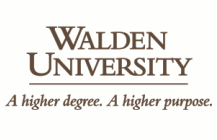

2017

The Challenges of Implementing Bring Your Own Device

Leslie DeShield
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Leslie DeShield

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Steven Case, Committee Chairperson, Information Technology Faculty
Dr. Timothy Perez, Committee Member, Information Technology Faculty
Dr. Gail Miles, University Reviewer, Information Technology Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2017

Abstract

The Challenges of Implementing Bring Your Own Device

by

Leslie A. DeShield

MS, Strayer University, 2008

BS, Strayer University, 2005

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2017

Abstract

Research conducted by Tech Pro (2014) indicated that the Bring Your Own Device (BYOD) concept is gaining momentum with 74% of organizations already having some BYOD program or planning to implement one. While BYOD offers several benefits, it also presents challenges that concern information technology leaders and information security managers. This correlational study used the systems theory framework to examine the relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation. Participants of the study consisted of information security managers in the eastern United States who had obtained the Certified Information Systems Manager certification. Data was collected from 94 information security managers through a survey instrument. The survey instrument integrated three other instruments with proven reliability developed by other researchers. Data was analyzed using a multiple regression analysis to test for a relationship between the variables of the study (security, compliance, and intent to implement BYOD). The multiple regression conducted in this study was insignificant indicating a relationship did not exist between the study's variables ($F(2, 86) = 0.33$, $p = .718$, $R^2 = .00$). A significant negative relationship was found between security and compliance indicating a weakly negative correlation ($r = -.26$, $p = .016$). Using the results from the study, information technology leaders may be able to develop strategies from which to implement BYOD successfully. Implications for social change include increased knowledge of securing personal devices for employees and consumers in general and reduction in costs associated with security and data breaches.

The Challenges of Implementing Bring Your Own Device

by

Leslie A. DeShield

MS, Strayer University, 2008

BS, Strayer University, 2005

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2017

Dedication

I would like to dedicate this study to my lovely wife, Alice, for her patience, support, and steadfast encouragement during the time dedicated to completing my study and achieving this goal.

Acknowledgments

First, I want to give thanks to Jesus, the Christ, for making all of this possible. I would like to thank Dr. Steven Case for his mentorship, support, and guidance during the course of my doctoral study. Without his guidance and encouragement, it would have been very difficult to complete this journey. Especially during the times I was tired and simply wanted to give up. I would also like to thank my second committee member, Dr. Timothy Perez, and my reviewer, Dr. Gail Miles for their valuable comments and feedback into making my study complete.

I would like to thank my mother, Sadie DeShield, and family members for their steadfast encouragement, and my pastor, Clyde W. Ellis Jr. and friends for their support over the course of this journey. Also, my late father, Leonard DeShield Sr., who would have been extremely proud of this accomplishment. Finally, I would like to thank my organizational leaders, Dale DeBruler and Clark Heidelbaugh, for their tremendous support and encouragement throughout this journey. You helped to make this possible in more ways than you could imagine.

Table of Contents

List of Tables v

List of Figures vi

Section 1: Foundation of the Study 1

Background of the Problem 2

Problem Statement 3

Purpose Statement 3

Nature of the Study 4

Research Question and Hypotheses 5

Theoretical Framework 5

Operational Definitions 6

Assumptions, Limitations, and Delimitations 8

Assumptions 8

Limitations 8

Delimitations 8

Significance of the Study 9

Contribution to Information Technology Practice 9

Implications for Social Change 9

A Review of the Professional and Academic Literature 10

Systems Theory 11

Evolution of Systems Theory 12

Application of Systems Theory 14

Supporting Theories 17
Contrasting Theories 21
Bring Your Own Device Implementation 22
Bring Your Own Device Overview 22
Benefits of Bring Your Own Device 24
Challenges of Bring Your Own Device Implementation 27
Compliance 30
The Need for a Bring Your Own Device Policy 30
Employees' Compliance with Policies 31
Security 32
Information Security Risk Management 33
Potential Impact to an Organization 34
Bring Your Own Device Security Challenges 35
Bring Your Own Device Security Framework 36
Gap in the Literature 38
Transition and Summary 40
Section 2: The Project 42
Purpose Statement 42
Role of the Researcher 43
Participants 44
Research Method and Design 45
Method 46

Research Design 47
Population and Sampling 48
Ethical Research 49
Data Collection 51
Instruments 51
Data Collection Technique 53
Data Organization Techniques 54
Data Analysis Techniques 54
Reliability and Validity 57
Reliability 58
Validity 59
Transition and Summary 61
Section 3: Application to Professional Practice and Implications for Change 62
Overview of Study 62
Presentation of the Findings 62
Data Management Procedures 63
Reliability Analysis 63
Descriptive Statistics 64
Analysis 67
Assumptions 67
Summary 71
Theoretical Conversation on Findings 71

Applications to Professional Practice 74

Implications for Social Change 76

Recommendations for Action 76

Recommendations for Further Study 78

Reflections 79

Summary and Study Conclusions 80

References 82

Appendix A: NIH Human Subject Research Certificate of Completion 114

Appendix B: Permission for Use and Publishing of Survey Instruments 115

Appendix C: Survey Instrument 121

Appendix D: E-mail Invitation to Participate in Research 124

List of Tables

Table 1. Previous Studies on BYOD 39

Table 2. Reliability Statistics 64

Table 3. Frequencies and Percentages of Demographic Characteristics 65

Table 4. Means and Standard Deviations for Study Variables 66

Table 5. Results of the Regression Analysis.....69

Table 6. Pearson Correlation Matrix.....71

List of Figures

Figure 1. Power as a function of sample size.....49

Figure 2. Normal P-P plot of the residuals 68

Figure 3. Scatterplot of the residuals 69

Section 1: Foundation of the Study

The use of personal mobile devices in the workplace is gaining prominence and acceptance as many people are using their personal devices to conduct certain aspects of their work (Kim, Lim, & Kim, 2016). A bring your own device (BYOD) policy affords the opportunity of using a single personal device for (a) anything, personal and business use; (b) anywhere, mobile use through the Internet or wireless LAN (WLAN); and (c) anytime, working hours and off-duty hours (Disterer & Kleiner, 2013). BYOD benefits such as cost savings, increased productivity, and improved efficiency are factors in its' gaining popularity and acceptance (Fiorenza, 2013).

While BYOD affords several opportunities and benefits, there are also challenges. The issues of managing security for BYOD, defining what is acceptable use for employees and organizations, and data retrieval from personal devices are key concerns for organizations that have implemented BYOD or are contemplating implementation (Waterfill and Dilworth, 2014; de las Cuevas et al., 2015) Privacy and legal concerns are also issues that need to be addressed from a strategic perspective to ensure a successful BYOD program as BYOD involves both organizational data and employees' private data residing on a personal device (Kiernan, 2016; Peretti & Sarkisian, 2014). A comprehensive BYOD security framework that encompasses people, policy, management, and technology should be developed to address security concerns and ensure organizations can realize the benefits afforded by BYOD (Zahadat, Blessner, Blackburn, & Olson, 2015).

Background of the Problem

The proliferation and use of mobile devices along with the many features they offer have given rise to the phenomenon called BYOD (Disterer & Kleiner, 2013). BYOD allows the use of personal devices for business purposes and reflects a blurring of the line between personal and business use on the same device (Gaff, 2015). Many organizations are adopting a BYOD strategy due to employees' increased desire to use their mobile devices for both personal and work related tasks (Astani, Ready, & Tessema, 2013).

BYOD presents several benefits for organizations. Employees' satisfaction, improved productivity, cost effectiveness, and flexibility are some of the reasons for BYOD adoption (Vignesh & Asha, 2015; Stone, 2014; Harris, Ives, & Junglas, 2012; Weeger, Wang, & Gewald, 2016). Many organizations are integrating a BYOD strategy into their business processes due to its' emerging prominence (Waterfill & Dilworth, 2014).

There are some challenges associated with BYOD adoption. Adequate security, protection of corporate data on personal devices, legal/privacy concerns, and employees' compliance with BYOD policies are some of the challenges to be considered (Kiernan, 2016; Garba, Armarego, & Murray, 2015). The lack of a comprehensive framework or strategy from which to implement BYOD further complicates its' adoption. The goal of this study was to examine the challenges of BYOD implementation.

Problem Statement

The BYOD phenomenon is a fast growing trend that is transforming the business processes of many organizations and institutions (Ansaldi, 2013). Eighty-nine percent of students and faculty in the United States and United Kingdom use personal mobile devices for academic purposes (De Kock & Futcher, 2016). The general information technology (IT) problem is that IT professionals lack a comprehensive strategy for BYOD implementation. The specific IT problem is that IT leaders often lack the knowledge of the relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation.

Purpose Statement

The purpose of this quantitative correlation study was to examine the relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation. The implementation of organizational BYOD programs without fully addressing the risks and challenges or offering countermeasures as to how they could be mitigated implies a lack of knowledge on the part of IT leaders who are typically tasked with implementing BYOD. Past studies (Semer, 2013; Ansaldi, 2013) have highlighted the benefits of BYOD without fully addressing the risks and challenges or offering countermeasures as to how they could be mitigated. The independent variables are security and compliance. The dependent variable is BYOD implementation. The targeted population of this study consisted of information security managers of small to medium sized organizations in the Eastern region of the United States who are Certified Information Security Managers (CISMs).

The study targeted those who had implemented BYOD and were facing risks and challenges and those who were considering the implementation of BYOD but were unsure of how to address the risks and challenges associated with BYOD. The results of this study have the potential to help IT leaders develop strategies or a framework from which to implement BYOD successfully. The results might also provide employees and consumers with best business practices on how to protect their personal devices and reduce costs associated with security and data breaches.

Nature of the Study

A quantitative research method was the chosen approach for this doctoral study. Quantitative research explains phenomena using numerical data that can be analyzed statistically (Yilmaz, 2013). This study's goal was to examine the correlation between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation. I chose a quantitative method over a qualitative method because of my desire to examine the relationship between variables by extracting and comparing data utilizing a statistical approach that allows for hypotheses testing rather than individual perceptions (McCusker & Gunaydin, 2015). A qualitative method takes an exploratory approach toward the causes and consequences of a phenomenon through the eyes of others (Bernard, 2013). A mixed methods approach combines elements of both quantitative and qualitative methods; empirical data and participants' experience, to examine relationships and differences between variables (Yin, 2013). A qualitative or mixed methods approach was not suitable for this study as the purpose was

to examine the relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation.

A nonexperimental correlational design was selected as it allows for the measure of variables without manipulation from which analysis can be conducted to determine whether the variables are related. An experimental design is used to infer causality (Spector & Meier, 2014). I aimed this study toward examining relationships, thereby rendering true experiments and quasi-experiments inappropriate.

Research Question and Hypotheses

The research question and hypotheses posed for this study were:

RQ: What is the relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation?

H_0: There is not a relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation.

H_1: There is a relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation.

Theoretical Framework

The theory used for this study was system theory, which is described as an interdisciplinary theory about the nature of complex systems in nature, society, and science and is a framework by which researchers can investigate and/or describe any group of objects that work together to produce some result. Bertalanffy (1968) developed

the general system theory from which system theory has its origin. Key tenets of this theory are (a) objects, the variables within the system; (b) the attributes of the system and its objects; (c) the interrelationship between objects in a system; and (d) the existence of a system within an environment. Adams, Hester, Bradley, Meyers, and Keating (2014) expanded the definition of systems theory as a unified group of propositions that are linked with the aim of achieving understanding of systems.

System theory is applicable to this study. The constructs align with mobile devices and enterprises as objects; security and compliance as attributes; mobile devices connected to an enterprise network depict interrelationships; BYOD implementation within an enterprise indicates the existence of a system within an environment. Systems theory provides a framework from which to examine the relationship between security, compliance, and BYOD implementation.

Operational Definitions

Bring Your Own Device (BYOD): BYOD is a fast growing concept in which employees may use their personally owned devices to access corporate networks and resources (Chang, Ho, & Chang, 2014; Totten & Hammock, 2014; Castro-Leon, 2014).

Compliance: Compliance refers to adherence to established policies and controls to protect an organization's intellectual property and information assets in the context of BYOD adoption (Crossler, Long, Lorass, & Trinkle (2014).

Countermeasures: Countermeasures constitute comprehensive approaches to address potential risks and security threats (Malandrino & Scarano, 2013).

Information Security: Information security refers to the preservation of data to ensure business continuity and minimal business damage by limiting the impact of security incidents (von Solms & van Niekerk, 2013).

IT consumerization: IT consumerization is ihe orientation of IT products and services towards consumers (Yevseyeva et al., 2014).

Mobile device: Mobile devices are portable devices such as smartphones and tablets that offer a variety of advantages for personal and work use (Raptis, Papachristos, Kjeldskov, Skov, & Avouris, 2014).

Mobile device management: Mobile device management refers to systems and solutions designed to enhance the security of mobile devices (Rhee, Won, Jang, Chae, & Park, 2013).

Information technology (IT) leaders: IT leaders are management executives who are typically in charge of IT governance practices in their organizations. These leaders typically have an IT background (Karanja & Zaveri, 2012).

Policy: In the context of this study, a policy consists of rules and guidelines employees must comply with to gain access to organizational resources (Silva, de Gusmão, Poleto, Silva, & Costa, 2014).

Risk: Risk is the technical, security, and legal concerns associated with BYOD as it relates to this study (Disterer & Kleiner, 2013).

Risk management: Risk management is the precautionary measures implemented to protect organizations from loss of data, intellectual property, or any other risks that could impact the organization (Beckett, 2014).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are unverifiable facts that are taken for granted as true (Jansson, 2013). Researchers consider assumptions important to their research although they are unverified (Lips-Wiersma & Mills, 2014). The first assumption of this study was that participants would provide accurate responses concerning the lack of a comprehensive strategy for BYOD implementation, as they would be IT professionals. The second assumption of the study was that participants would have a vested interest in understanding the challenges associated with BYOD implementation due to its fast growing trend and influence on the transformation of organizational business processes.

Limitations

Limitations are potential weaknesses in a study that may limit a researchers' ability to answer social, behavioral, and relational questions (Yeatman, Trinitapoli, & Hayford, 2013). A limitation of the study was that the sample population of IT professionals would be limited to information security managers who have obtained the CISM certification.

Delimitations

Delimitations refer to the boundaries or scope of the study (Thomas, Silverman, & Nelson, 2015). The scope of the study was limited to small and medium organizations in the eastern region of the United States. The boundaries of the study included conducting a survey of information security managers that have obtained the CISM certification.

Significance of the Study

Contribution to Information Technology Practice

The results of this correlation study produced options and suggestions from which IT leaders may be able to address some of the challenges associated with BYOD implementation. The use of technology in organizations presents both opportunities and challenges (McNaughton & Light, 2013). The increasing use and acceptance of mobile devices has been a factor in organizations' consideration of the benefits and challenges of allowing their employees to participate in a BYOD program (Marshall, 2014)

This study provides a comprehensive strategy for organizations' information security staff that will enable them to address the challenges associated with BYOD implementation. Studies have shown that BYOD presents several security risks that must be addressed for a successful implementation (Kiernan, 2016; de las Cuevas et al., 2015). Data results from this study contribute to the existing literature on BYOD and help provide decision makers with some options when considering BYOD implementation.

Implications for Social Change

This study will have implications for societal change as consumers will be able to take advantage of best business practices that might be developed from this study to protect their personal devices and reduce costs associated with security and data breaches. Employees will gain an understanding of their role in protecting organizational and private data when participating in a BYOD program. The knowledge gained by employees could be beneficial for family members as employees apply the same best practices and security measures from a BYOD program to securing the personal devices

of family members, thereby reducing the potential risks to their devices, including loss of personal data.

A Review of the Professional and Academic Literature

The literature review presented a collection of resources that examined the relationship between security, compliance and BYOD implementation. For example Rhee, Ryu, and Kim (2012) conducted a study related to information security based on the phenomenon that increased vulnerability to information security breaches correlates with a low level of managerial awareness and commitment regarding information security threats. Rhee et al. (2012) noted the need for more security awareness training in organizations and systematic approaches in dealing with security threats. Another example is a study in which Hovav and Putri (2016) examined employees' intent to comply with organizational BYOD security policies using a research model derived from reactance, protection motivation, and organizational justice theories.

The review consisted of peer-reviewed articles from journals, reports, articles, theses, and seminal books with a focus on research conducted within the past 5 years. I used 215 resources with 186 (86.51%) published between 2013 and 2017. One hundred eleven (85.59%) of the resources were used in the literature review of which 100 (90.91%) were peer-reviewed. They were acquired from databases such as EBSCOhost, Google Scholar, SAGE Journals Online, and Thoreau. The resources included seminal works that supported the theoretical framework applicable to this study. The strategy employed for searching the literature included the use of key words during database searches, incorporating key words related to the theoretical framework. Key words used

during database searches included *BYOD, BYOD strategies, risks, compliance, security, policies, countermeasures, security awareness, privacy, legal challenges, system theory, BYOD benefits, alternating theories,* and *mobile devices*. The review of the professional and academic literature was focused on the following themes: (a) systems theory, (b) BYOD implementation, (c) compliance, and (d) security. I chose to organize the professional and academic literature around these themes because the goal of this study was to examine the relationship between security, compliance, and BYOD implementation. Systems theory, as a theoretical framework, allows for the examination of the independent and dependent variables from an interrelated perspective.

Systems Theory

Von Bertalanffy (1972) defined systems theory as the interdisciplinary study of systems and the interrelationships between their separate components. It has been described as the theory underlying the study of systems (Yawson, 2013). Von Bertalanffy's (1950) theoretical viewpoint was that it is necessary to investigate a system not only by its parts but also as a whole due to the relationship and dynamic interactions of the individual parts. Systems theory looks at a system in its entirety and the interactions and interrelationships of its various subsystems (Von Bertalanffy, 1968). Systems theory's premise is based on the study of the whole system and not its individual elements (Karniouchina, Carson, Short, & Ketchen, 2013).

Key tenets of this theory are (a) objects, the variables within the system; (b) the attributes of the system and its objects; (c) the interrelationship between objects in a system; and (d) the existence of a system within an environment (Bertalanffy, 1968). As

it relates to the constructs of systems theory, mobile devices and enterprises are objects; security and compliance are attributes; mobile devices connected to an enterprise network depict interrelationships; BYOD implementation within an enterprise indicates the existence of a system within an environment. According to Kivipõld and Vadi (2013), wholeness has to be viewed from the interactions of its parts and how they impact each other in the context of systems theory.

Systems theory is the chosen theoretical framework for this study to examine the relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation. Researchers use this framework as a foundational basis for the examination of relationships between variables. In the context of this study, security, compliance, and BYOD implementation are separate components that are interrelated.

Evolution of Systems Theory

Bertalanffy (1968) developed the general system theory from which systems theory has its origin. He further expanded the theory in 1972 (Pouvreau, 2014). Von Bertalanffy (1972) theorized that a system is composed of separate subsystems that function as a whole. A core premise is the basic characteristic of all living things is organization; the analysis and rationalization of the organization cannot be limited to the individual entities of the organization but must consider the organization as a whole (Von Bertalanffy, 1968). As an analogy to this premise, the human body is a system; however, the individual parts of the body do not define it as a system, the body working as a whole defines the system (Von Bertalanffy, 1968). Von Bertalanffy (1972) stated that a holistic

approach should be used to define a system rather than the analysis of the individual subsystems (Von Bertalanffy, 1972).

