartphone do you currently use? *	Android	iPhone	Windows	Blackberry	Other	Don't know

Appendix D

Participant Recruitment Post

Hi everyone. As promised here is a link to my dissertation survey. I need at least 250 responses to make this a valid study, so if you all would please take about 10 minutes of your time and take this survey, I would greatly appreciate it.

Thank you ALL in advance.



Smartphone Survey

Dear participants,

I am a Ph.D. Candidate at Nova Southeastern University and am conducting a survey to gain a deeper understanding of smartphone users' security behaviors and practices as partial fulfillment of my Ph.D..

By participating in this survey you agree and understand that your responses are completely anonymous and responses cannot be traced to any individual. Additionally, you may exit this survey at anytime and your responses will not be recorded. Completing this survey indicates your voluntary participation in this study. By taking this survey you certify that you are over the age of 18 years old. The data collected in this survey may be published to facilitate further research on user security behavior on smartphones.

Please answer all the questions as honestly and accurately as possible. The data collected is completely anonymous.

* Required

Smartphone Survey

Dear participants, I am a Ph.D. Candidate at Nova Southeastern University and am conducting a survey to gain a deeper understanding of smartphone users' security behaviors and practices as partial fulfillment of my Ph.D.. By participating in this...

DOCS.GOOGLE.COM

Appendix E

IRB Approval

NOVA SOUTHEASTERN UNIVERSITY
Office of Grants and Contracts
Institutional Review Board

MEMORANDUM

To: Joseph Simpson

From: Ling Wang, Ph.D.
Institutional Review Board

Date: May 19, 2015

Re: *Empirical Analysis of Socio-Cognitive Factors Affecting Security Behaviors of Smartphone Users*

IRB Approval Number: wang05151501

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. 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 these 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 REACTIONS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and 954-262-2020 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.

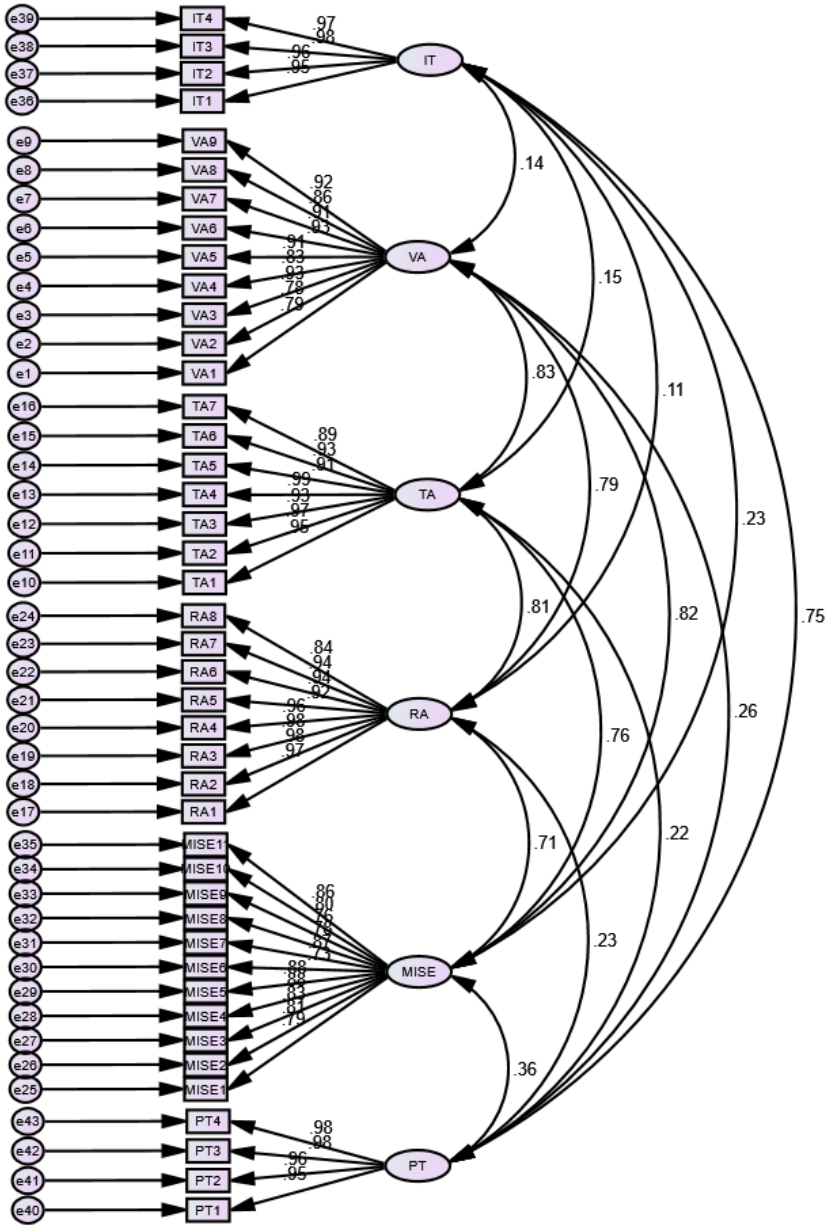
The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Protocol File