According to Laszlo and Krippner (1998), the term *system* connotes a complex of interacting components together with the relationships among them that permit the identification of a boundary-maintaining entity or process. Skoko (2013) described a complex system as a collection of individual agents with latitude to act in ways that are not always totally predictable but whose actions, however, are interrelated. According to Hughes, Newstead, Anund, Shu, and Falkmer (2015), system theory challenges reductionist views and analysis, which attempt to draw information and conclusions of certain sections in isolation from other parts of a system. Wilson (2014) described systems theory as the existence of systems with interdependent but related components that have a preset objective, purpose or function. Yawson (2013) further described systems theory as a framework by which elements acting together to produce some result could be studied.

Seminal thinkers Rapoport and Buckley (1968) have expanded Bertalanffy's (1968) body of work and made evolutionary contributions to system theory. Schwaninger's (2007) contribution to systems theory was overcoming the isolation of specialized disciplines and cultivating dialogue across them. Laszlo's (1987) contribution was the development of evolution systems theory, which is a merger of system theory and evolution theory. Sturmberg, Martin, and Katerndahl's (2014) contribution was further analysis of general systems theory that determined factors such

as dynamics in systems, science of network and evolution, complexity science, and adaptation were components of systems theory.

Application of Systems Theory

Systems theory is typically applied to qualitative studies, although researchers have applied this theory to quantitative studies. It is suitable for examining, analyzing, and understanding complex adaptive systems (Montgomery & Oladapo, 2014). Systems theory is used to address more complex software intensive systems today in comparison to less complex systems from years past. An example is the use of systems theory as the foundation for an integrated approach to security and safety for various systems such as nuclear power plants, spacecraft, and aircraft (Young & Leveson, 2014). Systems theory has been used to examine businesses and their functionalities from the perspective of a network of interdependent parts functioning as a whole (Gehlert, 2013). Systems theory allows for the examination of the interrelated parts of a system in order to understand the complexities (Kast & Rosenzweig, 1972). Systems theory does not reduce an entity to its individual components or subsystems for examination but instead views the interrelationship and interaction of the individual components or subsystems that encompass the whole system (Kast & Rosenzweig, 1972).

Adams, Hester et al. (2014) conducted a study in which they sought to propose systems theory as the theoretical foundation for understanding systems. The study incorporated the use of the internationally accepted classification for the 42 individual fields of science as the source for the propositions in the study. The goal of the study was to present a construct for systems theory incorporating the propositions put forth in the

study to present systems theory as the theoretical foundation for understanding multidisciplinary systems (Adams, Hester et al., 2014). The 42 individual fields of science were viewed as complex adaptive systems in the context of systems theory.

Systems theory was the theoretical foundation used in a psychotherapy study by Trop, Burke, and Trop (2013) to examine the complex interactions at work within individuals. Systems theory was the chosen theoretical framework for a study to identify and articulate interrelated components that positively or negatively impacted the effectiveness of health care interventions or programs (Adams, Jones et al., 2014). In the context of systems theory, these studies focused on interactions and interrelationships between components of systems.

An article by Nobles and Schiff (2012) examined the ability of systems theory to address the intricate issues of legal pluralism. The researchers examined the relationship between state law and violence, the issue of translation between disparate legal orders, and how systems theory constructs the differences between modern and premodern societies in relations to legal pluralism. Using systems theory as a foundation, Nobles and Schiff (2012) posited that modern society consists of separate subsystems of communication such as the political system, economic system, legal system, and education system that are interrelated. In the context of systems theory as defined by Von Bertalanffy (1972), the various systems mentioned were viewed as separate components with interrelationships between each system.

Mangal (2013) utilized systems theory as the theoretical foundation to examine social media in the context of systems, as all online websites can be considered systems.

The study examined whether self-organization, resilience, and hierarchy, as individual components, improved the functionality of websites. The result of the study showed that websites functionality and users' experience were impacted if self-organization, resilience, or hierarchy were affected. As it relates to systems theory, websites were considered systems and self-organization, resilience, and hierarchy considered separate interrelated components giving credence to Von Bertalanffy (1972) definition of systems theory.

Kivipõld and Vadi (2013) used the systems theory framework as the theoretical foundation of their study that explored the relationship between organizational leadership capability and organizational performance in the context of market orientation in financial services organizations, specifically in Estonia. The study's findings demonstrated a relationship between specific organizational leadership capabilities and organizational performance. The results showed that the interaction between the main behavioral principles of an organization has a direct relationship with organizational performance (Kivipõld & Vadi, 2013). In the context of systems theory, it is being used to examine interactions and interrelationship between variables and to establish relationship between variables.

Skoko (2013) employed the systems theory framework in conjunction with the qualitative-comparative analysis model to gain a better understanding of risk management in the context of developing countries. Systems theory was used to evaluate and improve the assessment and management of environmental and health risk in the complex world of developing countries. Environmental and health risk were considered

a complex adaptive system with interacting and interrelated factors (Skoko, 2013). In the context of this study, systems theory was used as a theoretical framework to examine a complex system with individual interrelated and interacting components.

A core principle of systems theory is that a system consists of independent parts that are interrelated and interact to form a whole. The aforementioned studies highlight systems theory as a theoretical framework used to examine complex systems and the interrelationships and interactions between their various components or subsystems. In the context of this study, systems theory is applicable in examining the relationship between the variables of security, compliancy, and BYOD implementation.

Supporting Theories

There are multiple theories that could be used to conduct research on the BYOD technological concept from several perspectives. Theories such as agency theory and protection motivation theory have been utilized as the theoretical framework for various BYOD related research. Systems theory is the chosen theoretical framework for this study to examine the relationship between the variables of security, compliance, and BYOD implementation. The supporting theories presented highlight their constructs and how they relate to BYOD although not chosen as the theoretical framework for this study.

Unified theory of acceptance and use of technology. The unified theory of acceptance and use of technology (UTAUT) is considered the most prominent method used for technology acceptance analysis consisting of four key constructs that influence behavioral intention to use a technology (Lescevica, Ginters, & Mazza, 2013). These

four constructs are (a) performance expectancy – the degree to which a technology provides benefits to consumers in performing certain activities, (b) effort expectancy – the degree of ease associated with consumers' technology usage, (c) social influence – the extent to which consumers perceive that others believe they should use a particular technology, and (d) facilitating conditions – consumers' perceptions of the resources and support available to perform a behavior (Lescevica et al., 2013). Researchers Martins, Oliveira, and Popovic (2014), used the UTAUT in a research study undertaken to explain customers' intention to adopt and use Internet banking. The results of this study supported a relationship between the constructs of UTAUT. Similarly, researchers Magsamen-Conrad, Upadhyaya, Joa, and Dowd (2015) used the UTAUT to determine users behavioral intention to use tablets. Maillet, Mathieu, and Sicotte, (2015) also used this theory to explain the acceptance and use of an Electronic Patient Record (EPR), as a new technology by nurses. As it relates to BYOD implementation and the constructs of UTAUT, increased productivity within organizations (performance expectancy), familiarity and ease of use (effort expectancy), status (social influence), and the proliferation of mobile devices (facilitating conditions) are contributing factors to the gaining prominence and acceptance of BYOD as a new technological concept.

Technology evolution theory. The technology evolution theory argues that technologies should not be viewed in isolation but as a dynamic system or ecosystem encompassing various interrelated technologies (Adomavicius, Bockstedt, Gupta, & Kauffman, 2007). The constructs of this technology ecosystem are (a) components, (b) products and applications, and (c) support and infrastructure wherein technologies

interact and impact each other's evolution (Adomavicius et al., 2007). The evolutions of technology provide opportunities such as the demand and proliferation of mobile devices, more robust applications, and the development of the necessary support and infrastructure required to sustain new technologies. BYOD implementation is an example of the evolution of a technological concept.

Socio-technical systems theory. The socio-technical systems theory is viewed as consisting of two interdependent systems. These systems are a technical system – comprising of equipment and processes, and a social system – comprising of people and tasks (Davis, Challenger, Jayewardene, & Clegg, 2014; Belanger, Watson-Manheim, & Swan, 2013). Dalpiaz, Giorgini, and Mylopoulos (2013) further described this theory as consisting of an interplay of humans, organizations, and technical systems. The socio-technical systems theory was developed by researchers to study the impact of new technologies on social behavior (Kull, Ellis, & Narasimhan, 2013). As it relates to BYOD implementation and the constructs of the socio-technical theory, mobile devices and their acceptable use illustrate the technical system component (equipment and processes) and users and their adherence to BYOD policies illustrate the social system component (people and tasks).

Theory of planned behavior. The theory of planned behavior (TPB) is a theoretical framework that has been used to understand, predict, and assess behavior from an action or inaction perspective (Ajzen & Sheikh, 2013). It has been the basis in the examination of users' acceptance of IT (Hung, Chang, & Kuo, 2013). It describes intention as the immediate antecedent of behavior rooted in the constructs of attitude,

subjective norm, and the perceived behavioral control (Ajzen & Sheikh, 2013). Researchers have used the theory of planned behavior in multiple studies to examine intentions and predict behaviors (Wang & Wang, 2015; Hasking & Schofield, 2015; Starfelt Sutton & White, 2016). As it relates to BYOD, this framework can be used to provide insight as to why BYOD acceptance is prevalent in some organizations and not so prevalent in others as it relates to users' acceptance of BYOD implementation.

Technology acceptance model. The technology acceptance model (TAM) is an information systems theory that assumes an individual's acceptance of a technology is determined by two major factors: perceived usefulness and perceived ease of use (Huang & Martin-Taylor, 2013). TAM is one of many theoretical frameworks used by researchers to examine and predict the adoption of technology by individuals (Brezavscek, Sparl, & Znidarsic, 2014; Yoon, 2016; Yeou, 2016). The attitude towards a new technology is a critical factor that influences the intention to use it (Cheung & Vogel, 2013). According to Lo (2014) different personality traits and attitudes toward innovations have the potential of influencing an individual's acceptance of technology. As an extension to TAM, additional research have identified the perception of resources and support as another major external factor that affects the adoption of new technologies (Wallace & Sheetz, 2014). In the context of this study, the TAM can be used to examine the acceptance and use of BYOD as a new technological concept.

Theory of reasoned action. The theory of reasoned action (TRA) is a theoretical model used to examine human behavior; it's a predictive model that is used in multiple fields to include IT (Mishra, Akman, & Mishra, 2014). The premise of the TRA is to

investigate the relationship between attitude and behavior based on two core concepts: principles of compatibility and behavioral intention. The TRA constructs are attitude, subjective norms, behavior intentions, and actual behavior (Mishra et al., 2014). Researchers have used this framework to examine and understand behaviors (Kim, Jeong, & Hwang, 2013). As it relates to BYOD, the TRA could be used to examine why users and organizations are adopting BYOD and also users' behavior and intent toward BYOD compliance.

Contrasting Theories

While there are multiple supporting theories that could have been selected to conduct research on the BYOD technological concept, there do also exist theories that are in contrast to the chosen theoretical framework. Systems theory is the applicable theoretical framework chosen for this study. The contrasting theories presented highlight their constructs and why they would be inappropriate theoretical frameworks in the context of this study.

Constructivism theory. Although associated with the qualitative research method, the constructivism theory states that individuals construct their own concept and understanding of the world through learned experiences (Enonbun, 2010). According to Duane and Satre (2014), constructivism expresses the notion that knowledge is created socially through communication. Constructivism contends that reality is the product of human intellects and changes as the individual constructor evolves (Hall, Griffiths, & McKenna, 2013). According to Lee (2012), constructivism is considered one of many paradigms in the field of qualitative research with a presupposition that constructivism's

beliefs are internally consistent. Constructivism theory also contends that truth or knowledge are not absolute and knowledge occurs in an iterative specific to its environment (Naidu & Patel, 2013). As it relates to the ontology and epistemology of constructivism, the paradigmatic beliefs are internally in tension (Lee, 2012). This is in direct contrast to systems theory where components are interrelated and work together to form a relationship without internal tension (Von Bertalanffy, 1972).

Grey systems theory. Julong Deng developed the grey systems theory in 1982 to study problems and systems for which partial information is known and partial information is unknown (Liu, Yang, Xie, & Forrest, 2016). Yin (2013) described this theory as an emerging multiple attribute decision-making tool requiring limited knowledge and understanding of a system to solve problems, make good estimations or predictions. According to Manouchehr, Seyyed Morteza, and Hossein (2016), fault tree analysis (FTA) using grey numbers is a useful risk assessment tool. In the context of this study, an effective system is described as one in which all-separate but interrelated components function together in alignment as a whole (Adams, Hester et al., 2014). Within this context, the grey systems theory stands in contrast to systems theory, as analysis of the relationship between interrelated components of a system could not adequately take place if there is incomplete or inaccurate system information.

Bring Your Own Device Implementation

Bring Your Own Device Overview

BYOD is a fast growing concept that allows employees to bring and utilize their personal devices at work to access company data and resources. It is a growing trend and

is fast becoming the rule rather than the exception in organizations. Although, BYOD is gaining prominence, this concept dates back to when individuals started bringing and using personal USB flash drives and installing personally preferred programs on organizational assets to accomplish their work related tasks (Zahadat et al., 2015). This is similar to the employee driven IT revolution from several years ago when employees started using Commodore Pet, Apple 1, and TRS personal computers in corporate offices to accomplish work related tasks (Harris et al., 2012).

The proliferation of mobile devices and their ever-increasing advanced capabilities have had a significant impact within the workplace (Waterfill & Dilworth, 2014). As a result, organizations have been introduced to the BYOD concept that has become a phenomenon in both the private and public sectors and have highlighted the importance of mobile devices such as tablets and smartphones (Ansaldi, 2013). Within the public sector, federal regulations, mandates, and executive orders are driving the adoption of BYOD as a strategic tool for the delivery of services (Fiorenza, 2013). Within the private sector, the acquisition of a startup software company by Google for its software that allows for the separation of personal and corporate data and technology giant Apple redesign of its iOS to address the BYOD phenomenon clearly demonstrate the widespread popularity and acceptance of the BYOD concept (Beckett, 2014).

This phenomenon presents several benefits and challenges to consider when contemplating a BYOD implementation (Waterfill & Dilworth, 2014). Technology expansion and the desire to cut cost is a driving factor for organizations' acceptance of BYOD within the corporate and enterprise environment (Utter & Rea, 2015). BYOD

benefits include increased mobility, flexibility, productivity, and employee satisfaction (Zahadat, Blessner, Blackburn & Olson, 2015). Organizations are faced with the challenge of exploring new options to secure data and networks as many employees are now using their personal mobile devices in the workplace (Leavitt, 2013).

Benefits of Bring Your Own Device

Waterfill and Dilworth (2014) and Ansaldi (2013) have reached a similar conclusion when describing the benefits of BYOD. That is the benefits of BYOD have triggered changes within organizations and their business processes. Vignesh and Asha (2015) noted a survey conducted on several organizations by Intel on the benefits of BYOD within their organizations which indicated 28% improved efficiency and productivity, 22% improved workers' mobility, 17% savings on investing in new machines, 9% job satisfaction, and 6% reduced IT management/troubleshooting. Benefits that are commonly referenced are those of cost savings, employee satisfaction improved productivity, and benefits to higher education.

Cost savings. The potential for cost savings is a contributing factor toward BYOD implementation. Fiscal challenges in both the private and public sectors present BYOD as a viable option. Stone (2014) reported that a 2013 study by Cisco revealed results indicating that employers could net an annual return of $3,150 per employee on device expenses through BYOD implementation. Organizations that choose to transfer some or all of devices procurement and usage cost from the organization to the employees could see a potential benefit in cost savings (Gaff, 2015). According to

Cheng, Guan, and Chau (2016), Intel Company employees' use of personal devices was a factor in organizational cost savings.

The health and hospitality industries provide some evidence of cost savings. From the perspective of health providers, BYOD implementation offers a reduction in overhead and cost for IT infrastructures and facilitation of patient care (Munroe, 2013). BYOD has enabled the hospitality industry to improve its' supply chain management process. Mobile devices are being used to deliver goods and services to the right place in a timely manner with the least cost (Car, Pilepić, & Šimunić, 2014). A recent survey conducted by GovLoop in partnership with Cisco Systems Inc. of federal, state, and local government employees found that 55% believe that cost savings is a benefit of BYOD (Fiorenza, 2013). Organizations can redirect the savings obtained from BYOD implementation to other purposes (Rose, 2013). According to Marshall (2014), organizations are encouraging employees to participate in a BYOD program in an effort to cut costs.

Employee satisfaction. Harris et al. (2012) conducted a study on IT consumerization. The findings categorized the benefits of IT consumerization into three categories; innovation, productivity, and employee satisfaction. The results for employee satisfaction revealed that 11% of older employees over age 45 and 13% of younger employees under age 35 valued the freedom and independence of being able to choose and utilize their device of choice. Employees' satisfaction has been positively associated with telework (Bosua, Gloet, Kurnia, Mendoza, & Yong, 2013). Telework is an option that is strategically used at times to recruit and retain a highly qualified workforce. It is

typically a fringe benefit that is offered to employees (Beham, Baierl, & Poelmans, 2014; Nijland & Dijst, 2015). Employees select and purchase the personal devices they desire for a reason. According to Waterfill and Dilworth (2014), employees are more efficient and satisfied when they are allowed to use devices and applications they are familiar with than unfamiliar devices and applications provided by organizations.

Improved productivity. According to Gaff (2015), the underlying theory as to why BYOD improves productivity is that employees tend to be more accustomed to their personal devices and will use them more efficiently in the workplace and after hours. Gaff (2015) also noted that employees' personal devices tend to be more advanced than organization owned devices and that most employees prefer working with newer advanced technology. Examples of improved productivity benefits to be obtained through BYOD adoption are employees being able to access corporate databases to complete real-time inquiries; eliminate onsite requirements to conduct functions such as dispatch, inventory, management, field sales and technical support; attend real-time company video conferences; and leverage bigger, high resolution smartphone screens and tablets to display graphics, medical charts, presentations, video feeds, and x-rays/MRIs (Waterfill & Dilworth, 2014). As reported by Harris et al. (2012), the results of their IT consumerization study related to productivity benefits revealed that 14% of employees access corporate resources after regular work hours and 22% consistently used their personal mobile phone to check corporate emails before going to bed while outside the physical boundaries of the organization and after hours, thereby, increasing and

improving productivity as a result of being able to utilize personal mobile devices to access corporate resources.

The hospitality industry has benefitted from the BYOD concept. Logistic managers are able to use personal mobile devices to determine the location of employees, goods, or services, thereby, leveraging access to information in the supply chain management process in real time (Car, Pilepic, & Simunic, 2014). Fiorenza (2013) noted from a research survey of federal, local, and state employees that 58% responded that they considered improved productivity to be the second greatest benefit of BYOD following 71% respondents who indicated that allowing employees to work on their device of choice was the greatest benefit. Williams (2014) reported that the results of a couple of surveys revealed that 91% of healthcare workers own a mobile phone with 87% actually using it during clinical applications. 98% of physicians are already using smartphones while another 68% are using tablets for workflow processes. These devices have the potential to improve productivity and efficiency as they can facilitate faster access to patients' information by healthcare workers (Williams, 2014).

Challenges of Bring Your Own Device Implementation

Several literatures exist that highlight the benefits of BYOD implementation. It's equally important to note the existence of literatures that highlight the associated risks and challenges. Security concerns have been on the rise, simultaneously, with the rapid increase of smartphones and tablets (Zahadat et al., 2015). According to Weiß and Leimeister (2014), mobile devices are infiltrating companies and creating challenges for Chief Information Officers (CIOs). As a result BYOD implementation increases security

risks. The lack of a comprehensive strategy for BYOD implementation further increases this risk.

There are several areas of concern that should be addressed prior to BYOD implementation. Waterfill and Dilworth (2014) identified three areas of concern that traditionally fall under the control of IT departments however this model and focus has changed with the prominence of BYOD adoption. These areas are managing security, controlling acceptable use, and retrieving data. Privacy is another area of concern to be considered in an organization's BYOD program; the employer's and employee's rights must be protected (Kiernan, 2016). The revelation and exposure of the PRISM program by Edward Snowden has been a factor in the increased awareness of privacy self-protection (Preibusch, 2015). The use of personal devices for personal and work purposes blurs the boundaries between personal and work domains thereby presenting many security challenges (Jovanovikj, Gabrijelcic, & Klobucar, 2014). According to Beckett (2014), organizations that do not address BYOD concerns put themselves at risk for data loss, loss of control, employees violations of industry regulations and company rules, breach of trust between employer and employee, exposure of organizations' intellectual property, and intentional or unintentional undermining of critical business obligations.

Harris et al. (2012) reported that 36% of employees ignore organization IT policy and utilize the device of their choice to do work while 46% of employees think their device of choice and available software applications are more useful than devices provided by organizations. Young tech-savvy employees consider using their own

devices at work a right instead of a privilege (Leclercq-Vandelannoitte, 2015). The introduction of personal mobile devices to an organization's network increases the potential for security problems as too often security responsibilities are left to the competences of device owners (Jones, Chin, & Aiken, 2014).

IT organizations are expected to maintain a certain level of service while supporting a variety of devices and operating systems (Astani et al., 2013). Organizations must investment in the various operating systems and platforms in their BYOD portfolio (Rose, 2013). With the many available options for mobile devices, IT departments should be responsible for managing, configuring and enforcing technical security controls to mitigate the risks of data loss associated with BYOD adoption (Garba et al., 2015).

BYOD adoption presents legal and policy issues such as privacy, fourth amendment concerns, ownership concerns, liability, and other legalities (Utter & Rea, 2015). Some legal issues centered around BYOD that impacts both organizations and employees are: (a) maintaining and storing data, (b) BYOD security, (c) BYOD and employee privacy, (d) breach response, notification, and investigation, (e) remote wiping and blocking, and (f) secure destruction of corporate data (Dhingra, 2016). According to Walker-Osborn, Mann, and Mann (2013), organizations are responsible for the protection of personal data that reside on their systems under the 1998 Data Protection Act (DPA). In the context of BYOD, adherence to the DPA is important as mobile devices can be easily lost or stolen. Organizations must craft the appropriate BYOD policies and implement appropriate technical and organizational security measures (Walker-Osborn,

Mann, & Mann, 2013). Organizations must ensure they have the legal right to access employees' personal devices or the data on these devices when they become the subject of an investigation to ensure there are no privacy violations (Peretti & Sarkisian, 2014). Organizations must ensure employees are trained on the importance of risk management, intellectual property, and the organization's right to access an employee's personal device to remove organization proprietary data (Beckett, 2015).

Compliance

Compliance in the context of BYOD is important. Employees own the devices that are use to access organizational resources thereby introducing added risks to the organization (Hovav & Putri, 2016). Compliance policies are the established rules, instructions, and actions that define organizational acceptable security levels and provide information security to organizational assets (Silva et al., 2014). Employees' non-compliance to security policies is the largest information systems security threat to organizations (Siponen, Adam Mahmood, & Pahnila, 2014).

The Need for a Bring Your Own Device Policy

The increased popularity of BYOD is the reason organizations are establishing BYOD polices to address the inherent risks associated with allowing personal devices to access organizational resources (Crossler et al., 2014). Vignesh and Asha (2015) referenced a survey conducted by SAANS Analyst Program of several organizations about the criticality of mobile security policies. The results revealed that 37.1% believed a mobile security policy was critical, 40% believed extremely important, 19.7% believed important, 0.7% believed unimportant, and 2.6% didn't know. The survey also revealed

that 36% of organizations do not have a formal BYOD policy. The adoption of corporate policies governing BYOD is the common response in addressing security and data privacy issues posed by BYOD (Crossler et al., 2014).

According to Dhingra (2016), an effective and efficient BYOD policy must have clear objectives and constraints related to the usage of personal devices on organizational networks. A BYOD policy should be well constructed, include penalties, understood and accepted by all users, and enforceable (Coates, 2014). At a minimum, a BYOD policy should clearly define the mobile devices allowed to participate in an organization's BYOD program (Gaff, 2015). Users adherence to a policy is highly influenced when they feel personal responsibility for their policy related actions (Yazdanmehr & Wang, 2016). According to Semer (2013), a BYOD policy should also include a mobile device management (MDM) solution to mitigate data security, compliance, and privacy risks. IT and security stakeholders like CIOs, CISOs, and CTOs should be able to articulate approaches for handling the risks associated with BYOD and capture these articulations in an information security policy document (Saha & Sanyal, 2015). BYOD policies require a philosophical change for both employees and management (Jackson, 2013). Munroe (2013) reported that a Gartner Group report revealed that 30% of midsize and large companies utilized MDM software while 80% utilized Microsoft Exchange ActiveSync to enforce BYOD polices on mobile devices.

Employees' Compliance with Policies

Putri and Hovav (2014) conducted an empirical study that examined employees' intention to comply with an organization's BYOD security policy. The theoretical

foundation for this study consisted of reactance, protection motivation, and organizational justice theories. The results obtained from the analysis conducted showed that employees' perceived response efficacy and perceived justice had a positive impact on their intention to comply with an organization's BYOD policy. The study's results also showed that restrictions in a BYOD policy perceived by employees as a threat to their freedom could impact their intention to comply with the policy.

A similar study conducted by researchers Liang, Xue, and Wu (2013) examined how incentives of reward and punishment influenced employees' compliance behavior. Using control and regulatory focus theories as the theoretical basis, the researchers examined the relationship between reward, punishment, regulatory focus, and compliance behavior in an IT environment. The results of the study revealed that punishment expectancy determines employees' compliance behavior while the effects of reward expectancy were insignificant. The study suggested that regulatory focus impacts how employees comply with organization controls such as BYOD policies.

Security

Security is a critical component of consideration for organizations as it relates to BYOD implementation. Organizations can leverage new technologies such as BYOD by adopting a proper risk-based approach to security (Saunders, 2014). BYOD implementation has direct implications on security, information ownership, device/network control, and helpdesk resources (Astani et al., 2013).

Information security encompasses the protection of organizations' assets when using mobile devices (Jones et al., 2014). Security challenges include knowing who and

what has access to the network, ensuring the network is malware-free, determining the classification of information that can be stored on a mobile device, and enforcing access policies for compliancy and audit requirements (Astani et al., 2013). According to Ifinedo (2016), employees' adherence to information security policies is influenced significantly by senior management's commitment to information security.

Information Security Risk Management

Risk assessment is critical to the viability of an organization in protecting against or minimizing potential impacts to business operations, quality of service, profitability, and convenience. The ultimate objective of risk assessment and risk management is to provide the most comprehensive information about the risks so that decision-makers can make the best decisions as to how to mitigate the risks (Skoko, 2013). A risk assessment should include insider related information to ensure effective measure and analysis of potential insider risks as insider threats are a major source of threats to organizational information (Cho & Lee, 2016).

The evolution of the Internet and the increased sharing of information and collaboration among organizations put organizational information systems assets at constant risk (Silva et al., 2014). The increased vulnerability to substantial economic loss as a result of potential Internet attacks is a factor in organizations adopting information security risk management as a component of their core business processes (Bojanc & Jerman-Blažič, 2013). Organizations manage risks as a part of their routine daily operations by using established risk management frameworks (Jondle, Maines, Burke, & Young, 2013). According to Zhao, Xue, and Whinston (2013), organizations can also

manage risks using an alternative risk management approach that is known as risk-pooling arrangement (RPA). An RPA is a mutual form of insurance arrangement in which multiple organizations are both policyholders and owners that share interdependent risks; security losses are shared equally among all organizations (Zhao, Xue, & Whinston, 2013).

Information security risk management is a critical task in addressing and minimizing the potential risks to information systems in modern businesses (Bojanc & Jerman-Blažič, 2013). The approach consists of identifying the organizational assets, identifying threats and assessing damages that may be caused by an attack, identifying vulnerabilities that could be exploited, conducting a security risk assessment, implementing appropriate controls to minimize risks, and monitoring the effectiveness of the implemented controls (Bojanc & Jerman-Blažič, 2013). Shamala, Ahmad, and Yusoff, (2013) described information security risk management as an analytical and structured assessment or an organization's security posture. Studies have shown that deficiencies in the practice of information security risk assessment are cause of inadequate or inappropriate security strategies (Webb, Ahmad, Maynard, & Shanks, 2014).

Potential Impact to an Organization

According to Rhee et al. (2012), organizations increased dependence on IT and the Internet increases their vulnerability to various security threats. Management's low-level awareness and commitment to addressing information security threats further increases this vulnerability. Organizations must employ the necessary organizational and

technical measures to ensure data security and compliance when allowing the use of mobile devices (Disterer & Kleiner, 2013). Separation techniques such as virtualization, dual boot capability, and virtual remote platforms are potential security controls that can be employed for a BYOD implementation, although, there is high initial cost to implement these controls (Chang et al, 2014). According to Dhingra (2015), organizations should consider one of the three software-based security models that are currently used to address BYOD security concerns. They are (a) Mobile Device Management (MDM), (b) Mobile Application Management (MAM), and (c) Mobile Information Management (MIM).

Bring Your Own Device Security Challenges

Information security and privacy are key concerns of BYOD implementation (Kiernan, 2016). While the focus of information security concerns is data confidentiality for organizational assets, other security concerns involve the risk introduced by the co-mingling of personal and organizational data on personal mobile devices, stolen, lost or hacked devices, unapproved software, the potential introduction of malware and viruses that can infect personal devices and potentially lead to the compromise of organizations' proprietary data, and the retainment of organizational data on employees personal devices (Garba et al., 2015). According to Tokuyoshi (2013), there has been a paradigm shift with BYOD in which employees are now dictating the type of technology they prefer to use in the enterprise as oppose to the traditional process in which IT departments established the standards and mandates for vetting, monitoring, and auditing IT equipment for proper use in the enterprise. As a result, additional security issues need to

be considered such as network traffic protection, network traffic protection from vulnerabilities and exploits, application policy enforcement, device policy enforcement, and data protection on devices.

Crossler et al. (2014) stated that while BYOD presents several benefits, it carries risks in the areas of security and privacy. Organizations should be concerned about consequences such as legal liability, regulatory consequences, and damage to organization's reputation as a result of potential confidentiality breaches (Crossler et al., 2014). According to Ghosh and Rai (2013), another security challenge is that personal devices may lack the sophistication of traditional security such as antiviruses, patches, firmware updates and configuration settings. This creates a potential risk for the integrity of the device and the organizational data that resides on it.

Bring Your Own Device Security Framework

Several researchers have put forth proposals and recommendations related to a security strategy or framework for addressing the security concerns associated with a BYOD implementation. According to researchers Ghosh and Rai (2013), the portability of mobile devices and their susceptibility to being lost or stolen presented a security challenge that had to be addressed through a framework. Similarly, Zahadat et al. (2015) stated that security concerns of BYOD necessitated the development of a BYOD security framework from which to address these concerns.

Ghosh and Rai (2013) recommended a framework that organizations could use to define a security strategy for mitigating risk in a BYOD environment. The framework is based on four concepts that are: (a) here is your own device (HYOD) - a concept in

which devices are provided, controlled, and supported by the organization, (b) choose your own device (CYOD) - a strategy wherein the organization provides employees with a number of devices to choose from with some flexibility to install limited specific applications and software, (c) bring your own device (BYOD) - the concept in which devices are owned by employees, organizations have less control of the devices, and users have almost total flexibility as long as they are in compliance with established organizational policies, and (d) own your own device (OYOD) - concept where the employee has discretion to use any device, however, there is no organizational support and compliance policies. While these concepts have varying degrees of security, it is to be noted that each also has an impact on employees' satisfaction at various levels. From a similar perspective, Zahadat et al. (2015) proposed a framework to be employed by organizational leaders, IT infrastructure support staff, security personnel, and acquisition officials to plan and implement a successful BYOD program. The proposed framework consists of the following components: (a) Plan – phase in which there is coordination amongst all stakeholders to understand the business environment and requirements and to discuss asset management, network environment, and governance as it relates to BYOD, (b) Identify – the identification and registration of devices and users that will be participating in a BYOD program, (c) Protect – appropriate protection of the data that will reside on the devices, (d) Detect – being able to detect threats and vulnerabilities to devices in a BYOD program and provide countermeasures for mitigation, (e) Respond – the ability to address a threat once it has occurred, (f) Recover – the ability to recover from a threat event through the use of backups and device tracking mechanisms, (g)

Assess and monitor – continuous assessment and monitoring of a BYOD program for effectiveness and efficiency and to address the evolution of threats, technology, and security solutions. The proposals presented by these researchers illustrate the security challenges surrounding BYOD and highlight the need for a comprehensive security strategy or framework to address the security challenges posed by BYOD.

Gap in the Literature

To date, most BYOD studies have focused on its gaining popularity and widespread adoption by users and organizations. The benefits are often highlighted as the cause of its adoption and tend to overshadow the security concerns and issues associated with its implementation. While the benefits and security concerns of BYOD are highlighted in BYOD studies and articles, there is a noticeable gap in literature related to BYOD security frameworks. Table 1 highlights some existing studies of BYOD that discuss the benefits as well as security challenges, however, do not address BYOD security frameworks.

Table 1

Previous Studies on BYOD

Author/date	Research focus	BYOD security framework	Theory in use	Findings
Putri & Hovav (2014)	Employees' compliance with BYOD security policy	No	Protection Motivational Theory (PMT), Reactance Theory, and Organizational Justice Theory	Useful insights in shaping a BYOD implementation strategy.
Son (2011)	Understanding employees' motivation to follow IS security policies	No	General Deterrence Theory (GDT)	Intrinsic motivation has a stronger effect on employees' compliance than extrinsic motivation
Ifinedo (2012)	Understanding security policies compliance	No	Theory of Planned Behavior (TPB) and Protection Motivation Theory (PMT)	Behavioral compliance intention influenced by several external factors
Zahadat et al (2015)	BYOD Security Engineering Framework	No	Framework comprised of a combination of Technology Management and Policy Management	BYOD security concerns necessitate the need for a BYOD security framework.

Of the four studies that are highlighted in Table 1, only one study puts forth a proposal for a BYOD security framework (Zahadat et al., 2015). The other three studies address the benefits of BYOD as well as challenges in the context of security and compliance (Putri and Hovav, 2014; Son, 2011; Ifinedo, 2012). All three studies employed a quantitative research approach. The study that put forth a proposal for a BYOD security framework relied on literature review and extensive interviews with security professionals, as there was no study to be found that proposed a BYOD security framework (Zahadat et al., 2015).

Transition and Summary

Section 1 was an introduction to the phenomenon known as BYOD that has gained prominence and the benefits and challenges associated with its' implementation. In this section, I discussed the background of the problem and provided a comprehensive literature review that presented and supported some of the benefits of BYOD that have been factors in its' widespread acceptance and implementation within many organizations. I provided literature that discussed some of the challenges associated with BYOD, specifically, in the areas of compliance and security. Providing additional information on BYOD and the challenges associated with its' implementation will contribute to the existing literature which will potentially provide IT leaders with options to develop strategies or a framework that will assist in implementing BYOD successfully. I also provided a comprehensive review of systems theory, the theoretical framework for this study. The review consisted of the evolution of systems theory and its application by

researchers in various studies. I also discussed other supporting theories relative to this study's topic and contrasting theories.

Section 2 describes the procedures and methodology to be used for the collection of data for this study and its' applicability to the challenges of implementing BYOD. The goal of Section 2 is to identify the role of the researcher and the survey population, describe the survey instrument and its' use in gathering data, and defend the chosen design methodology.

Section 2: The Project

In Section 2 I provide a description of the research study and address how the research question will be answered. I restate the purpose statement, explained the researcher's role and describe participant population and sample size. This section further provides details on the research method and design, ethical research requirements, data collection, instruments and techniques, and analysis process. Finally, this section concludes with a discussion of reliability and validity

Purpose Statement

The purpose of this quantitative correlation study was to examine the relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation. The implementation of organizational BYOD programs without fully addressing the risks and challenges or offering countermeasures as to how they could be mitigated implies a lack of knowledge on the part of IT leaders who are typically tasked with implementing BYOD. Past studies (Semer, 2013; Ansaldi, 2013) have highlighted the benefits of BYOD without fully addressing the risks and challenges or offering countermeasures as to how they could be mitigated. The independent variables are security and compliance. The dependent variable is BYOD implementation. The targeted population of this study consisted of information provided by security managers of small to medium organizations in the eastern region of the United States who are CISMs. The study targeted those who have implemented BYOD and are facing risks and challenges and those who are considering the implementation of BYOD but are unsure of how to address the risks and challenges

associated with BYOD. The results of this study have the potential to help IT leaders develop strategies or a framework from which to implement BYOD successfully. The results might also provide employees and consumers with best business practices on how to protect their personal devices and reduce costs associated with security and data breaches.

Role of the Researcher

As the researcher in this study, my role consisted of participant recruitment, collection of data for analysis, utilization of a survey instrument to examine the relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation, and dissemination of the results of the analysis. According to Cokley and Awad (2013), a researcher must be able to recognize bias in research. I selected survey instruments that met the criteria for validity of empirical measurements and supported the theoretical framework of the study. According to Barry, Chaney, Piazza-Gardner, and Chavarria (2014), survey instruments must be assessed to ensure the integrity of the collected data.

This study had practical significance due to my position as the information assurance manager in my organization. As the information assurance manager, I am responsible for the protection of the organization's data assets and ensuring its' security posture remains at an acceptable level, especially with the introduction and integration of newer technologies into the organization. I did not have a relationship with the participants of this study as the survey was administered remotely and consisted of a questionnaire that was anonymous in nature. According to Rowley (2014),

questionnaires are normally designed for completion without any direct interaction with researchers, either in person or remotely.

Researchers must protect their research participants and ensure participants' identities are protected. Researchers musts adhere to the principles of the Belmont Report (Fiske & Hauser, 2014). I adhered to the ethical principles required for research and made full disclosure of my status to participants of the study. As a prerequisite, I read the Belmont Report to gain an understanding of the ethical principles and guidelines required for the protection of human subjects in research (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1978). I validated this understanding by completing the National Institutes of Health Protecting Human Research Participants online training course (Certification Number: 614873, Appendix A).

Participants

Research requires the right participants for the subject or topic being researched. According to Elo, Kaariainen, Kanste, Polkki, Utriainen, and Kyngas (2014), researchers must establish criteria to ensure selection of participants who best represent or have knowledge of the research topic; they must be dependable in order to ensure the results of the study are transferable and repeatable in other studies. Research participants should be informed on how their participation benefits a research study (McCullagh, Sanon, & Cohen, 2014). The participants in this study consisted of IT professionals with information security experience. Information security professionals play an important role in the protection of organizations' assets (Steinbart, Raschke, Gal, & Dilla, 2013).