3301 College Avenue • Fort Lauderdale, FL 33314-7796 • (954) 262-5369
Fax: (954) 262-3977 • Email: *inga@nsu.nova.edu* • Web site: www.nova.edu/cwis/ogc

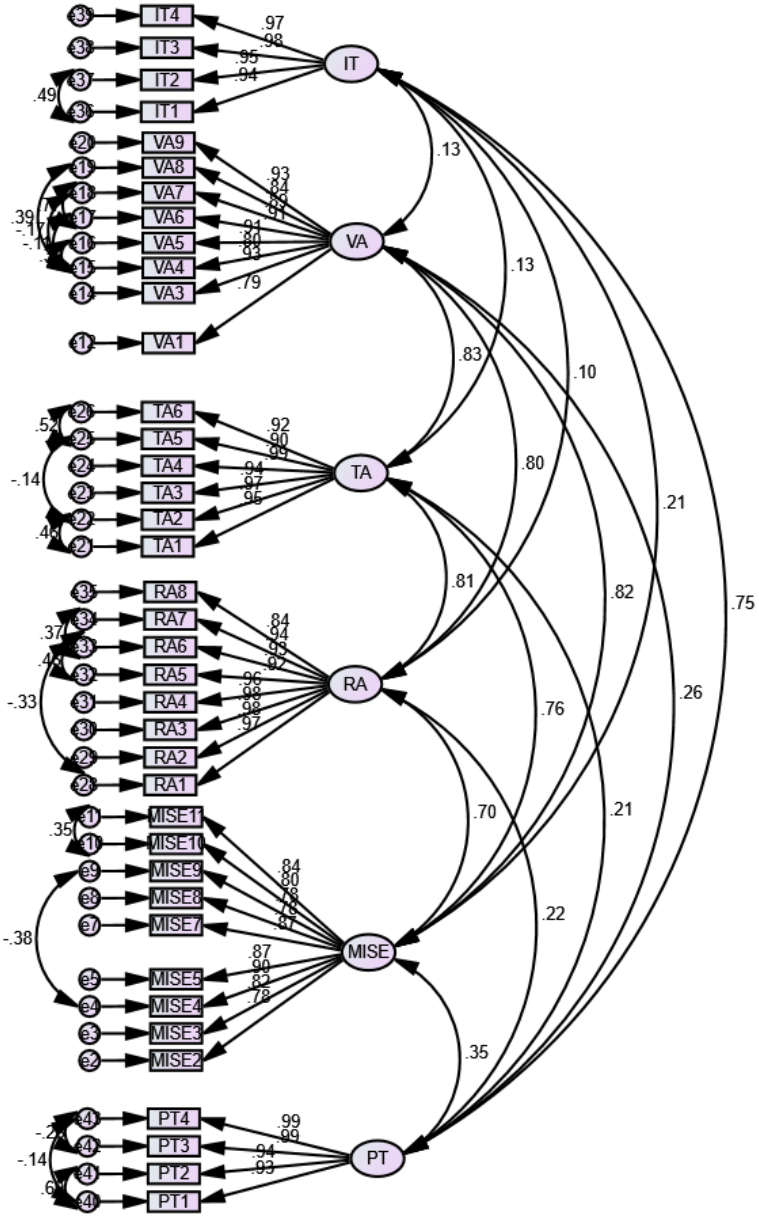
Appendix F

Initial CFA Model with Estimation



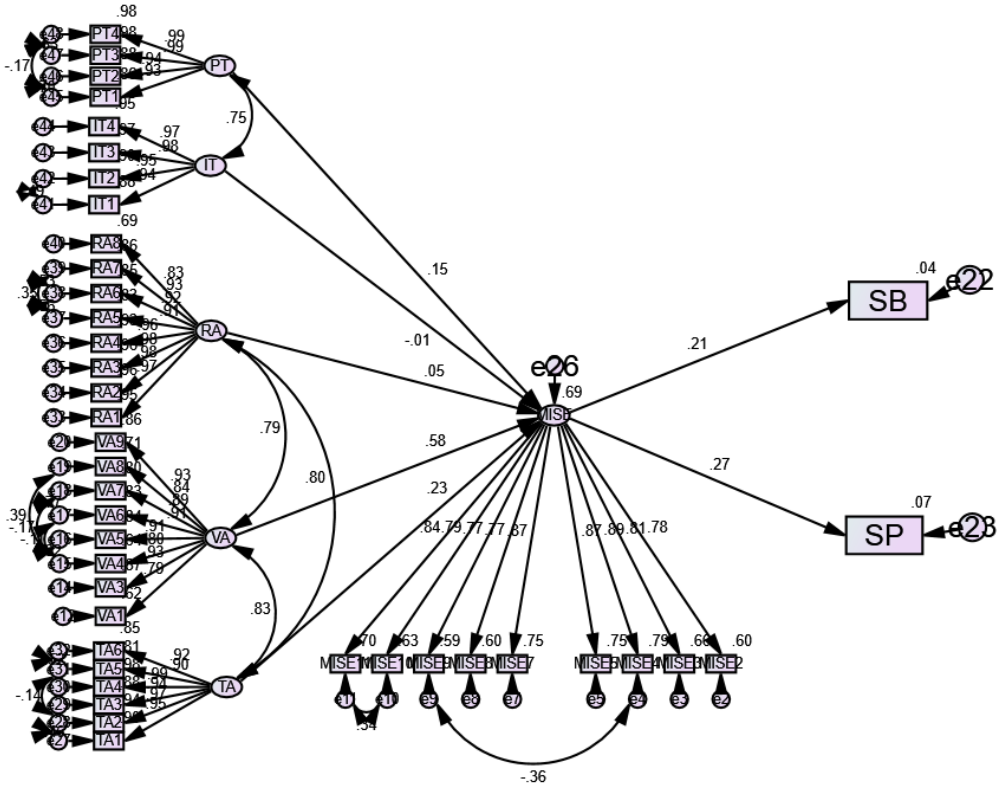
Appendix G

Modified CFA Model with Estimation



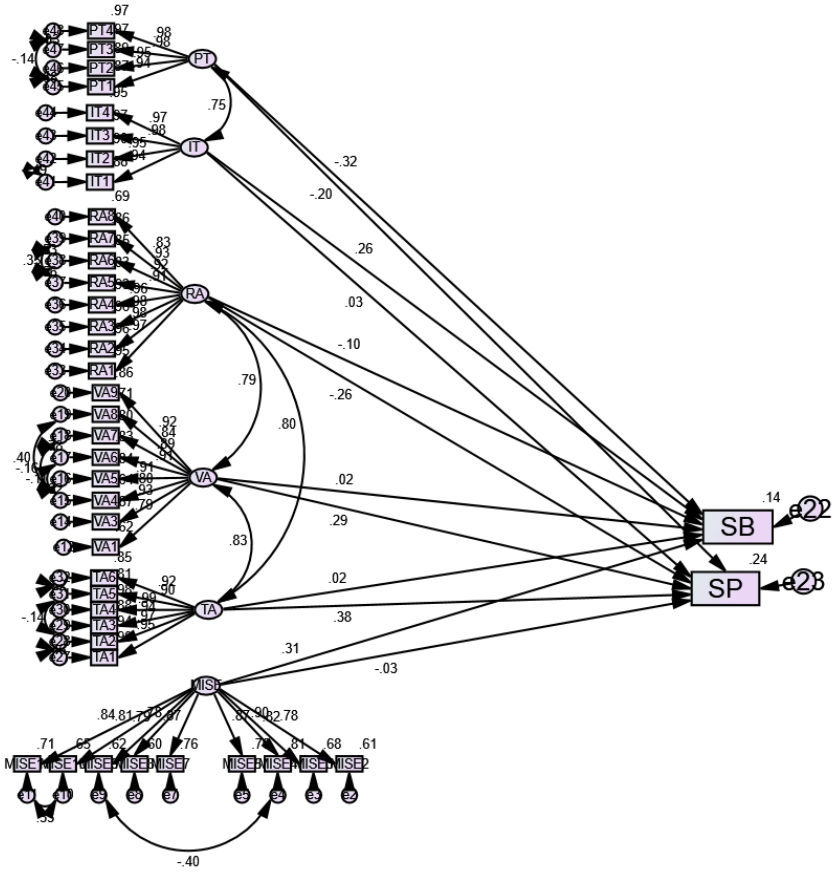
Appendix H

Initial SEM Model with Estimation



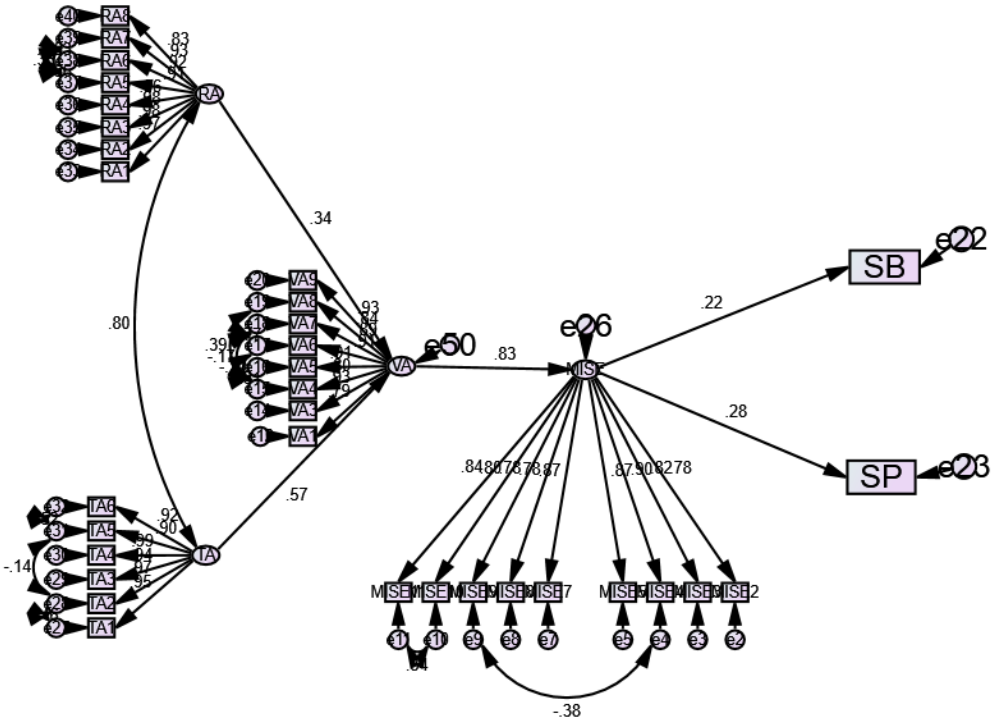
Appendix I

Direct Effect SEM Model with Estimation



Appendix J

Final SEM Model with Estimation



References

Agarwal, R., Sambamurthy, V., & Stair, R. M. (2000). Research report: The evolving relationship between general and specific computer self-efficacy – an empirical assessment. *Information Systems Research, 11*(4), 418-430.

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security, 42*(1), 56-65.

Anderson, K. B., Durbin, E., & Salinger, M. A. (2008). Identity theft. *Journal of Economic Perspectives, 22*(2), 171-192.

Arbuckle, J. (2007). *Amos 16.0 user's guide*. Chicago, IL: SPSS.

Aytes, K., & Connolly, T. (2004, July/Sept). Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing, 16*(3), 22-40.

Ba, S., & Pavlou, P. A. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. *MIS quarterly*, 243-268.

Ball, D.M. (2008). *An empirical investigation of the contribution of computer self-efficacy, computer anxieties, and instructors' experience with the use of technology to their intention to use emerging educational technology in traditional classrooms.* (Doctoral dissertation). Retrieved from *Dissertations and Theses*. (Publication No. AAT 3297720).

Ballagas, R., Borchers, J., Rohs, M., & Sheridan, J. G. (2006). The smart phone: A ubiquitous input device. *Pervasive Computing, IEEE, 5*(1), 70-77.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological review, 84*(2), 191.

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 Services* (pp. 465-473). Munich: ACM.

Bickford, J., O'Hare, R., Baliga, A., Ganapathy, V., & Iftode, L. (2010). Rootkits on smart phones: Attacks, implications and opportunities. *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*, 49-54.

Blackmon, M. H., Kitajima, M., & Polson, P. G. (2003). Repairing usability problems identified by the cognitive walkthrough for the Web. *Proceedings of the conference on human factors in computing systems,* (pp. 497-504). Fort Lauderdale, FL: ACM Press.

Bogen, K. (1996). The effect of questionnaire length on response rates: A review of the literature. In *Proceedings of the Section on Survey Research Methods* (pp. 1020-1025). American Statistical Association Alexandria, VA.

Botha, R. A., Furnell, S. M., & Clarke, N. L. (2009). From desktop to mobile: Examining the security experience. *Computers & Security, 28*(3), 130-137.

Brenner, J. (2013, September 18). Pew Internet: Mobile. *Pewinternet.org.* Retrieved September 20, 2013, from http://pewinternet.org/Commentary/2012/February/Pew-Internet-Mobile.aspx

Bresz, F. P. (2004). People–often the weakest link in security, but one of the best places to start. *Journal of Health Care Compliance*, *6*(4), 57-60.

Brown, T. A. and Moore, M. (2015). *Confirmatory factor analysis for applied research*. Guilford Publications.

Burns, A. J., & Johnson, M. E. (2015). Securing health information. *IT Professional, 17*(1), 23-29.

Chan, F., Lee, G. K., Lee, E. J., Kubota, C., & Allen, C. A. (2007). Structural equation modeling in rehabilitation counseling research. *Rehabilitation Counseling Bulletin, 51*(1), 44-57.

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, *15*(5/6), 358-368.

Chen, K., Chen, J. V., & Yen, D. C. (2011). Dimensions of self-efficacy in the study of smart phone acceptance. *Computer Standards & Interfaces, 33*(4), 422-431.

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012, July). Measuring user confidence in smartphone security and privacy. *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 1.

Chipperfield, C., & Furnell, S. (2010). From security policy to practice: Sending the right messages. *Computer Fraud & Security, 10*(3), 13-19.

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719-731.

Cisco mConcierge. (2013, March) *BYOD Insights 2013: A Cisco Partner Network Study*. Retrieved March 20, 2015 from http:// www.ciscomcon.com/sw/swchannel/ registration/internet/registration.cfm?SWAPPID=91&RegPageID=350200&S WTHEMEID=12949.

Cook, T. D., & Campbell, D. T. (1979). *Quasi-experimentation: Design and analytical issues for field settings.* Chicago, IL: Rand McNally.

comScore. (6 January 2014). *comScore Reports November 2013 U.S. Smartphone Subscriber Market Share.* Retrieved January 11, 2014 from http://www.comscore.com/Insights/Press_Releases/2013/11/comScore_Reports_ November_2013_U.S._Smartphone_Subscriber_Market_Share

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly, 19*(2), 189-211.

Comrey, A., & Lee, H. (1992). A first course in factor analysis. Hillsdale, NJ: Erlbaum.

Consumer Reports. (2014). *Smart phone thefts rose to 3.1 million last year, Consumer Reports finds*. Consumerreports.org. Retrieved April 17, 2014, from http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm

Crossler, R. E., & Bélanger, F. (2006, September). The effect of computer self-efficacy on security training effectiveness. In *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development* (pp. 124-129). New York, NY: ACM.

Department of Navy [DoN]. (2012, July 15). What is personally identifiable information?. *The DON IT Resource.* Retrieved May 20, 2013, from http://www.doncio.navy.mil/ContentView.aspx?id=2428

Dishaw, M. T., Strong, D. M., & Bandy, D. B. (2002, August). Extending the task-technology fit model with self-efficacy constructs. In *Eighth Americas Conference on Information Systems* (pp. 1021-1027).

Distefano, A., Grillo, A., Lentini, A., & Italiano, G. F. (2010, April). SecureMyDroid: Enforcing security in the mobile devices lifecycle. In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research* (p. 27). ACM.