A nonprobabilistic sampling method consisting of a convenience sample was used for this study. A convenience sample is a sampling technique applicable to both qualitative and quantitative studies, although most frequently used with quantitative studies. This method utilizes participants who are more readily accessible to researchers (Wu Suen, Huang, & Lee, 2014). It allows for participants who fit the criteria of a study to be identified in any way possible (Peterson & Merunka, 2014). However, a convenience sample limits the opportunity for all qualified participants in the target population and study results are not necessarily generalizable to this population (Wu Suen et al., 2014; Sedgwick, 2013a). I addressed this limitation by ensuring the participants had a characteristic that represented the target population. Participants in the target population must have obtained the CISM certification.

Participants were solicited through e-mail requests. A working relationship was established by disclosing the nature and purpose of the study to participants. They were informed that their participation would remain confidential. Additionally, I provided assurance to participants by informing them that all data collected for the study would be stored in a secure safe and destroyed after 5 years. Participants were asked to sign a consent form prior to participation to ensure they had a clear understanding of the parameters of the study.

Research Method and Design

This study examined the relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation using a quantitative research method with a nonexperimental correlational design.

Research methodologies that are available for research are quantitative, qualitative, and mixed methods (Mertens, 2015). Studies using a correlational design seek to determine if a variable or factor might be influencing another (Pinder, Prime, & Wilson, 2014).

Method

I chose a quantitative research method to examine the relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation. Quantitative research allows for systematic quantification and analysis using numerical data (Turner, Balmer, & Coverdale, 2013). Researchers use the quantitative method to examine relationships and test hypotheses (Morgan, 2015). Quantitative research can also be used to provide large representative samples of cultural communities and assert cause and effect relationships among constructs (Fassinger & Morrow, 2013). A quantitative study was more appropriately suited for the research approach as the goal of the study was to examine the correlation between identified variables.

A qualitative research method uses an exploratory approach to understand phenomena, human behavior, groups, or individuals; it uses an interpretive approach for the collection, analysis, and interpretation of data (Yin, 2013). According to Palinkas (2014), qualitative research is ideal for eliciting the perspective of those being studied in their own voice. Qualitative research is inductive in its approach wherein researchers can explore situations without the imposition of pre-existing expectations on the setting (Dasgupta, 2015). My study was not exploratory in nature, thereby rendering a qualitative research method inappropriate for this study.

A mixed methods approach combines elements of both quantitative and qualitative research methods; researchers are able to combine empirical data and participants' experience for research (Yin, 2013). According to Venkatesh, Brown, and Bala (2013), triangulation is a core component of mixed methods research. It involves attempts to validate research through the merger of qualitative and quantitative data to understand the topic being researched. According to Mayoh & Onwuegbuzie (2015), mixed methods research is appropriate when a single research method in isolation cannot adequately explore a phenomenon. Mixed methods research requires in-depth research experience and can be time consuming (Venkatesh et al., 2013). As this study did not combine elements of both quantitative and qualitative research methods, it was not appropriate for this study.

Research Design

This study used a nonexperimental correlational design consisting of a survey. According to Pinder et al. (2014), a correlational design measures the relationship between variables and assesses the strength of such relationship. This design was used to assess the strength of the relationship between this study's variables of security, compliance, and BYOD implementation. A questionnaire was used to collect data for this study. According to a study by Rada and Dominguez-Alvarez (2013), self-administered questionnaires offered more advantages for data collection with a low number of unanswered questions. The survey for this study was administered online. Online surveys are cost effective, allow for flexibility, and provide faster access to research participants (Roberts & Allen, 2015).

According to Spector and Meier (2014), experimental designs allow researchers to identify causality for a particular research topic. This is achieved by two primary methods. The first is making observations before and after each step in a research process to show how a variable changes from before and after an event. The second is to continuously monitor a variable to see how it changes as events occur (Spector & Meier, 2014). Researcher Dehejia (2015) stated that experimental designs tend to be unbiased in their results as they are more scientific in nature. As this study did not involve the identification of causality or manipulation of variables, a nonexperimental design was more suited for this study.

Population and Sampling

The targeted population of this study consisted of information security managers from small to medium sized organizations in the eastern region of the United States that have obtained the CISM certification. Specific focus was toward CISMs who may have already implemented BYOD along with its' risks and challenges and those who were considering BYOD implementation. CISMs are individuals who have acquired the necessary expertise and have the ability to assess security; that is why they were the targeted population for this study.

The study used a nonprobabilistic convenience sample. According to Emerson (2015), a convenience sample is a nonrandom sampling method in which participants who fit the established criteria of a research study are identified in any way possible and are typically from the same geographic area. It targets participants who are convenient sources of data and are available (Sedgwick, 2013a). However, it limits the opportunity

for all qualified individuals in the target population, and study results are not necessarily generalizable to this population (Wu Suen et al., 2014). Participants were solicited through e-mail requests.

The sample size required from the targeted population of small to medium sized organizations was achieved by using the software G*Power3 (Faul, Erdfelder, Buchner, & Lang, 2009). The G*Power3 software is open sourced and was created by the Institute for Experimental Psychology in Dusseldorf, Germany (Faul et al., 2009). An a priori power analysis assuming a medium effect size (*f* = .15), a = .05, indicated a minimum sample size of 68 participants would be required to achieve a power of .80. The required sample size was 107. An increase in the sample size to 110 increased power to .95. I sought between 68 and 115 participants for this study (Figure 1)

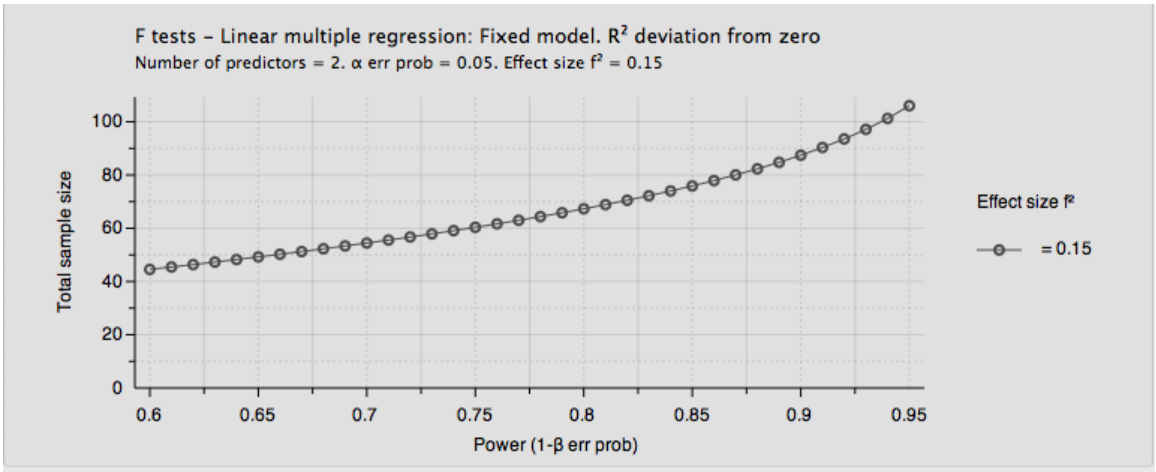

Figure 1. Power as a function of sample size.

Ethical Research

Pick, Berry, Gilbert, and McCaul (2013) stated that informed consent is the process by which an individual freely agrees to participate in research. Research

participants must have the capacity to understand the information provided and be able to decide whether to proceed or not for consent to be valid (Pick et al., 2013; Judkins-Cohn & Kielwasser-Withrow, 2014). According to Chiumento, Khan, Rahman, and Frith (2016), the objective of the informed consent process is to ensure ethical standards are upheld in research; participants' rights are to be protected and respected. Participants were provided a consent form (Appendix B) prior to participation in this study. The nature and purpose of the study was disclosed to participants and they were informed that participation would remain confidential. Assurance of confidentiality and the purpose for a study are important elements of a consent form (Yin, 2014). Participants were asked to sign a consent form prior to participation, as is the norm in research (Bernard, 2013).

Participants could withdraw from the study at any time by simply discontinuing the survey or not starting the survey if the conditions and terms of the study were unacceptable. Tideman and Svensson (2015) emphasized the importance of informed consent for research participants to ensure voluntary participation, the option to opt out of a research, confidentiality assurance, and the understanding to make an informed decision. If a participant discontinues the survey for this study, it will be considered incomplete and not included in the analysis. Participants did not receive any incentives for participating in this study. The study results will be made available to anyone who requests a copy.

It is essential that the confidentiality of participants in a study be protected. According to Robinson (2014) participants should be informed of the study's purpose and what participation entails, the voluntary nature of the study and how confidentiality will

be protected. Electronic data originating from the study will be password protected, secured on a password-protected disk drive, and stored in a secured safe for a period of 5 years. All data will be destroyed in accordance with established destruction procedures at the end of this period. I did not collect names and organizations of participants in this study to ensure confidentiality and provide participants an expectation of confidentiality. The process of data collection began upon receiving approval from Walden University's Institutional Review Board along with an assigned approval number for this study.

Data Collection

This study employed the use of a survey instrument to collect data. To eliminate the need for a pilot study to test reliability and validity, this study used pre-existing surveys from past studies that met the reliability and validity criteria. The data collection utilized an online survey tool. The Statistical Package for the Social Sciences (SPSS) was used to conduct analysis of the collected data.

Instruments

I developed an instrument that is based on three instruments developed by other researchers that have been proven as reliable (Lease, 2005; Putri & Hovav, 2014; Rhee et al., 2012). Minor revisions to the survey instruments will not invalidate them. The requisite consent and approval for use of these instruments were obtained (see Appendix C). The survey instrument was designed to measure information security managers' intentions, perceptions of security and compliance toward BYOD implementation.

Lease (2005) survey instrument from his research titled "Factors Influencing the Adoption of Biometric Security Technologies by Decision Making Information

Technology and Security Managers" was adapted for this study. The reliability and validity of this instrument was demonstrated through its' subsequent use by other researchers (Yoon, 2009; Stavinoha, 2012). The instrument consisted of Likert-type scale questions with ordinal values. The use of Likert scales is common and useful in attitude research projects (Joshi, Kale, Chandel, & Pal, 2015). Lease (2005) original survey instrument was constructed and organized to measure the following: (a) IT/information assurance managers' perception of biometrics security effectiveness (Items 1 through 5), (b) perceptions of the need for biometric security technologies (Items 6 through 8), (c) managers' perceptions of biometrics reliability (Items 9 through 11), (d) IT/information assurance managers' attitudes toward the cost-effectiveness of biometrics (Items 12 through 14), (e) understanding of the research participants' perceptions of biometrics technology (Items 15 and 16). The only change to this instrument involved all references to biometrics being replaced with BYOD or BYOD implementation. For this study, the survey instrument was used to measure information security managers' intentions toward BYOD implementation.

Putri and Hovav (2014) survey instrument used in their research on employees' compliance with BYOD security policy was adapted for this study. The instrument consisted of Likert-type scale questions adapted from existing scales to ensure reliability and validity (Vance, Siponen, & Pahnila, 2012; Sullivan & Artino, 2013). As it relates to this study, the survey instrument was used to measure information security managers' intent to comply with BYOD security policies.

Rhee et al. (2012) survey instrument used in their study titled Unrealistic Optimism on Information Security Management was also used for this study. Items to be measured were generated based on review of previous literature (Armitage, Conner, Loach, & Willetts, 1999). To further ensure content validity and reliability of the scales of their instrument, Rhee et al. (2012) conducted a pilot test of a sample of their population consisting of MIS faculty, graduate students, and practitioners. For this study, the survey instrument was used to measure security risks perception of information security managers.

Data Collection Technique

I worked with the presidents of local chapters of ISACA and the Information Systems Security Association (ISSA) to identify participants with the CISM certification for this study. ISACA is the global association and governing body of the CISM certification and actively promotes research that contributes to IT governance, control, assurance, risks, and produces value that security professionals can use in their organizations. ISSA is a non-profit organization of information security professionals committed to promoting effective global cyber security. Data was collected anonymously using Survey Monkey, an online web-based survey tool. Participants were solicited through email to participate in the web-based survey and directed to a link that launched the survey. Email delivery lowers cost substantially while ensuring faster delivery and allows for ease of analysis for vast amounts of data (McPeake, Bateson, & O'Neill, 2013). There are some limitations associated with using online surveys. Online surveys typically include low response rates that can reduce sample size and statistical

power (Sauermann & Roach, 2013). The use of appropriate sample specification and selection, data processing, screening, and editing can boost the quality of online survey data and yield valid results (Chang & Vowles, 2013). My data collection plan included sending out a follow-up request if my first outreach was unsuccessful in reaching the required range of participants. I allowed a week prior in between sending out follow-up requests. I used five cycles of outreach to participants. I expected a higher return rate due to the role of ISACA and ISSA in the data collection.

The survey questions originated from validated pre-existing survey instruments for which permissions were obtained (Lease, 2005; Putri & Hovav, 2014; Rhee et al., 2012). The utilization of survey instruments that have been previously tested with proven validity and reliability results eliminated the need for a pilot test. Questions to be used for the survey can be found in Appendix D.

Data Organization Techniques

The online data collection process using Survey Monkey was monitored daily for responses. At the end of the data collection period, data was downloaded from Survey Monkey to be stored and analyzed. Data was imported into SPSS for analysis. SPSS files from the analysis will be maintained to ensure research integrity. Data originating from the study will be stored in a secured safe for a period of 5 years and will be destroyed in accordance with established destruction procedures at the end of this period

Data Analysis Techniques

Data analysis procedures and techniques were used to test for the existence of a relationship between the identified variables of this study (security, compliance, and

BYOD implementation). The analysis tested the hypotheses developed from the study's research question: What is the relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation? Data collected via Survey Monkey, the online web-based survey tool, was analyzed to address the research question and hypotheses. According to Gill, Leslie, Grech, and Latour (2013) the use of the Internet as a data collection medium to access research participants has increased as online surveys provide numerous advantages over traditional survey approaches such as high quality data collection, ease and speed of survey administration, and direct communication with participants.

The use of inferential statistics was my preference for this study. According to Bernard (2013), inferential statistics parametric techniques such as t-test, ANOVA, linear regression, and Pearson's coefficient and non-parametric techniques such as Chi-square test, Spearman's rank correlation coefficient, or Mann-Whitney U-test are used for predictive purposes. Descriptive statistics is used to describe data and allows for the examination of the central tendency of data (Jankowski & Flannelly, 2015; Rovai, Baker, & Ponton, 2013). Unlike inferential statistics, descriptive statistics does not allow for making inferences.

According to Nimon and Oswald (2013), multiple regression analysis is used to predict the variation in a dependent variable based on the value of multiple independent variables. I used multiple regression statistical analysis to test for relationships between my variables. I also used Pearson's product moment correlation coefficients to determine the level of relationship between the dependent and independent variables. These are

appropriate statistical tests, as the intent of the study was to examine relationships between multiple predictors (Puth, Neuhäuser, & Ruxton, 2014; Uyanık & Güler, 2013; Sedgwick, 2013b).

I tested the assumptions of multicollinearity, normality, outliers, linearity, and homoscedasticity prior to conducting a full data analysis. An accurate analysis of inferential statistics can only occur if there are no violations of the assumptions (Bernard, 2013). Violations of the assumptions can result in multiple problems such as untrustworthy confidence intervals, biased standard errors, and biased estimates of relationships (Williams, Grajales, & Kurkiewicz, 2013).

Multicollinearity exists when multiple predictors are highly correlated in a multiple regression model (Dormann et al., 2013). I tested multicollinearity by conducting a correlational analysis and reviewing the Variance Inflation Factor (VIF) scores to determine if any multicollinearity issues existed. I also reviewed the correlation coefficients among the predictor variables for multicollinearity. According to Dormann et al. (2013), bivariate correlations exceeding .90 between predictor variables indicate the existence of multicollinearity. I ensured bivariate correlations did not exceed .90 when testing for multicollinearity.

Normality assumes that the populations from which samples are derived are normally distributed (Ghasemi & Zahediasl, 2012). Visual assessment can be used to assess normality (Ghasemi & Zahediasl, 2012). I tested normality by using normal probability plots (P-P) for graphical interpretations of normality.

Homoscedasticity assumes the variance of the dependent variables is the same for all analyzed data (Zolna, Dao, Staszewski, & Barszcz, 2015). Linearity assumes a linear relationship between dependent and independent variables that is represented graphically as a straight line (Osborne & Waters, 2002). I tested these assumptions by using scatterplots. Outliers are deviations whose values differ substantially from other observations in a sample (Williams, 2016).

Bootstrapping is another method that can be used to address violations of these assumptions (Wu & Jia, 2013; Field, 2013). According to Mader, Mader, Sommerlade, Timmer, and Schelter (2013), bootstrapping complements the analytic approaches to the extent of replacing them when they are not possible. I did not have to use SPSS bootstrapping analysis to address violations of these assumptions.

The statistical analysis was conducted using SPSS software. SPSS allows researchers to conduct simple or complex analyses by eliminating the need to learn, understand, and write elaborate code to conduct analyses (Green & Salkind, 2014). It eases the computational burden for researchers (Bernard, 2013). SPSS missing values module allows for the identification and appropriate corrective measures to address missing values after data analysis (Field, 2013).

Reliability and Validity

Reliability and validity is critical to the authenticity of any research. Reliability ensures measures are consistent and repeatable in research (Venkatesh et al., 2013). The following sections will discuss the reliability and validity of instruments as applicable to this study.

Reliability

Reliability is the extent to which measures are error free and therefore yield consistent results (Lakshmi & Mohideen, 2013). It is the degree of consistency between two ratings of the same measurement (Flower, McKenna, & Upreti, 2016). Instruments used for measurement in research are considered reliable when used by other researchers to obtain similar results (Cook, Zendejas, Hamstra, Hatala, & Brydges, 2014). For this study, I developed an instrument that is based on three instruments developed by other researchers that have been proven as reliable through their use by other researchers (Lease, 2005; Putri & Hovav, 2014; Rhee et al., 2012).

Lease (2005) used a test-retest reliability sequence to test the instrument via field trials to ensure its' reliability and validity. The researcher's first test consisted of 42 participants that yielded 36 completed surveys resulting in an 86% response rate. The second test consisted of 36 participants and yielded 36 completed surveys with a response rate of 100% and a .94 Cronbach's alpha for the 16 Likert-scale survey items. The researcher conducted the second test within a two-week to one-month timeframe to ensure the second test results were adequately independent of the first test and to mitigate the potential for test-retest bias. The researcher accomplished this by ensuring the survey items were randomly ordered and that the survey questions did not change for the second test.

Putri and Hovav (2014) survey instrument was primarily adapted from existing scales with some newly developed measures based on results from a pilot test (Vance et al., 2012). The survey instrument consisted of a 7 point Likert scale to measure

participants' level of agreement with the survey's questions. The researchers used the composite reliability statistic to ensure the homogeneity, unidimensionality, and overall reliability of the survey instrument (Peterson & Kim, 2013). A composite value of 0.7 or above is considered acceptable (Kazman, Galecki, Lisman, Deuster, & O'Connor, 2014). An average variance extracted (AVE) value of 0.5 is the minimum acceptable standard while a value of 0.7 is recommended (Fornell & Larcker, 1981; Arenas-Gaitán, Peral-Peral, & Ramón-Jerónimo, 2015; Nimako, Ntim, & Mensah, 2014). The composite reliability value was 0.9 and the AVE value was 0.7. The values of all constructs measured by the survey instrument exceeded the minimum acceptable value levels to prove reliability.