Dorflinger, T., Voth, A., Kramer, J., & Fromm, R. (2010, July). “My smartphone is a safe!” The user's point of view regarding novel authentication methods and gradual security levels on smartphones. In *Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference,* (pp. 1-10). IEEE.

European Network and Information Security Agency ENISA. (December 2010). *Smartphone: Information security risks, opportunities and recommendations for users*. Retrieved 7 January 2013, from http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users

Fenech, T. (1998). Using perceived ease of use and perceived usefulness to predict acceptance of the World Wide Web. *Computer Networks and ISDN Systems, 30*(1), 629-630.

Furnell, S. (2008). End-user security culture a lesson that will never be learnt? *Computer Fraud & Security, 2008*(4), 6-9.

Furnell, S., Bryant, P., & Phippen, A. (2007). Assessing the security perceptions of personal internet users. *Computers & Security, 26*(1), 410-417.

Furnell, S., Tsaganidi, V., & Phippen, A. (2008). Security beliefs and barriers for novice Internet users. *Computers & Security, 27*(7-8), 235-240.

Fung, R., & Lee, M. (1999). EC-trust (trust in electronic commerce): exploring the antecedent factors. *Proceedings of the Fifth Americas Conference.* (pp. 517-519).

Galesic, M., & Bosnjak, M. (2009). Effects of questionnaire length on participation and indicators of response quality in a Web survey. *Public Opinion Quarterly, 73*(2), 349-360.

Gillaspy, J. A. (1996). A primer on confirmatory factor analysis. Paper presented at the *Annual Meeting of the Southwest Educational Research Association*, New Orleans.

Gorsuch, R. (1983). *Factor analysis*+ (2nd ed.). Hillsdale, NJ: Erlbaum.

Grossklags, J., & Acquisti, A. (2007). When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information, *Proceedings of the Sixth Workshop on the Economics of Information Security (WEIS 2007)* (pp. 7-18).

Hair Jr. J. F., Anderson R. E., Tatham R. L., Black W. C. (1998). *Multivariate data analysis*. 5th ed. Upper Saddle River, NJ. Prentice-Hall, Inc.

Hair, J., Black, W., Babin, B., and Anderson, R. (2010). *Multivariate data analysis.*7th ed. Upper Saddle River, NJ, USA. Prentice-Hall, Inc.

Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2013). *A primer on partial least squares structural equation modeling (PLS-SEM)*. SAGE Publications, Incorporated.

Haley, K. (2012). Introducing the Symantec smartphone honey stick project. *Symantec.com.* Retrieved October 1, 2013, from http://www.symantec.com/connect/blogs/introducing-symantec-smartphone-honey-stick-project?cnn=yes

Hart, C. (1998). *Doing a literature review: Releasing the social science research imagination.* London, UK: Sage.

Hazari, S., Haragrave, W., & Clenney, B. (2008). An empirical investigation of factors influencing information security behavior. *Journal of Information Privacy & Security, 4*(4), 3-20.

Herzog, A. R., & Bachman, J. G. (1981). Effects of questionnaire length on response quality. *Public Opinion Quarterly, 45*(4), 549-559.

Hox, J. J. (1995). *Amos, EQS, and LISREL for Windows: A comparative review. Structural Equation Modeling: A Multidisciplinary Journal, 2*(1), 79-91.

Huang, D. L., Rau, P. L. P., & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology, 29*(3), 221-232.

Husted, N., Saïdi, H., & Gehani, A. (2011, December). Smartphone security limitations: Conflicting traditions. *Proceedings of the 2011 Workshop on Governance of Technology, Information, and Policies*, 5-12.

Jeon, W., Kim, J., Lee, Y., & Won, D. (2011). A practical analysis of smartphone security. *Human Interface and the Management of Information: Interacting with Information* (pp. 311-320). Heidelberg: Springer.

Jones, B. H., & Heinrichs, L. R. (2012). Do Business Students Practice Smartphone Security?. *Journal of Computer Information Systems, 53*(2), 22-30.

Kaartina, S., Chin, Y. S., Wahida, R. F., Woon, F. C., Hiew, C. C., Zalilah, M. S., & Nasir, M. T. M. (2015). Adolescent self-report and parent proxy-report of health-related quality of life: an analysis of validity and reliability of PedsQL™ 4.0 among a sample of Malaysian adolescents and their parents. *Health and quality of life outcomes, 13*(1), 44.