Researchers Rhee et al. (2012) tested the survey instrument for reliability using a Partial Least Squares (PLS) factor analysis framework for reliability and convergent and divergent validity. Good reliability requires composite reliability of at least .70 and AVE of at least .50 (Kazman et al., 2014; Nimako et al., 2014). The composite reliability and AVE for the constructs measured by the survey instrument were .908 and .925, respectively, that indicates good reliability.

Validity

Internal and external validity are important in quantitative research studies. Validity is an indication of a study's legitimacy (Venkatesh et al., 2013). Internal validity is the extent to which inferences can be made about the causal relationship between two variables (Torre & Picho, 2016). External validity is when valid

conclusions obtained from a sample can be generalized to a larger population (Torre & Picho, 2016).

External validity forms the basis of whether the model used, data collected, and results can be generalized to other samples, time periods, and settings (Lancsar & Swait, 2014). Population validity is a threat to external validity when inferences cannot be drawn from the given population of a study due to selection bias (Bevan, Baumgartner, Johnson, & McCarthy, 2013). External validity can be improved by a sample size increase, the selection of a sample population reflective of the general population and a longitudinal study (Bernard, 2013).

Statistical conclusion validity refers to the stability and reliability of statistical analysis from which correct inferences can be made (Gibbs & Weightman, 2014). Statistical conclusion validity is strengthen through: (a) the use of appropriate statistical tests for data analysis, (b) determining an adequate sample size, (c) adequate statistical power and (d) accurate Type I error rates (Barends, Janssen, Have, & Have, 2013; Hales, 2016). Some threats to statistical conclusion validity are: (a) low statistical power, (b) overestimates of effect size and low reproducibility of results, and (c) Type I and Type II error results (Button, Ioannidis, Mokrysz, Nosek, Flint, Robinson, & Munafò, 2013). I addressed the identified threats to statistical conclusion validity by conducting a power analysis prior to research to ensure an adequate statistical power, utilizing substantive theory to guide significant tests in lieu of fishing for findings, and selecting a homogeneous population instead of a random heterogeneity of respondents (Bolte, 2014).

The specific statistical tests I used for this study were multiple linear regression, Pearson product-moment correlation coefficient (Pearson's *r*), and hypothesis testing (Tan, Ooi, Leong, & Lin, 2014; Woodside, 2013). Multiple regression was used to determine the relationship between the dependent and independent variables (Bernard, 2013). Pearson's *r* was used to measure the correlation between the independent and dependent variables and hypothesis testing was used to test the statistical significance of the null and alternative hypotheses (Bernard, 2013; Woodside, 2013).

Transition and Summary

Section 2 discussed my role as the researcher and my strategies for participants' recruitment and data collection. I presented a review of my research methods in which I discussed and compared the various research methods (quantitative, qualitative, and mixed methods) and justified my choice of a quantitative research method. I also discussed my research design (non-experimental correlation design) and provided peer-reviewed information to substantiate my use of this design. I provided information on my sample population and discussed the statistical software used to obtain an appropriate sample size. I described my data collection process, which included discussions on instruments and techniques (collection, organization, and analysis). Finally, I discussed reliability and validity as applicable to this study. Section 3 will provide an analysis of the results obtained from the collected data.

Section 3: Application to Professional Practice and Implications for Change

This study used a correlational quantitative research method to examine the relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation. In this section, the results of the analyses used to answer the research question are presented.

Overview of Study

The purpose of this quantitative correlational study was to analyze the relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation. The G*Power software was used to calculate, *a priori*, the sample size, the error probability, the power, and the number of variables. The calculation results indicated a minimum sample size of 68 participants would be required to achieve a power of .80 while an increase in the sample size to 110 would achieved a power of .95. I used a 32 question online survey to examine the relationship between the independent variables of (a) security, and (b) compliance, and the dependent variable of BYOD implementation. I could not reject the null hypotheses as the analysis indicated there was not a relationship between security, compliance, and intent to implement BYOD.

Presentation of the Findings

In this section, I present the results of the analysis used to answer the research question. I discuss data management procedures, provide descriptive statistics, and present the main analysis. I conclude with a summary of the findings.

Data Management Procedures

The data collected consisted of 94 responses. The data were assessed for missing responses and outliers. There were negligible missing responses, which were managed using the default SPSS likewise deletion method. Outliers were detected using the procedures set forth by Tabachnick and Fidell (2013); standardized (*Z*) scores were calculated and then assessed for responses with values less than -3.29 or greater than +3.29. There were three outliers, which were removed. This resulted in a final dataset of 91 responses to be used in the analyses.

Reliability Analysis

It was necessary to create composite scores to be used in the analyses. The reliability of each composite score was assessed using Cronbach's alpha. Alpha coefficients were interpreted using George and Mallery's (2016) guidelines, where coefficients of .70 and above are considered acceptable, coefficients of .80 and above are good, and coefficients of .90 and above are excellent. Intent to implement BYOD was created from the mean of survey questions 1-16, and had good reliability ($\alpha = .82$). Compliance was created from the mean of survey questions 17-23, and had excellent reliability ($\alpha = .98$). Security was created from the mean of survey questions 24-27, and also had excellent reliability ($\alpha = .96$). Table 2 shows the summarized results.

Table 2

Reliability Statistics

Variables	Cronbach's alpha	*N* of items
Compliance	.967	7
Security	.960	4
Intent to implement BYOD	.818	16

Descriptive Statistics

The sample consisted of CISMs (95.6%) and those with a title of IT manager (21.8%), and a majority had five or more years of experience implementing BYOD (57.5%). The majority worked with an organization that supports more than 500 users (51.7%). Primarily, the largest proportion worked in IT services (26.4%). Missing (4.4%) indicates participants who did not answer the demographic questions but answered all other questions on the survey. It is not known if they fit the demographic or not or why they didn't answer as they were assumed to be a part of the demographic. I indicate that there is a possibility that a small sample may or may not have been a part of the demographic. Table 3 presents all frequencies and percentages.

Table 3

Frequencies and Percentages of Demographic Characteristics

Variable		n	%
Certified Information Security Manager (CISM)	Yes	87	95.6
	No	0	0.0
	Missing	4	4.4
Title	CIO	3	3.4
	CTO	2	2.3
	CISO	7	8.0
	Information Assurance Manager	17	19.5
	IT Director	2	2.3
	IT Manager	19	21.8
	IT Supervisor or Lead	10	11.5
	Other Director	4	4.6
	Other Manager	12	13.8
	None of the Above	11	12.6
	Missing	4	4.4
Experience Implementing BYOD	None	2	2.3
	Less than five years	5	5.7
	Two years to less than five years	30	34.5
	Five years or more	50	57.5
	Missing	4	4.4
Users supported by Organization	Less than 50 users	4	4.6
	50 to 249	9	10.3
	250 to 500	29	33.3
	More than 500	45	51.7
	Missing	4	4.4

(*table continues*)

Variable		n	%
Primary Business or Industry	Education	5	5.7
	Energy/Utilities	3	3.4
	Financial Services/Banking	10	11.5
	Government	17	19.5
	State	7	8
	Health Care	8	9.2
	Information Technology- Services	23	26.4
	Information Technology- Manufacturing	4	4.6
	Retail	1	1.1
	Telecommunications	1	1.1
	Travel/Leisure/Hospitality	5	5.7
	Wholesale Distribution and Services	1	1.1
	Other	2	2.3
	Missing	4	4.4

Participants scored an average of 4.24 (*SD* = 0.47) in compliance, which corresponds to a response slightly higher than "I agree." Participants scored an average of 3.42 (*SD* = 1.33) in security, which corresponds to a response between "somewhat low" and "average." For intent to implement BYOD, participants scored an average of 2.75 (*SD* = 0.52), which corresponds to an average response of between "disagree" and "neutral." All ranges, means, and standard deviations are presented in Table 4.

Table 4

Means and Standard Deviations for Study Variables

Variable	Min	Max	*M*	*SD*
Compliance	3.00	5.00	4.24	0.47
Security	1.00	6.00	3.42	1.33
Intent to implement BYOD	2.00	4.31	2.75	0.52

Analysis

RQ: What is the relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation?

H_0:There is not a relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation.

H_1: There is a relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation.

This research question was answered using a multiple linear regression and a series of Pearson's correlations. The multiple linear regression is the appropriate analysis to perform when seeking to assess the relationship between one or more continuous or categorical independent (predictor) variables and a continuous dependent variable (Field, 2013). As such, it is the appropriate analysis to perform to either accept or reject the null hypothesis. In this analysis, the continuous dependent variable is intent to implement BYOD. The continuous predictor variables are security and compliance. The Pearson correlations were used to gather additional information about the intercorrelations between all three variables.

Assumptions

Prior to the analysis, the assumptions of the multiple linear regression were assessed. These assumptions include normality, homoscedasticity, linearity, and absence of multicollinearity. In this subsection, I present the findings that support these assumptions.

Normality. Normality was assessed through a normal P-P plot of the residuals. Data points that generally follow the diagonal normality line indicate that normality can be assumed (Tabachnick & Fidell, 2013). Figure 2 provides a graphical representation of this assumption.

Homoscedasticity and linearity. Homoscedasticity and linearity were assessed through a scatterplot of the residuals indicating the assumptions of homoscedasticity and linearity were met. Data points that are generally evenly distributed about the zero-line in a block-shaped random pattern indicate that the assumptions of homoscedasticity and linearity are met (Stevens, 2009). Figure 3 provides a graphical representation.

Multicollinearity. Absence of multicollinearity was assessed through Variance Inflation Factor (VIF) values. All VIF values were below 5 indicating the assumption of multicollinearity was met (Stevens, 2009). Table 5 depicts the VIF values.

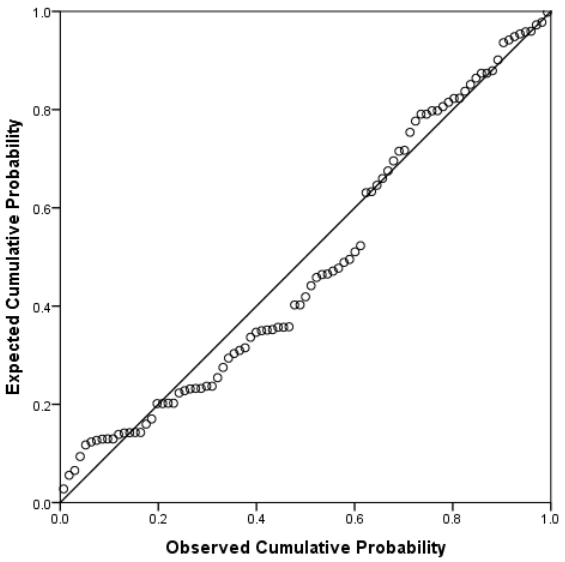

Figure 2. Normal P-P plot of the residuals.

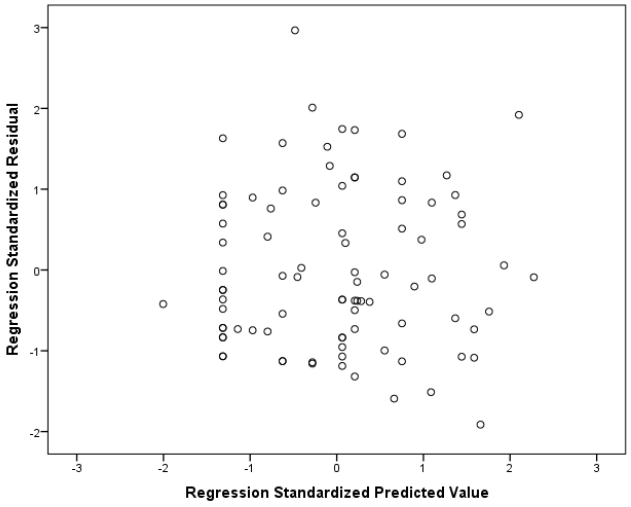

Figure 3. Scatterplot of the residuals.

The results of the overall regression model were not significant, $F(2, 86) = 0.33$, $p = .718$, $R^2 = .00$. This indicates that there is not a relationship between the combined values of security and compliance and the dependent variable of intent to implement BYOD. Due to nonsignificance of the overall model, the individual predictor variables were not further examined. As the regression was not significant, the null hypotheses cannot be rejected. Table 5 presents the full results of this analysis.

Table 5

Results of the Regression Analysis

Variable	*B*	*SE*	β	*t*	*p*	VIF
Compliance	0.00	0.13	0.06	0.55	.584	1.07
Security	0.00	0.04	0.08	0.72	.472	1.07

Although the regression results did not provide evidence of a relationship, the Pearson correlations were continued in an exploratory manner. Bivariate Pearson correlations were conducted between the variables of compliance, security, and intent to implement. The assumptions of the Pearson correlation, normality and linearity, were previously assessed in the analysis of the regression model. Pearson correlations range from -1.00 to 1.00, where values closer to the absolute value of 1.00 indicate stronger associations (Field, 2013). Negative values indicate relationships that are negative or inverse (i.e., as one variable increases, the other decreases; Field, 2013). Positive values indicate relationships that are positive (i.e., as one variable increases, the other also increases; Field, 2013). Coefficient values may be interpreted through Cohen's standard where values between .10 and .29 are considered small or weak, values between .30 and .49 are considered medium, and values of .50 and above are considered large or strong (Cohen, 1988).

The results of the correlations are presented in Table 6. The only significant correlation was between security and compliance (r = -.26, p = .016). This is a small, negative association, which indicates that security and compliance are weakly negatively correlated. In other words, as security increased (i.e., as participants indicated less concern about security risks), compliance tended to decrease.

Table 6

Pearson Correlation Matrix

Variables	Compliance	Security	Intent to implement
Compliance	-		
Security	-.26*	-	
Intent to implement BYOD	.03	0.07	-

*indicates significance at .05 level.

Summary

A multiple linear regression was performed in order to assess the research question. The multiple linear regression was not significant, indicating that there is not a relationship between compliance, security, and intent to implement BYOD. The null hypotheses cannot be rejected. A Pearson correlation was performed with the intent to explore the bivariate relationships amongst all the variables. A significant negative relationship was found between security and compliance indicating a weakly negative correlation.

Theoretical Conversation on Findings

I used systems theory developed by Von Bertalanffy (1972) as the theoretical framework for this study. Von Bertalanffy (1972) defined systems theory as the interdisciplinary study of systems and the interrelationships between their separate components. The systems theory framework was appropriate for this study as the goal was to examine the relationship between the independent variables of security and compliance and the dependent variable of BYOD implementation.

The analysis of the data collected from the survey produced findings that showed a relationship did not exist between the combined values of compliance, security, and

intent to implement BYOD from an interrelated perspective in the context of the system theory fram ework. However, the model did show a significant negative relationship between the independent variables of security and compliance.

In Section 1, I discussed the application of systems theory in several studies to address interrelationships, a core construct of the systems theory framework. Systems theory was used as the basis for proposing a systems theory construct with systems theory as the theoretical foundation for understanding multidisciplinary systems (Adams, Hester et al., 2014); a psychotherapy study to examine the complex interactions at work within individuals (Trop et al., 2013); a legal pluralism study to examine the relationship between state law and violence, the issue of translation between disparate legal orders, and the differences between modern and pre-modern societies (Nobles & Schiff, 2012); and a study to identify and articulate interrelated components that positively or negatively impacted the effectiveness of health care interventions or programs (Adams, Jones et al., 2014).

In a study conducted by Hovav and Putri (2016) to examine employees' intent to comply with an organizational BYOD policy, the results showed that the independent variables of perceived threat appraisal, perceived response efficacy, and perceived digital mutualism justice significantly and positively affected employees' intent to comply with an organizational BYOD policy. The results highlighted the interrelationship of these independent variables to the dependent variable of employees' intent to comply with an organizational BYOD policy, thereby, signifying a key tenet of the system theory framework that is interrelationship between objects. The results of my study related to

information security managers' compliance toward an organizational BYOD policy were similar to these results as information security managers scored an average which corresponded to a response slightly higher than "I agree" in regards to compliance with an organizational BYOD policy. Additionally, the results of Hovav and Putri (2016) study showed the independent variable of perceived freedom threat had a significant negative relationship with the dependent variable of employees' intent to comply with an organizational policy. This is also similar to the type of significant negative relationship found in my study between the independent variables of security and compliance that indicated as security increased, compliance tended to decrease.

Rhee et al. (2012) conducted a study to address the phenomenon that increased vulnerability to information security breaches is coupled with the low level of managerial awareness and commitment in regards to information security threats. Participants of the study were MIS executives. The independent variables of perceived risk and perceived controllability of information security threats indicated a relationship with the low level of managerial awareness and commitment toward information security threats that also highlighted the interrelationship construct of the systems theory framework. The results of the study suggested that MIS executives demonstrate unrealistic optimism in perceiving risk and controllability associated with their organization's information security threats meaning that they perceived their information security risk as being lower and their own controllability of information security much higher than that of comparison targets in the study. Similarly, in my study, information security managers scored an

average that corresponded to a response between “somewhat low” and “average” related to organizational security perceptions.

The results of the study showed that information security managers did not fully embrace the concept of BYOD although it is a fast growing phenomenon. It may be worth exploring and examining the results from other theoretical perspectives. The TAM may provide an explanation, as it is a theoretical framework used by researchers to examine and predict the adoption of technology by individuals (Brezavscek, Sparl, & Znidarsic, 2014). Similarly, the UTAUT may also provide an explanation as it consists of four constructs that influence behavioral intention to use a technology (Lescevica, Ginters, & Mazza, 2013). Both of these theoretical frameworks are described as supporting theories to system theory in this study.

Applications to Professional Practice

The purpose of this study was to examine the relationship between information security managers’ intentions, perceptions of security, and compliance regarding BYOD implementation. Survey data were collected from information security managers that had obtained the CISM certification, as this demonstrates expertise in the areas of security and compliance in the context of an organization’s information security program and the alignment to its goals and objectives. The statistical results of the study showed that a relationship did not exist between security, compliance and the dependent variable of BYOD implementation. I observed a significant negative relationship between security and compliance through regression analysis.

The results of the data collected indicate that information security managers have some reservations toward implementing BYOD although it is gaining prominence and acceptance. Statistical results showed information security managers that participated in this study mostly disagreed or were neutral toward BYOD implementation. Additionally, participants showed a strong inclination for compliance toward BYOD in the context of an organization's BYOD information systems security policy while indicating a somewhat low and average risk from information security threats within their respective organizations. While there are many benefits afforded by BYOD for both employees and organizations, the data results highlight challenges related to implementing BYOD as indicated by the participants of this study.

This study may serve as a basis for researchers to conduct further studies to examine the relationship between the variables of security, compliance, and intent to implement BYOD. From a practical standpoint, compliance and security tend to be considered in the implementation of most IT solutions. In terms of this particular population's perception, the results indicated a relationship did not exist between these variables considering the study was based on the premise that IT leaders often lack the knowledge of the relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation. As organizations develop strategies toward BYOD implementation, they shouldn't focus on these variables. The results of the study do provide statistical data that may be used by IT leaders to develop strategies toward BYOD implementation and also contribute to the existing literature on BYOD.

Implications for Social Change

The implications for social change are individuals participating in a BYOD program could apply the same knowledge, practices, and security measures toward securing the personal devices of family members, thereby, reducing potential risks, including the loss of personal data. It was assumed that the results of this study might potentially lead to the development of best business practices toward the protection of personal devices and a reduction in costs associated with security and data breaches that could prove beneficial for consumers. Instead, the results showed that participants of the study mostly disagreed or were neutral toward BYOD implementation implying that these participants might be resistant to implementing BYOD within their respective organizations even if it was driven by senior management. However, the results of the study also showed that participants had a strong inclination toward compliance with an organization's BYOD information systems security policy indicating an understanding of the criticality of their role in the protection of organizational and private data, hence, the transferability of this knowledge towards the protection of family members' personal devices..

Recommendations for Action

The recommendations from this study begin with recommending IT leaders within organizations take some time to gain an understanding and awareness of information security managers' intentions and perceptions toward BYOD implementation. This can be accomplished through the use of surveys, focus groups, and sensing sessions. Understanding the perspectives of information security managers

toward BYOD will enable technology leaders to develop strategies, formulate plans, and make informed decisions toward BYOD implementation.

Information security managers should also become more familiar with BYOD and its' implementation as it is gaining prominence. They need to understand the benefits BYOD affords an organization and be able to develop holistic solutions to address challenges associated with its' implementation from a security perspective. This can be accomplished by reviewing lessons learned from peers in other organizations that have implemented BYOD successfully.

Additionally, security awareness training for employees should be a critical component for a BYOD program. A concerted effort should be made to ensure employees understand the potential security and legal challenges that could arise due to the comingling of organizational and private data on a personal mobile device and how they can protect the data. Organizations should ensure security awareness training for employees is effective.

I will share the results of this study with the Presidents of the local ISACA chapters from which participants were surveyed. I will also share the results with ISACA and its research department, as they are the governing body for CISMs. Sharing the results with ISACA presents a potential opportunity for the results of the study being shared at conferences or ISACA training events. Lastly, the results of the study can be disseminated through peer-reviewed publishing.

Recommendations for Further Study

There were some limitations to the study. The first limitation is that the study was limited to only information security managers that had obtained the CISM certification. I recommend future studies include information security managers with certifications other than the CISM such as the Certified Information Systems Security Professional and Certified in Risk and Information Systems Control certifications. Future studies could also include a broader range of IT professionals who do not necessarily hold a security related certification as they could potentially provide other perspectives related to BYOD implementation that are not solely security focused. Further studies could also incorporate the use of other theoretical frameworks such as the theory of planned behavior, the TAM, and the UTAUT.

Another limitation is that a non-probabilistic convenience sample was used for the study that limits the opportunity for all qualified individuals in the target population, and study results are not necessarily generalizable to this population. Future studies could employ the use of purposive sampling in which participants of other specific groups are purposefully sought after to address the same research question and hypotheses of this study to determine if the results would be similar or produce a different outcome. Future studies could also be conducted using probabilistic sampling such as random sampling wherein all members of a population have an equal chance of being selected

Outside the scope of this study, researchers could try to understand the intentions of other populations toward BYOD implementation. Populations such as educators, health practitioners, and marketing executives could be researched to determine their

intentions and perceptions toward BYOD implementation. Researchers could expand futue studies toward BYOD implementation to other geographic locations to determine if the results obtained in multiple geographic locations are similar or dissimilar to the results of this study. During my research for this study, I came across several research materials with potential variables related to BYOD that could also be researched further. Potential variables such as governance, privacy, and legal challenges could be included in future research related to BYOD implementation. Lastly, future researchers could use this study as a basis to conduct further research using other potential theoretical frameworks to address the challenges of implementing BYOD.

Reflections

The DIT doctoral study process has been a rewarding challenge. I was able to learn how to conduct scholarly academic research and understand its implications and contributions toward society. I found the DIT residencies hosted by Walden University to be very beneficial in shaping my research focus, establishing my research foundation, and helping me gain an understanding of quantitative, qualitative, and mixed methods research methodologies. I gained a tremendous amount of respect for the rigors associated with academic research especially the data collection and data analysis phases of research.

Although I had some knowledge of the systems theory framework used in this study, my knowledge of this theoretical framework was further expanded as I worked on the literature review. I was able to delve into the evolution of this theoretical framework

and its application by other researchers in their studies. I also gained an appreciation of other theories that were both supportive and in contrast to systems theory.

I went through several iterations of the Institutional Review Board process prior to gaining approval (no. 04-30-17-0462376). I found the evaluators to be strict, however, helpful in their evaluations and comments. Any potential biases or preconceived ideas and values I may have had as an information security professional who holds the CISM certification was mitigated through the use of an anonymous online survey that ensured I did not have any direct interaction with participants of the study.

After completing this study, I've come to the realization that there are many perspectives related to BYOD implementation and that information security managers are not monolithic in their intentions toward implementing BYOD. While I have my views and opinions about the BYOD phenomenon, it was interesting to discover that there are other information security professionals with views and opinions that are quite the opposite. I believe the BYOD phenomenon offers opportunities and challenges that are yet to be researched, evaluated, and analyzed in future studies

Summary and Study Conclusions

The goal of this study was to examine the relationship between information security managers' intentions, perceptions of security, and compliance regarding BYOD implementation. Although the results of the study showed that there was not a relationship between compliance, security, and intent to implement BYOD and the null hypotheses could not be rejected, the model showed a significant negative relationship between security and compliance which indicates these variables could be examined

further in order to understand and address the challenges associated with implementing BYOD. Further studies could employ research methodologies, research designs, variables, and theoretical frameworks not used in this study. As indicated in the literature review, BYOD presents both opportunities and challenges for organizations and employees. The challenges must be addressed if the benefits afforded by BYOD are to be experienced fully.

References

Adams, K. M., Hester, P. T., Bradley, J. M., Meyers, T. J., & Keating, C. B. (2014). Systems theory as the foundation for understanding systems. *Systems Engineering*, *17*(1), 112–123. doi:10.1002/sys.21255

Adams, R., Jones, A., Lefmann, S., & Sheppard, L. (2014). Utilising a collective case study systems theory mixed methods approach: A rural health example. *BMC Medical Research Methodology, 14*, 1-9. doi:10.1186/1471-2288-14-94

Adomavicius, G., Bockstedt, J. C., Gupta, A., & Kauffman, R. J. (2007). Technology roles and paths of influence in an ecosystem model of technology evolution. *Information Technology and Management, 8*, 185-202. doi:10.1007/s10799-007-0012-z

Ajzen, I., & Sheikh, S. (2013). Action versus inaction: Anticipated affect in the theory of planned behavior. *Journal of Applied Social Psychology*, *43*(1), 155–162. doi:10.1111/j.1559-1816.2012.00989.x

Ansaldi, H. (2013). Addressing the challenges of the 'bring your own device' opportunity. *CPA Journal*, *83*, 63-65. Retrieved from http://www.cpajournal.com/

Arenas-Gaitán, J., Peral-Peral, B., & Ramón-Jerónimo, M. A. (2015). Elderly and internet banking: An application of UTAUT2. *Journal of Internet Banking and Commerce*, *20*(1). doi.org/10.1007/978-3-531-92534-9_12

Armitage, C. J., Conner, M., Loach, J., & Willetts, D. (1999). Different perceptions of control: Applying an extended theory of planned behavior to legal and illegal drug use. *Basic and Applied Social Psychology, 21,* 301-316. Retrieved from http://www.tandf.co.uk/journals/titles/01973533.asp

Astani, M., Ready, K., & Tessema, M. (2013). BYOD issues and strategies in organizations. *Issues in Information Systems, 14,* 346-352. Retrieved from http://www.iacis.org/iis/iis.php

Barends, E., Janssen, B., Have, W. ten, & Have, S. ten. (2013). Difficult but doable: Increasing the internal validity of organizational change management studies. *Journal of Applied Behavioral Science*, *50*(1), 50-54. doi:10.1177/0021886313515614

Barry, A. E., Chaney, B., Piazza-Gardner, A. K., & Chavarria, E. A. (2014). Validity and reliability reporting practices in the field of health education and behavior: A review of seven journals. *Health Education & Behavior*, *41*(1), 12–8. doi:10.1177/109019811348313

Beckett, P. (2014). BYOD - popular and problematic. *Network Security*, *2014*(9), 7-9. doi:10.1016/S1353-4858(14)70090-X

Beham, B., Baierl, A., & Poelmans, S. (2014). Managerial telework allowance decisions – a vignette study among german managers. *International Journal of Human Resource Management, 26,* 1-22. doi:10.1080/09585192.2014.934894

Belanger, F., Watson-Manheim, M. B., & Swan, B. R. (2013). A multi-level socio-technical systems telecommuting framework. *Behaviour and Information Technology*, *32*, 1257–1279. doi:10.1080/0144929X.2012.705894

Bernard, H. R. (2013). *Social research methods: Qualitative and quantitative approaches* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Bevan, S., Baumgartner, F. R., Johnson, E. W., & McCarthy, J. D. (2013). Understanding selection bias, time-lags and measurement bias in secondary data sources: Putting the encyclopedia of associations database in broader context. *Social Science Research*, *42*, 1750-1764. doi:10.1016/j.ssresearch.2013.08.003

Bojanc, R., & Jerman-Blažič, B. (2013). A quantitative model for information-security risk management. *Engineering Management Journal*, *25*, 25-37. doi:10.1080/10429247.2013.11431972

Bolte, S. (2014). The power of words: Is qualitative research as important as quantitative research in the study of autism? *Autism, 18*, 67–68. doi:10.1177/1362361313517367

Bosua, R., Gloet, M., Kurnia, S., Mendoza, A., & Yong, J. (2013). Telework, productivity and wellbeing. *Telecommunications Journal of Australia*, *63*(1). doi:10.7790/tja.v63i1.390

Brezavscek, A., Sparl, P., & Znidarsic, A. (2014). Extended technology acceptance model for SPSS acceptance among slovenian students of social sciences. *Organizacija*, *47*, 116-127. doi:10.2478/orga-2014-0009

Button, K. S., Ioannidis, J. P. A., Mokrysz, C., Nosek, B. A., Flint, J., Robinson, E. S. J., & Munafò, M. R. (2013). Power failure: why small sample size undermines the reliability of neuroscience. *Nature Reviews Neuroscience*, *14*, 365–376. doi:10.1038/nrn3475

Car, T., Pilepić, L., & Šimunić, M. (2014). Mobile technologies and supply chain management - lessons for the hospitality industry. *Tourism and Hospitality Management, 20*, 207-219. Retrieved from http://www.fthm.hr/

Castro-Leon, E. (2014). Consumerization in the IT service ecosystem. *IT Professional*, *16*, 20-27. doi:10.1109/MITP.2014.66

Chang, J. M., Ho, P., & Chang, T. (2014). Securing BYOD. *IT Professional*, *16*, 9-11. doi:10.1109/MITP.2014.76

Chang, T. Z., & Vowles, N. (2013). Strategies for improving data reliability for online surveys: A case study. *International Journal of Electronic Commerce Studies, 4*(1), 121-130. doi:10.7903/ijecs.1121

Cheng, G., Guan, Y., & Chau, J. (2016). An empirical study towards understanding user acceptance of bring your own device (BYOD) in higher education. *Australasian Journal of Educational Technology*, *32*(4), 1–17. doi:10.14742/ajet.279

Cheung, R., & Vogel, D. (2013). Predicting user acceptance of collaborative technologies: An extension of the technology acceptance model for e-learning. *Computers and Education*, *63*, 160-175. doi:10.1016/j.compedu.2012.12.003

Chiumento, A., Khan, M. N., Rahman, A., & Frith, L. (2016). Managing ethical challenges to mental health research in post-conflict settings. *Developing World Bioethics*, *16*(1), 15-28. doi:10.1111/dewb.12076

Cho, I., & Lee, K. (2016). Advanced risk measurement approach to insider threats in cyberspace. *Intelligent Automation and Soft Computing*, *22*, 405–413. doi:10.1080/10798587.2015.1121617

Coates, S. (2014). BYOD business issues. *Internal Auditor*, *71*(1), 21-23. Retrieved from http://www.theiia.org/intauditor/

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). St. Paul, MN: West Publishing Company.

Cokley, K., & Awad, G. (2013). In defense of quantitative methods: Using the "master's tools" to promote social justice. *Journal for Social Action in Counseling and Psychology*, *5*(2), 26–41. Retrieved from http://www.psysr.org

Cook, D. A., Zendejas, B., Hamstra, S. J., Hatala, R., & Brydges, R. (2014). What counts as validity evidence? Examples and prevalence in a systematic review of simulation-based assessment. *Advances in Health Sciences Education*, *19*, 233–250. doi:10.1007/s10459-013-9458-4

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory bridging the intention-behavior gap. *Journal of Information Systems*, *28*(1), 209-226. doi:10.2308/isys-50704

Dalpiaz, F., Giorgini, P., & Mylopoulos, J. (2013). Adaptive socio-technical systems: A requirements-based approach. *Requirements Engineering*, *18*(1), 1-24. doi:10.1007/s00766-011-0132-1

Dasgupta, M. (2015). Exploring the relevance of case study research. *Vision: Journal of Business Perspective*, *19*, 147–160. doi:10.1177/0972262915575661

Davis, M. C., Challenger, R., Jayewardene, D. N. W., & Clegg, C. W. (2014). Advancing socio-technical systems thinking: A call for bravery. *Applied Ergonomics*, *45*, 171-180. doi:10.1016/j.apergo.2013.02.009

Dehejia, R. (2015). Experimental and non-experimental methods in development economics: A porous dialectic. *Journal of Globalization and Development, 6*(1), 47-69. doi:10.1515/jgd-2014-0005

De Kock, R., & Futcher, L. A. (2016). Mobile device usage in higher education institutions in South Africa. *Proceedings of the 2016 Information Security for South Africa (ISSA) meeting, Johannesburg, South Africa* (pp. 27–34). doi:10.1109/ISSA.2016.7802925

de las Cuevas, P., Mora, A. M., Merelo, J. J., Castillo, P. A., Garcia-Sannchez, P., & Fernandez-Ares, A. (2015). Corporate security solutions for BYOD: A novel user-centric and self-adaptive system. *Computer Communications*, *68*, 83–95. doi:10.1016/j.comcom.2015.07.019

Dhingra, M. (2016). Legal issues in secure implementation of bring your own device (BYOD). *Procedia Computer Science, 78,* 179-184. doi:10.1016/j.procs.2016.02.030

Disterer, G., & Kleiner, C. (2013). BYOD bring your own device. *Procedia Technology, 9,* 43-53. doi:10.1016/j.protcy.2013.12.005

Dormann, C. F., Elith, J., Bacher, S., Buchmann, C., Carl, G., Carré, G., . . . Marquéz, J. R. G., (2013). Collinearity: A review of methods to deal with it and a simulation study evaluating their performance. *Ecography, 36*(1), 27-46. doi:10.1111/j.1600-0587.2012.07348.x

Duane, B. T., & Satre, M. E. (2014). Utilizing constructivism learning theory in collaborative testing as a creative strategy to promote essential nursing skills. *Nurse Education Today, 34*(1), 31–34. doi:10.1016/j.nedt.2013.03.005

Elo, S., Kaariainen, M., Kanste, O., Polkki, T., Utriainen, K., & Kyngas, H. (2014). Qualitative content analysis: A focus on trustworthiness. *SAGE Open, 4*(1), 1-10. doi:10.1177/2158244014522633

Emerson, R. W. (2015). Convenience sampling, random sampling, and snowball sampling: How does sampling affect the validity of research? *Journal of Visual Impairment & Blindness, 109,* 164-168. Retrieved from http://www.afb.org/info/publications/jvib/12

Enonbun, O. (2010). Constructivism and web 2.0 in the emerging learning era: A global perspective. *Journal of Strategic Innovation and Sustainability, 6,* 17-28. Retrieved from http://www.na-businesspress.com/jsisopen.html

Fassinger, R., & Morrow, S. L. (2013). Toward best practices in quantitative, qualitative, and mixed- method research: A social justice perspective. *Journal for Social Action in Counseling & Psychology, 5*(2), 69–83. Retrieved from http://www.psysr.org/jsacp/social-action-authors.htm

Faul, F., Erdfelder, E., Buchner, A., & Lang, A. -G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods, 41,* 1149-1160. doi:10.3758/brm.41.4.1149

Field, A. (2013). *Discovering statistics using IBM SPSS statistics* (4th ed.). London, England: SAGE Publications.

Fiorenza, P. (2013). Mobile technology forces study of bring your own device. *Public Manager, 42*(1), 12-14. Retrieved from http://www.astd.org/

Fiske, S. T., & Hauser, R. M. (2014). Protecting human research participants in the age of big data. *Proceedings of the National Academy of Sciences, 111*(38), 13675–13676. doi:10.1073/pnas.1414626111

Flower, A., McKenna, J. W., & Upreti, G. (2016). Validity and reliability of GraphClick and DataThief III for data extraction. *Behavior Modification, 40,* 396-413. doi:10.1177/0145445515616105

Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18,* 39-50. doi:10.2307/3151312

Gaff, B. M. (2015). BYOD? OMG! *Computer, 48,* 10-11. doi:10.1109/MC.2015.34

Garba, A. B., Armarego, J., & Murray, D. (2015). Bring your own device organisational information security and privacy. *ARPN Journal of Engineering and Applied Sciences, 10,* 1279-1287. Retrieved from http://www.arpnjournals.com/jeas/

Gehlert, K. M., Ressler, T., & Baylon, D. (2013). Global challenges demand global education of systems thinking. *Human Systems Management, 32*(2), 79–84. doi:10.3233/HSM-120777

George, D. & Mallery, P. (2016). *SPSS for Windows step by step: a simple guide and reference, 15.0 update* (14th ed.). New York, NY: Routledge.

Ghasemi, A., & Zahediasl, S. (2012). Normality tests for statistical analysis: A guide for non-statisticians. *International Journal of Endocrinology and Metabolism, 10,* 486-489. doi:10.5812/ijem.3505

Ghosh, A., & Rai, P. K. G. S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science, 4,* 62-70. Retrieved from http://www.jgrcs.info/index.php/jgrcs

Gibbs, N. M., & Weightman, W. M. (2014). An audit of the statistical validity of conclusions of clinical superiority in anaesthesia journals. *Anaesthesia and Intensive Care, 42*(5), 599–607. Retrieved from http://www.aaic.net.au

Gill, F. J., Leslie, G. D., Grech, C., & Latour, J. M. (2013). Using a web-based survey tool to undertake a Delphi study: *Application for nurse education research. Nurse Education Today, 33,* 1322-1328. doi:10.1016/j.nedt.2013.02.016

Green, S. B., & Salkind, N. J. (2014). *Using SPSS for windows and macintosh: Analyzing and understanding data* (7th ed.). Upper Saddle River, NJ: Pearson.