Keith, M. J., Babb, J. S., Furner, C. P., & Abdullat, A. (2011, January). The role of mobile self-efficacy in the adoption of location-based applications: An iPhone experiment. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on* (pp. 1-10). IEEE.

Kline, R. B. (2005). *Principles and practice of structural equation modeling*. New York, NY: Guilford press.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296.

Kumar, N., Mohan, K., & Holowczak, R. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems, 46*(1), 254-264.

Landman, M. (2010, October). Managing smart phone security risks. *2010 Information Security Curriculum Development Conference*, 145-155.

Lee, S. Y. (2014). Examining the factors that influence early adopters' smartphone adoption: The case of college students. *Telematics and Informatics, 31*(2), 308-318.

Levy, Y. (2006). *Assessing the value of E-learning systems*. Hershey, PA: Information Science Publishers.

Levy, Y., & Green, B. D. (2009). An empirical study of computer self-efficacy and the technology acceptance model in the military: A case of a U. S. Navy combat information system. *Journal of Organizational and End User Computing, 21*(3), 1-23.

Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social engineering: The neglected human factor for information security management. *Information Resources Management Journal, 24*(3), 1-8.

Mertler, C. A., & Vannatta, R. A. (2013). Advanced and multivariate statistical methods (5th ed.): Practical application and interpretation. Glendale, CA: Pyrczak Publishing

Mui, L., Mohtashemi, M., & Halberstadt, A. (2002, January). A computational model of trust and reputation. In *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on* (pp. 2431-2439). IEEE.

Muslukhov, I., Boshmaf, Y., Kuo, C., Lester, J., & Beznosov, K. (2013, August). Know your enemy: The risk of unauthorized access in smartphones by insiders. *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services* (pp. 271-280). Munich: ACM.

Mylonas, A., Gritzalis, D., Tsoumas, B., & Apostolopoulos, T. (2013). A qualitative metrics vector for the awareness of smartphone security users. In *Trust, Privacy, and Security in Digital Business* (pp. 173-184). Springer. Berlin, Heidelberg.

Nurse, J. R., Erola, A., Goldsmith, M., & Creese, S. (2015). Investigating the leakage of sensitive personal and organisational information in email headers. *Journal of Internet Services and Information Security (JISIS), 5*(1), 70-84.

Okenyi, P. O., & Owens, T. J. (2007). On the anatomy of human hacking. *Information Systems Security*, *16*(6), 302-314.

Ong, C. S., Lai, J. Y., & Wang, Y. S. (2004). Factors affecting engineers' acceptance of asynchronous e-learning systems in high-tech companies. *Information & Management*, *41*(6), 795-804.

Park, Y., & Chen, J. V. (2007). Acceptance and adoption of the innovative use of smartphone. *Industrial Management & Data Systems*, *107*(9), 1349-1365.

Park, Y., Lee, C., Kim, J., Cho, S. J., & Choi, J. (2012). An Android security extension to protect personal information against illegal accesses and privilege escalation attacks. *Journal of Internet Services and Information Security*, *2*(3/4), 29-42.

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research*, *15*(1), 37-59.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y., and Podsakoff, N.P. (2003) Common method biases in behavioral research: A critical review of the literature and recommended remedies, *Journal of Applied Psychology 88*(5), 879.

Proprietary Data. (n.d.). In *The Law Dictionary Online.* Retrieved January 15, 2014, from http://thelawdictionary.org/proprietary-data/

Ramim, M., & Levy, Y. (2006). Securing e-learning systems: A case of insider cyberattacks and novice IT management in a small university. *Journal of Cases on Information Technology*, *8*(4), 24-34.

Ramo, D. E., & Prochaska, J. J. (2012). Broad reach and targeted recruitment using Facebook for an online survey of young adult substance use. *Journal of medical Internet research*, *14*(1), e28.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, *27*(7-8), 241-253.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816-826.

Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE*, *63*(9), 1278-1308.

Schreiber, J. B., Nora, A., Stage, F. K., Barlow, E. A., & King, J. (2006). Reporting structural equation modeling and confirmatory factor analysis results: A review. *The Journal of Educational Research*, *99*(6), 323-338.

Schumacker, R. E., & Lomax, R. G. (2010). *A beginner's guide to structural equation modeling*. (3rd ed.). New York: Routledge.