Hales, A. H. (2016). Does the conclusion follow from the evidence? Recommendations for improving research. *Journal of Experimental Social Psychology, 66,* 39-46. doi:10.1016/j.jesp.2015.09.011

Hall, H., Griffiths, D., & McKenna, L. (2013). From Darwin to constructivism: The evolution of grounded theory. *Nurse Researcher, 20,* 17–21. doi:10.7748/nr2013.01.20.3.17.c9492

Harris, J., Ives, B., & Junglas, I. (2012). IT consumerization: When gadgets turn into enterprise IT tools. *MIS Quarterly Executive, 11,* 99-112. Retrieved from http://www.misqe.org

Hasking, P., & Schofield, L. (2015). Examining alcohol consumption with the theory of planned behaviour: Do health and alcohol knowledge play a role? *Psychology, Health and Medicine, 20,* 838–845. doi:10.1080/13548506.2014.969748

Hovav, A., & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing, 32,* 35-49. doi:10.1016/j.pmcj.2016.06.007

Huang, J., & Martin-Taylor, M. (2013). Turnaround user acceptance in the context of HR self-service technology adoption: an action research approach. *International Journal of Human Resource Management, 24,* 621-642. doi:10.1080/09585192.2012.677460

Hughes, B. P., Newstead, S., Anund, A., Shu, C. C., & Falkmer, T. (2015). A review of models relevant to road safety. *Accident Analysis and Prevention, 74,* 250-270. doi:10.1016/j.aap.2014.06.003

Hung, S.-Y., Chang, C.-M., & Kuo, S.-R. (2013). User acceptance of mobile e-government services: An empirical study. *Government Information Quarterly, 30,* 33–44. doi:10.1016/j.giq.2012.07.008

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security, 31*(1), 83-95. doi:10.1016/j.cose.2011.10.007

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

Jackson, R. A. (2013). Audit in a digital business world. *Internal Auditor, 70*, 36-41. Retrieved from http://www.theiia.org/ecm/magazine.cfm?doc_id=540

Jankowski, K. R. B., & Flannelly, K. J. (2015). Measures of central tendency in chaplaincy, health care, and related research. *Journal of Health Care Chaplaincy, 21*(1), 39–49. doi:10.1080/08854726.2014.989799

Jansson, N. (2013). Organizational change as practice: A critical analysis. *Journal of Organizational Change Management, 26*, 1003–1019. doi:10.1108/JOCM-09-2012-0152

Jondle, D., Maines, T. D., Burke, M. R., & Young, P. C. (2013). Modern risk management through the lens of the ethical organizational culture. *Risk Management, 15*(1), 32-49. doi:10.2307/23351535

Jones, B. H., Chin, A. G., & Aiken, P. (2014). Risky business: Students and smartphones. *TechTrends: Linking Research and Practice to Improve Learning*, *58*, 73–83. doi:10.1007/s11528-014-0806-x

Joshi, A., Kale, S., Chandel, S., & Pal, D. (2015). Likert scale: Explored and explained. *British Journal of Applied Science & Technology, 7*, 396-403. doi:10.9734/BJAST/2015/14975

Jovanovikj, V., Gabrijelcic, D., & Klobucar, T. (2014). A conceptual model of security context. *International Journal of Information Security*, *13*, 571–581. doi:10.1007/s10207-014-0229-x

Judkins-Cohn, T. M., & Kielwasser-Withrow, K. (2014). Ethical principles of informed consent: Exploring nurses' dual role of care provider and researcher. *Journal of Continuing Education in Nursing*, *4545*, 35-42. doi:10.3928/00220124-20131223-03

Karanja, E., & Zaveri, J., (2012). IT Leaders: Who are they and where do they come from?. *Journal Of Information Systems Education, 23*(2), 143-163. Retrieved from: http://www.jise.appstate.edu

Karniouchina, E. V., Carson, S. J., Short, J. C., & Ketchen, D. J. (2013). Extending the firm vs. industry debate: Does industry life cycle stage matter? *Strategic Management Journal*, *34*(8), 1010-1018. doi:10.1002/smj.2042

Kast, F. E., & Rosenzweig, J. E. (1972). General system theory: Applications for organization and management. *Academy of Management Journal, 15*, 447-465. doi:10.2307/255141

Kazman, J. B., Galecki, J. M., Lisman, P., Deuster, P. A., & O'Connor, F. G. (2014). Factor structure of the functional movement screen in marine officer candidates. *Journal of Strength and Conditioning Research, 28,* 672–678. doi:10.1519/JSC.0b013e3182a6dd83

Kiernan, M.D. (2016). Legal ethics and concerns with security in a bring your own device program. *Issues in Information Systems, 17,* 254. Retrieved from http://www.iacis.org/iis/iis.php

Kim, G., Lim, J., & Kim, J. (2016). Secure user authentication based on the trusted platform for mobile devices. *EURASIP Journal on Wireless Communications and Networking*, *2016*(1), 1-15. doi:10.1186/s13638-016-0729-7

Kim, S., Jeong, S. H., & Hwang, Y. (2013). Predictors of pro-environmental behaviors of American and Korean students: The application of the theory of reasoned action and protection motivation theory. *Science Communication, 35,* 168-188. doi:10.1177/1075547012441692

Kivipõld, K., & Vadi, M. (2013). Market orientation in the context of the impact of leadership capability on performance. *International Journal of Bank Marketing*, *31*(5), 368-387.

Kull, T. J., Ellis, S. C., & Narasimhan, R. (2013). Reducing behavioral constraints to supplier integration: A socio-technical systems perspective. *Journal of Supply Chain Management*, *49*(1), 64-86. doi:10.1111/jscm.12002

Lakshmi, S., & Mohideen, M. A. (2013). Issues in reliability and validity of research. *International Journal of Management Research and Reviews, 3,* 2752-2758. Retrieved from http://ijmrr.com

Lancsar, E., & Swait, J. (2014). Reconceptualising the external validity of discrete choice experiments. *PharmacoEconomics, 32,* 951-965. doi:10.1007/s40273-014-0181-7

Laszlo, E. (1987). *Evolution –the grand synthesis*. Boston, MA: New Science Library

Laszlo, A., & Krippner, S. (1998). Systems theories: Their origins, foundations, and development. In G. E. Stelmach (Series Ed.) *Advances in psychology*, J. S. Jordan (Ed.), Systems theories and a priori aspects of perception (Vol. 126, pp. 47-74). doi:10.1016/S0166-4115(98)80017-4

Lease, D. R. (2005). *Factors influencing the adoption of biometric security technologies by decision-making information technology and security managers* (Doctoral dissertation). Available from ProQuest Dissertations & Theses Global. (UMI No. 3185680)

Leavitt, N. (2013). Today's mobile security requires a new approach. *Computer, 46*, 16–19. doi:10.1109/MC.2013.400

Leclercq-Vandelannoitte, A. (2015). Leaving employees to their own devices: new practices in the workplace. *Journal of Business Strategy, 36,* 18–24. doi:10.1108/JBS-08-2014-0100

Lee, C. J. G. (2012). Reconsidering constructivism in qualitative research. *Educational Philosophy and Theory, 44,* 403-412. doi:10.1111/j.1469-5812.2010.00720.x

Lescevica, M., Ginters, E., & Mazza, R. (2013). Unified theory of acceptance and use of technology (UTAUT) for market analysis of FP7 CHOReOS products. *Procedia Computer Science, 26*, 51–68. doi:10.1016/j.procs.2013.12.007

Liang, H., Xue, Y., & Wu, L. (2013). Ensuring employees' IT compliance: Carrot or stick? *Information Systems Research, 24*, 279-294. doi:10.1287/isre.1120.0427

Lips-Wiersma, M., & Mills, A. J. (2014). Understanding the basic assumptions about human nature in workplace spirituality: Beyond the critical versus positive divide. *Journal of Management Inquiry, 23*, 148-161. doi:10.1177/1056492613501227

Liu, S., Yang, Y., Xie, N., & Forrest, J. (2016). New progress of grey system theory in the new millennium. *Grey Systems, 6*(1), 2–31. doi:10.1108/GS-09-2015-0054

Lo, H. (2014). Quick response codes around us: Personality traits, attitudes towards innovation, and acceptance. *Journal of Electronic Commerce Research, 15*(1), 25-39. Retrieved from http://www.csulb.edu/journals/jecr

Mader, M., Mader, W., Sommerlade, L., Timmer, J., & Schelter, B. (2013). Block-bootstrapping for noisy data. *Journal of Neuroscience Methods, 219*, 285-291. doi:10.1016/j.jneumeth.2013.07.022

Magsamen-Conrad, K., Upadhyaya, S., Joa, C. Y., & Dowd, J. (2015). Bridging the divide: Using UTAUT to predict multigenerational tablet adoption practices. *Computers in Human Behavior, 50*, 186–196. doi:10.1016/j.chb.2015.03.032

Maillet, E., Mathieu, L., & Sicotte, C. (2015). Modeling factors explaining the acceptance, actual use and satisfaction of nurses using an Electronic Patient Record in acute care settings: An extension of the UTAUT. *International Journal of Medical Informatics, 84*(1), 36–47. doi:10.1016/j.ijmedinf.2014.09.004

Malandrino, D., & Scarano, V. (2013). Privacy leakage on the web: Diffusion and countermeasures. *Computer Networks, 57*, 2833-2855. doi:10.1016/j.comnet.2013.06.013

Mangal, V. (2013). Systems theory and social networking: Investigation of systems theory principles in web 2.0 social network systems. *International Journal of Business and Commerce*, *3*, 117-135. Retrieved from www.ijbcnet.com

Manouchehr, O., Seyyed Morteza, A., & Hossein, M. (2016). An investigation of the influence of managerial factors on industrial accidents in the construction industry using the gray FTA method. *Grey Systems: Theory And Application*, (1), 96. doi:10.1108/GS-01-2016-0001

Marshall, S. (2014). IT Consumerization: A case study of BYOD in a healthcare setting. *Technology Innovation Management Review*, *4*, 14–18. Retrieved from http://timreview.ca/article/771

Martins, C., Oliveira, T., & Popovic, A. (2014). Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management*, *34*(1), 1-13. doi:10.1016/j.ijinfomgt.2013.06.002

Mayoh, J., & Onwuegbuzie, A. J. (2015). Toward a conceptualization of mixed methods phenomenological research. *Journal of Mixed Methods Research, 9*(1), 91–107. doi:10.1177/1558689813505358

McCullagh, M. C., Sanon, M. A., & Cohen, M. A. (2014). Strategies to enhance participant recruitment and retention in research involving a community-based population. *Applied Nursing Research, 27*, 249–253. doi:10.1016/j.apnr.2014.02.007

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

McNaughton, D., & Light, J. (2013). The ipad and mobile technology revolution: Benefits and challenges for individuals who require augmentative and alternative communication. *Augmentative and Alternative Communication, 29*(2), 107–116. doi:10.3109/07434618.2013.784930

McPeake, J., Bateson, M., & O'Neill, A. (2013). Electronic surveys: How to maximise success. *Nurse Researcher*, *21,* 24-26. doi:10.7748/nr2014.01.21.3.24.e1205

Mertens, D. M. (2015). Mixed methods and wicked problems. *Journal of Mixed Methods Research*, *9*(1), 1-4. doi:10.1177/1558689814562944

Mishra, D., Akman, I., & Mishra, A. (2014). Theory of reasoned action application for green information technology acceptance. *Computers in human behavior*, *36*, 29-40. doi:10.1016/j.chb.2014.03.030

Montgomery, E. G., & Oladapo, V. (2014). Talent management vulnerability in global healthcare value chains: A general systems theory perspective. *Journal of Business Studies Quarterly, 5*, 173. Retrieved from http://jbsq.org/

Morgan, D. L. (2015). From themes to hypotheses: Following up with quantitative methods. *Qualitative Health Research, 25*, 789–793. doi:10.1177/1049732315580110

Mounteney, J., Fry, C., McKeganey, N., & Haugland, S. (2010). Challenges of reliability and validity in the identification and monitoring of emerging drug trends. *Substance Use and Misuse*, *45*(1), 266-87. doi:10.3109/10826080903368598

Munroe, F. (2013). Technological transformation -- implications for compliance from big data to BYOD. *Journal of Health Care Compliance*, *15*, 41-46. Retrieved from http://www.aspenpublishers.com

Naidu, D., & Patel, A. (2013). A comparison of qualitative and quantitative methods of detecting earnings management: Evidence from two fijian private and two fijian state-owned entities. *Australasian Accounting Business & Finance Journal*, *7*(1), 79–98. doi:10.14453/aabfj.v7i1.6

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1978). The Belmont report: Ethical principles and guidelines for the protection of human subjects of research. Washington, DC: U.S. Department of Health and Human Services.

Nijland, L., & Dijst, M. (2015). Commuting-related fringe benefits in the Netherlands: Interrelationships and company, employee and location characteristics. *Transportation Research Part A: Policy and Practice, 77*, 358–371. doi:10.1016/j.tra.2015.04.026

Nimako, S. G., Ntim, B. A., & Mensah, A. F. (2014). Effect of mobile number portability adoption on consumer switching intention. *International Journal of Marketing Studies*, *6*(2) 117. doi.org/10.5539/ijms.v6n2p117

Nimon, K. F., & Oswald, F. L. (2013). Understanding the results of multiple linear regression: Beyond standardized regression coefficients. *Organizational Research Methods, 16*, 650-674. doi:10.1177/1094428113493929

Nobles, R., & Schiff, D. (2012). Using systems theory to study legal pluralism: What could be gained? *Law and Society Review*, *46*(2), 265–296. doi:10.1111/j.1540-5893.2012.00489.x

Osborne, J., & Waters, E. (2002). Four assumptions of multiple regression that researchers should always test. *Practical Assessment, Research and Evaluation*, *8*(2), 1. Retrieved from http://pareonline.net/

Palinkas, L. A. (2014). Qualitative and mixed methods in mental health services and implementation research. *Journal of Clinical Child & Adolescent Psychology*, *43*, 851–861. doi:10.1080/15374416.2014.910791

Pegrum, M., Oakley, G., & Faulkner, R. (2013). Schools going mobile: A study of the adoption of mobile handheld technologies in western australian independent schools. *Australasian Journal of Educational Technology*, *29*(1), 66-81. doi:10.1234/ajet.v29i1.64

Peretti, K., & Sarkisian, B. (2014). Peering into personal space: Investigating employee-owned mobile devices. *Journal of Internet Law*, *17*, 3-6. Retrieved from http://www.aspenpublishers.com

Peterson, R. A, & Kim, Y. (2013). On the relationship between coefficient alpha and composite reliability. *Journal of Applied Psychology*, *98*(1), 194-8. doi:10.1037/a0030767

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

Pick, A., Berry, S., Gilbert, K., & McCaul, J. (2013). Informed consent in clinical research. *Nursing Standard, 27*, 44-7. Retrieved from http://nursingstandard.rcnpublishing.co.uk

Pinder, P., Prime, G., & Wilson, J. (2014). An exploratory quantitative study comparing and correlating parental factors with environmental science achievement for black american and black caribbean students in a mid-atlantic state. *Journal of Negro Education*, *83*(1), 49–60. doi:10.7709/jnegroeducation.83.1.0049

Pouvreau, D. (2014). On the history of Ludwig von Bertalanffy's "general systemology", and on its relationship to cybernetics - Part II: Contexts and developments of the systemological hermeneutics instigated by von Bertalanffy. *International Journal of General Systems, 43,* 172-245. doi:10.1080/03081079.2014.883743

Preibusch, S. (2015). Privacy behaviors after snowden. *Communications of the ACM, 58,* 48-55. doi:10.1145/2663341

Puth, M. T., Neuhäuser, M., & Ruxton, G. D. (2014). Effective use of Pearson's product–moment correlation coefficient. *Animal Behaviour, 93*, 183-189. doi:10.1016/j.anbehav.2014.05.003

Putri, F. & Hovav, A. (2014). Employees´ compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory. *Twenty Second European Conference on Information Systems*, 1-17. Retrieved from http://aisel.aisnet.org/ecis2014/proceedings/track16/2/

Rada, V. D. D., & Dominguez-Alvarez, J. A. (2013). Response quality of self-administered questionnaires: A comparison between paper and web questionnaires. *Social Science Computer Review*, *32*, 256-269. doi:10.1177/0894439313508516

Rapoport, A., & Buckley, W. (1968). Sociology and modern systems theory. *American Sociological Review*, *33*, 463. doi:10.1177/003803856800200211

Raptis, D., Papachristos, E., Kjeldskov, J., Skov, M. B., & Avouris, N. (2014). Studying the effect of perceived hedonic mobile device quality on user experience evaluations of mobile applications. *Behaviour and Information Technology, 33,* 1168-1179, doi:10.1080/0144929X.2013.848239

Rhee, H. S., Ryu, Y. U., & Kim, C. T. (2012). Unrealistic optimism on information security management. *Computers and Security*, *31*(2), 221-232. doi:10.1016/j.cose.2011.12.001

Rhee, K., Won, D., Jang, S., Chae, S., & Park, S. (2013). Threat modeling of a mobile device management system for secure smart work. *Electronic Commerce Research, 13,* 243-256. doi:10.1007/s10660-013-9121-4

Roberts, L. D., & Allen, P. J. (2015). Exploring ethical issues associated with using online surveys in educational research. *Educational Research and Evaluation,* (2), 95-108. doi:10.1080/13803611.2015.1024421

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology*, *11*(1), 25–41. doi:10.1080/14780887.2013.801543

Rose, C. (2013). BYOD: An examination of bring your own device in business. *Review of Business Information Systems, 17*(2), 65-70. Retrieved from http://www.cluteinstitute.com/journals/review-of-business-information-systems-rbis/

Rovai, A. P., Baker, J. D., & Ponton, M. K. (2013). *Social science research design and statistics: A practitioner's guide to research methods and IBM SPSS analysis.* [Kindle edition]. Chesapeake, VA: Watertree Press LLC.

Rowley, J. (2014). Designing and using research questionnaires. *Management Research Review, 37,* 308-330. doi:10.1108/MRR-02-2013-0027

Saha, A., & Sanyal, S. (2015). Review of considerations for mobile device based secure access to financial services and risk handling strategy for CIOs, CISOs and CTOs. *International Journal Of Advanced Networking and Applications*, *6*, 2427-2434. Retrieved from http://www.ijana.in/

Sauermann, H., & Roach, M. (2013). Increasing web survey response rates in innovation research: An experimental study of static and dynamic contact design features. *Research Policy*, *42*(1), 273–286. doi:10.1016/j.respol.2012.05.003

Saunders, S. (2014). Protecting against espionage. *Network Security*, *2014*(9), 5–7. doi:10.1016/S1353-4858(14)70089-3

Schwaninger, M. (2007). Optimal structures for social systems. *Kybernetes*, *36*(3-4), 307-318. doi:10.1108/03684920710746977

Sedgwick, P. (2013a). Convenience sampling. *British Medical Journal, 347*(2), 6304-6304. doi:10.1136/bmj.f6304

Sedgwick, P. (2013b). Multiple regression. *BMJ*, 347(jul05 2), f4373–f4373. doi:10.1136/bmj.f4373

Semer, L. (2013). Auditing the BYOD program. *Internal Auditor, 70*(1), 23-27. Retrieved from http://www.theiia.org/intauditor/

Shamala, P., Ahmad, R., & Yusoff, M. (2013). A conceptual framework of info structure for information security risk assessment (ISRA). *Journal of Information Security and Applications, 18*(1), 45-52. doi:10.1016/j.jisa.2013.07.002

Silva, M. M., de Gusmão, A. P. H., Poleto, T., Silva, L. C. e, & Costa, A. P. C. S. (2014). A multidimensional approach to information security risk management using FMEA and fuzzy theory. *International Journal of Information Management, 34,* 733-740. doi:10.1016/j.ijinfomgt.2014.07.005

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

Skoko, H. (2013). Systems theory application to risk management in environmental and human health areas. *Journal of Applied Business and Economics, 14*, 93-111. Retrieved from http://www.na-businesspress.com/jabeopen.html

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48,* 296-302. doi:10.1016/j.im.2011.07.002

Spector, P. E., & Meier, L. L. (2014). Methodologies for the study of organizational behavior processes: How to find your keys in the dark. *Journal of Organizational Behavior*, 35, 1109-1119. doi:10.1002/job.1966

Starfelt Sutton, L. C., & White, K. M. (2016, November 1). Predicting sun-protective intentions and behaviours using the theory of planned behaviour: a systematic review and meta-analysis. *Psychology and Health*. Routledge. doi:10.1080/08870446.2016.1204449

Stavinoha, K. E. (2012). *Factors influencing adoption of encryption to secure data in cloud*. (Unpublished doctoral dissertation). University of Fairfax, Vienna, VA.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2013). Information security professionals' perceptions about the relationship between the information security and internal audit functions. *Journal of Information Systems, 27*(2), 65-86. doi:10.2308/isys-50510

Stevens, J. P. (2009). *Applied multivariate statistics for the social sciences* (5th ed.). Mahwah, NJ: Routledge Academic.