Sekaran, U. (2003). *Research methods for business - A skill building approach*. Hoboken, NJ: John Wiley & Sons.

Sharma, S., Mukherjee, S., Kumar, A., & Dillon, W. R. (2005). A simulation study to investigate the use of cutoff values for assessing model fit in covariance structure models. *Journal of Business Research, 58*(7), 935-943.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 52*(1), 92-100.

Sheng, Y. P., Pearson, M., & Crosby, L. (2003). Organizational culture and employees' computer self-efficacy: an empirical study. *Information Resources Management Journal*, *16*(3), 42-58.

Shneiderman, B. (1992). *Designing the user interface: strategies for effective human-computer interaction* (2nd Ed). Reading, MA: Addison-Wesley.

Simpson, J., Nilsen, R., Levy, Y., & Cohen, M. (2014). *An Empirical Assessment of Factors Effecting Information Security Risks of Smartphone Users.* Unpublished manuscript, Graduate School of Computer and Information Sciences, Nova Southeastern University, Ft. Lauderdale, FL

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Siponen, M. T. (2001). Five dimensions of information security awareness. *Computers and Society, 31*(2), 24-29.

Sposito, G., Holtzclaw, K. M., Charlet, L., Jouany, C., & Page, A. (1983). Sodium-calcium and sodium-magnesium exchange on Wyoming bentonite in perchlorate and chloride background ionic media. *Soil Science Society of America Journal, 47*(1): 51-56.

Stanton, J., Stam, K., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user behavior. Computers & Security, 24, 124-133.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly,* 147-169.

Straub, D.W., Boudreau, M., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems,* 13, 380-427.

Straub, D. W., Rai, A. & Klein, R. (2004). Measuring firm performance at the network level: A 29 nomology of the business impact of digital supply networks. *Journal of Management Information Systems, 21*(1), 83-114.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 441-469.

Summers, R. (1997). *Secure Computing: Threats and safeguards*. New York, NY: McGraw-Hill.

Tabachnick, B. G., & Fidell, L. S. (2007). Using multivariate statistics (5th ed.). Boston, MA: Pearson/Allyn & Bacon.

Tan, H., Forgasz, H., Leder, G., & McLeod, A. (2012, August). Survey recruitment using Facebook: Three studies. In *International Conference on Internet Studies* (pp. 17-18).

Tan, F. B., & Sutherland, P. (2004). Online consumer trust: a multi-dimensional model. *Journal of Electronic Commerce in Organizations (JECO), 2*(3), 40-58.

Teer, F. P., Kruck, S. E., & Kruck, G. P. (2007). Empirical study of students' computer security practices / perceptions. *The Journal of Computer Information Systems, 47*(3), 105-110.

Terrell, S. R. (2012). Statistics translated: A step-by-step guide to analyzing and interpreting data. New York: Guilford Press.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. A. (2009). Aligning Security Awareness With Information Systems Security Management. In *MCIS* (p. 73).

Udo, G. (2001). Privacy and security concerns as major barriers for e-commerce: A survey study. *Information Management & Computer Security, 9*(4), 165-174.

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* (pp. 10-24). ACM.

Venkatesh, V., & Davis, F. D. (1996). A model of the antecedents of perceived ease of use: Development and test. *Decision Sciences, 27*(3), 451-481.

Verhagen, T., Meents, S., & Tan, Y. H. (2006). Perceived risk and trust associated with purchasing at electronic marketplaces. *European Journal of Information Systems, 15*(6), 542-555.

Vijayasarathy, L. R. (2004). Predicting consumer intentions to use on-line shopping: The case for an augmented technology acceptance model. *Information & Management, 41*(6), 747-762.

Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in human behavior, 21*(1), 105-125.

Webroot. (2012). *Survey: Mobile Threats are Real and Costly.* Retrieved January 15, 2014 from http://www.Webroot.com/shared/pdf/byod-mobile-security-study.pdf

Weston, R., & Gore, P. A. (2006). A brief guide to structural equation modeling. *The Counseling Psychologist, 34*(5), 719-751.

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security, 16*(6), 315-331.

Zhou, Y., Zhang, X., Jiang, X., & Freeh, V. W. (2011). Taming information-stealing smartphone applications (on android). In Trust and Trustworthy Computing (pp. 93-107). Springer Berlin, Heidelberg.