Stone, A. (2014). Barriers to BYOD. *Government Technology, 27*, 22-26. Retrieved from http://www.govtech.com/

Sturmberg, J. P., Martin, C. M., & Katerndahl, D. A. (2014). Systems and complexity thinking in the general practice literature: An integrative, historical narrative review. *Annals of Family Medicine, 12,* 66-74. doi:10.1370/afm.1593

Sullivan, G. M., & Artino, A. R. (2013). Analyzing and interpreting data from Likert-Type scales. *Journal of Graduate Medical Education, 5*, 541–542. doi:10.4300/JGME-5-4-18

Tabachnick, B. G., & Fidell, L. S. (2013). *Using multivariate statistics* (6th ed.). Boston, MA: Allyn and Bacon.

Tan, G. W. H., Ooi, K. B., Leong, L. Y., & Lin, B. (2014). Predicting the drivers of behavioral intention to use mobile learning: A hybrid SEM-Neural Networks approach. *Computers in Human Behavior*, *36*, 198–213. doi:10.1016/j.chb.2014.03.052

Thomas, J. R., Silverman, S., & Nelson, J. (2015). *Research methods in physical activity*, (7th ed.). Champaign, IL: Human Kinetics

Tideman, M., & Svensson, O. (2015). Young people with intellectual disability—the role of self-advocacy in a transformed Swedish welfare system. *International journal of qualitative studies on health and well-being*, *10*. doi:10.3402/qhw.v10.25100

Tokuyoshi, B. (2013). The security implications of BYOD. *Network Security*, *2013*(4), 12-13. doi:10.1016/S1353-4858(13)70050-3

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

Totten, J. A., & Hammock, M. C. (2014). Personal electronic devices in the workplace: Balancing interests in a BYOD world. *ABA Journal of Labor & Employment Law*, *30*(1), 27-45. Retrieved from http:// http://www.abanet.org/

Trop, J. L., Burke, M. L., & Trop, G. S. (2013). Psychoanalytic theory and psychotherapy: A dynamic systems view of change. *Clinical Social Work Journal*, *41*(1), 34-42. doi:10.1007/s10615-012-0403-4

Turner, T. L., Balmer, D. F., & Coverdale, J. H. (2013). Methodologies and study designs relevant to medical education research. *International Review of Psychiatry, 25*, 301-10. doi:10.3109/09540261.2013.790310

Utter, C. J., & Rea, A. (2015). The " bring your own device " conundrum for organizations and investigators : An examination of the policy and legal concerns in light of investigatory challenges. *Journal of Digital Forensics, Security & Law*, *10*, 55–72. doi:10.15394/jdfsl.2015.1202

Uyanık, G. K., & Güler, N. (2013). A study on multiple linear regression analysis. *Procedia - Social and Behavioral Sciences*, *106*, 234-240. doi:10.1016/j.sbspro.2013.12.027

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*, 190-198. doi:10.1016/j.im.2012.04.002

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, *37*(1), 21-54. Retrieved from http://misq.org/misq/downloads

Vignesh, U., & Asha, S. (2015). Modifying security policies towards BYOD. *Procedia Computer Science*, *50*, 511-516. doi:10.1016/j.procs.2015.04.023

von Bertalanffy, L. (1950). An outline of general systems theory. *British Journal for the Philosophy of Science, 1*, 134–165. doi:10.1093/bjps/I.2.134

von Bertalanffy, L. (1968). *General systems theory: Foundations, developments, applications*. New York, NY: George Braziller. Retrieved from https://monoskop.org/images/7/77/Von_Bertalanffy_Ludwig_General_System_Theory_1968.pdf

Von Bertalanffy, L. (1972). The history and status of general systems theory. *Academy of Management Journal*, *15*, 407-426. doi:10.2307/255139

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*(October 2013), 97–102. doi:10.1016/j.cose.2013.04.004

Walker-Osborn, C., Mann, S., & Mann, V. (2013). To BYOD or . . . not to BYOD. *ITNOW, 55*(1), 38-39. doi:10.1093/itnow/bws142

Wallace, L. G., & Sheetz, S. D. (2014). The adoption of software measures: A technology acceptance model (TAM) perspective. *Information and Management, 51*(2), 249-259. doi:10.1016/j.im.2013.12.003

Wang, L., & Wang, L. (2015). Using theory of planned behavior to predict the physical activity of children: Probing gender differences. *BioMed Research International*, *2015*, 1-9. doi:10.1155/2015/536904

Waterfill, M. R., & Dilworth, C. A. (2014). BYOD: Where the employee and the enterprise intersect. *Employee Relations Law Journal*, *40*(2), 26-36. Retrieved from http://www.aspenpublishers.com/

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security, 44*, 1-15. doi:10.1016/j.cose.2014.04.005

Weeger, A., Wang, X., & Gewald, H. (2016). IT consumerization: Byod-program acceptance and its impact on employer attractiveness. *Journal of Computer Information Systems, 56*(1), 1–10. doi:10.1080/08874417.2015.11645795

Weiss, F., & Leimeister, J. M. (2014). Why can't I use my iPhone at work?: Managing consumerization of IT at a multi-national organization. *Journal of Information Technology Teaching Cases, 4*(1), 11–19. doi:10.1057/jittc.2013.3

Williams, J. (2014). Left to their own devices how healthcare organizations are tackling the BYOD trend. *Biomedical Instrumentation & Technology / Association for the Advancement of Medical Instrumentation, 48*, 327-339. doi:10.2345/0899-8205-48.5.327

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

Williams, R. (2016). *Outliers.* Retrieved from www3.nd.edu/~rwilliam/stats2/l24.pdf

Wilson, J. R. (2014). Fundamentals of systems ergonomics/human factors. *Applied Ergonomics, 45*(1), 5-13. doi:10.1016/j.apergo.2013.03.021

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

Wu Suen, L. J., Huang, H. M., & Lee, H. H. (2014). A comparison of convenience sampling and purposive sampling. *Journal of Nursing*, *61*, 105-111. doi:10.6224/JN.61.3.105

Wu, W., & Jia, F. (2013). A new procedure to test mediation with missing data through nonparametric bootstrapping and multiple imputation. *Multivariate Behavioral Research*, *48*, 663–691. doi:10.1080/00273171.2013.816235

Yawson, R. M. (2013). Systems theory and thinking as a foundational theory in human resource development—A myth or reality? *Human Resource Development Review*, *12*(1), 53-85. doi:10.1177/1534484312461634

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

Yeatman, S., Trinitapoli, J., & Hayford, S. (2013). Limitations of clinic-based studies on HIV and fertility preferences. *American Journal of Public Health, 103*(6), e5. doi:10.2105/AJPH.2013.301333

Yeou, M. (2016). An investigation of students' acceptance of moodle in a blended learning setting using technology acceptance model. Journal of Educational Technology Systems, 44, 300–318. doi:10.1177/004723951561846

Yevseyeva, I., Morisset, C., Turland, J., Coventry, L., Groß, T., Laing, C., & Moorsel, A. van. (2014). Consumerisation of IT: Mitigating risky user actions and improving productivity with nudging. *Procedia Technology*, *16*, 508-517. doi:10.1016/j.protcy.2014.10.118

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education, 48,* 311-325. doi:10.1111/ejed.12014

Yin, M. S. (2013). Fifteen years of grey system theory research: a historical review and bibliometric analysis. *Expert systems with Applications*, *40,* 2767-2775. doi:10.1016/j.eswa.2012.11.002

Yin, R. K. (2014). Case study research: Design and methods (5th ed.). Thousand Oaks, CA: Sage Publications.

Yin, R. K. (2013). *Case study research: Design and methods* (5th ed.). Thousand Oaks, CA: Sage Publications.

Yoon, H.-Y. (2016). User acceptance of mobile library applications in academic libraries: An application of the technology acceptance model. *Journal of Academic Librarianship, 42,* 687–693. doi:10.1016/j.acalib.2016.08.003

Yoon, T. (2009). *An empirical investigation of factors affecting organizational adoption of virtual worlds* (Doctoral dissertation). Available from ProQuest Dissertations & Theses Global. (UMI No. 3399253)

Young, W., & Leveson, N. G. (2014). An integrated approach to safety and security based on systems theory. *Communications of the ACM*, *57*(2), 31-35. doi:10.1145/2556938

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework & its analysis. *Computers & Security, 55*, 81-99. doi:10.1016/j.cose.2015.06.011

Zhao, X., Xue, L., & Whinston, A. B. (2013). Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. *Journal of Management Information Systems*, *30*(1), 123-152. doi:10.2753/MIS0742-1222300104

Zolna, K., Dao, P. B., Staszewski, W. J., & Barszcz, T. (2015). Towards homoscedastic nonlinear cointegration for structural health monitoring. *Mechanical Systems and Signal Processing*. Cambridge, MA: Academic Press. doi:10.1016/j.ymssp.2015.12.014

Appendix A: NIH Human Subject Research Certificate of Completion

Certificate of Completion

The National Institutes of Health (NIH) Office of Extramural Research certifies that **Leslie DeShield** successfully completed the NIH Web-based training course "Protecting Human Research Participants".

Date of completion: 11/09/2014.

Certification Number: 1614873.

Appendix B: Permission for Use and Publishing of Survey Instruments

Requesting Permission to Use Survey Instrument

Leslie DeShield <leslie.deshield@waldenu.edu> Wed, Dec 30, 2015 at 10:14 PM
To: [redacted]
Cc: Leslie DeShield <leslie.deshield@waldenu.edu>

Dr. Lease

I am a doctoral student from Walden University working on a doctoral research study tentatively titled " The Challenges of Implementing Bring Your Own Device" under the direction of my doctoral study committee chaired by Dr. Steven Case.

I would like your permission to obtain, use, and print the survey instrument presented in your work titled **"Factors Influencing The Adoption Of Biometric Security Technologies By Decision Making Information Technology And Security Managers" (2005).**

I will use this survey only for my research study and not in any other manner.

If this request is acceptable and you approve, please indicate so via an email response.

Sincerely,

Leslie DeShield
Doctoral Candidate

Requesting Permission to Use Survey Instrument

Lease, David <[redacted]> Thu, Dec 31, 2015 at 8:20 AM
To: Leslie DeShield <leslie.deshield@waldenu.edu>

Hi Leslie:

You have my permission to use my survey instrument and adapt it as necessary for your dissertation research. Please feel to contact me should you have any questions or need to add a member to your committee.

Best wishes on your dissertation journey and I hope you enjoy the New Year!

Regards,

David

Requesting Permission to Use Survey Instrument

Leslie DeShield <leslie.deshield@waldenu.edu> Wed, Dec 30, 2015 at 9:03 PM
To: [redacted]
Bcc: Leslie DeShield <leslie.deshield@waldenu.edu>

Ms. Putri

I am a doctoral student from Walden University working on a doctoral research study tentatively titled " The Challenges of Implementing Bring Your Own Device" under the direction of my doctoral study committee chaired by Dr. Steven Case.

I would like your permission to obtain, use, and print the survey instrument presented in your work titled **"Employees Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory".**

I will use this survey only for my research study and not in any other manner.

If this request is acceptable and you approve, please indicate so via an email response.

Sincerely,

Leslie DeShield
Doctoral Candidate

Requesting Permission to Use Survey Instrument

Frida <[redacted]> Thu, Dec 31, 2015 at 1:07 PM
To: Leslie DeShield <leslie.deshield@waldenu.edu>

Dear Ms. Leslie,
I'd be happy if my survey instrument can be used for further research. Please kindly use the survey instrument for your research

Best Regards,

Frida

Requesting Permission to Use Survey Instrument

Leslie DeShield <leslie.deshield@waldenu.edu> Sat, Jan 9, 2016 at 3:58 PM
To: [redacted]
Cc: Leslie DeShield <leslie.deshield@waldenu.edu>

Dr. Young

I am a doctoral student from Walden University working on a doctoral research study tentatively titled " The Challenges of Implementing Bring Your Own Device" under the direction of my doctoral study committee chaired by Dr. Steven Case.

I would like your permission to obtain, adopt and use the survey instrument presented in your work titled **"Unrealistic Optimism on Information Security Management" (2011).**

I will use this survey only for my research study and not in any other manner.

If this request is acceptable and you approve, please indicate so via an email response.

Sincerely,

Leslie DeShield
Doctoral Candidate

Requesting Permission to Use Survey Instrument

ryoung <[redacted]> Sat, Jan 9, 2016 at 4:52 PM
To: Leslie DeShield <leslie.deshield@waldenu.edu>

Leslie,

You may use the survey instrument.

Regards,

Young Ryu

From: Anat Zeelim-Hovav <[redacted]>
Sent: Sunday, December 10, 2017 4:46 AM
To: Leslie Deshield
Subject: RE: Request to Use and Publish Survey Instrument

Thank you for your interest in our work.

Anything that has been published could (and should) be used by other scholars as long as it is for academic purposes and not for commercial purposed **and as long as it is being propoerly cited.**

You may also interested in the following journal paper, which has a more percise discussion of the results.

Good luck with your research

Anat

----------Original message----------
From: "Leslie Deshield"<leslie.deshield@waldenu.edu>
To: "[redacted]>
Cc.: Leslie Deshield <leslie.deshield@waldenu.edu>
Sent date: 2017-12-10 06:39:06 GMT +0900 (Asia/Seoul)
Title: Request to Use and Publish Survey Instrument

Dr. Hovav

I am a doctoral student from Walden University working on a doctoral research study tentatively titled " The Challenges of Implementing Bring Your Own Device" under the direction of my doctoral study committee chaired by Dr. Steven Case.

For my study, I would like your permission to use and publish the survey instrument presented in your work titled **"Employees Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory".**

I will use this survey only for my research study and not in any other manner.

If this request is acceptable and you approve, please indicate so via an email response.

Sincerely,
Leslie DeShield
Doctoral Candidate

From: Lease, David <[redacted]>
Sent: Saturday, December 9, 2017 8:16 AM
To: Leslie Deshield
Subject: Re: Requesting Permission to Publish Survey Instrument

Hi Leslie:

Congratulations! I'm sure the past two years have been a rollercoaster of emotions as you completed you analysis and findings.

You have my permission to publish the adapted survey in your dissertation. I'd be very interested in reading your dissertation when you finish.

Best wishes on your continuing dissertation journey and for the New Year.

Regards,

David Lease

From: Leslie Deshield <leslie.deshield@waldenu.edu>
Sent: Friday, December 8, 2017 10:01 PM
To: Lease, David
Cc: Leslie Deshield
Subject: Fw: Requesting Permission to Publish Survey Instrument

Dr. Lease

Thanks again for granting approval to use and adapt your survey instrument for my doctoral study.

To ensure there are no copyright concerns, I'm specifically requesting your permission to **publish** the adapted survey instrument with my study upon completion.

If this request is acceptable and you approve, please indicate so via an email response.

Sincerely,

Leslie DeShield
Doctoral Candidate

From: ryoung <[redacted]>
Sent: Friday, December 8, 2017 11:28 PM
To: Leslie Deshield
Subject: Re: Fw: Requesting Permission to Use Survey Instrument

Yes, you may.

Young Ryu

-------- Original message --------
From: Leslie Deshield <leslie.deshield@waldenu.edu>
Date: 12/9/17 12:11 PM (GMT+09:00)
To: [redacted]
Cc: Leslie Deshield <leslie.deshield@waldenu.edu>
Subject: Fw: Requesting Permission to Use Survey Instrument

Dr. Young

Thanks again for granting approval to use your survey instrument for my doctoral study.

To ensure there are no copyright concerns, I'm specifically requesting your permission to **publish** the survey instrument with my study upon completion.

If this request is acceptable and you approve, please indicate so via an email response.

Sincerely,

Leslie DeShield
Doctoral Candidate

Appendix C: Survey Instrument

Item No.	**Part I – Bring Your Own Device (BYOD) Questions**	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	I feel that BYOD is secure.	1	2	3	4	5
2	I am/would be concerned with the security of the technology used by BYOD	1	2	3	4	5
3	I feel that the security of the technology used by BYOD is more secure	1	2	3	4	5
4	I am willing to protect sensitive data through the use of BYOD	1	2	3	4	5
5	BYOD technology was not secure three years ago.	1	2	3	4	5
6	Organizations need to improve their implementation of BYOD.	1	2	3	4	5
7	Organizations need BYOD to meet the needs of their employees.	1	2	3	4	5
8	BYOD would/does provide significant benefits to organizations.	1	2	3	4	5
9	Employees are inherently productive with BYOD.	1	2	3	4	5
10	Employees' productivity significantly improves/increases with BYOD.	1	2	3	4	5
11	Employees' productivity decreases with BYOD.	1	2	3	4	5
12	BYOD provides good value for the cost.	1	2	3	4	5
13	The cost of maintenance is lower with BYOD than with traditional IT-related costs.	1	2	3	4	5
14	I would consider BYOD implementation to have considerable cost savings for organizations.	1	2	3	4	5
15	I would feel comfortable recommending BYOD in my organization.	1	2	3	4	5
16	I feel that BYOD uses proven technology.	1	2	3	4	5
	Part II – Intention to Comply					
17	I intend to comply with the requirements of my organization's BYOD information systems security policy.	1	2	3	4	5

18	I intend to protect my personal device used for work according to the requirements of my organization's BYOD information systems security policy.	1	2	3	4	5
19	I intend to carry out my responsibilities prescribed in my organization's BYOD information systems security policy when I use my personal device for work.	1	2	3	4	5
20	I am likely to follow my organization's BYOD information systems security policy.	1	2	3	4	5

21	There is a possibility that I will comply with my organization's BYOD information systems security policy to protect my organizational computing resources.	1	2	3	4	5
22	There is a possibility that I will comply with my organization's BYOD information systems security policy to protect my own device.	1	2	3	4	5
23	I am certain that I will follow my organization's BYOD information systems security policy.	1	2	3	4	5

	Part III – Security Risks Perceptions	Very Low	Low	Somewhat Low	Average	Somewhat High	High	Very High
24	The risk from information security threats to my organization is	1	2	3	4	5	6	7
25	The likelihood that the information systems in my organization are disrupted due to information security breaches in the next 12 months is	1	2	3	4	5	6	7
26	The chance that my organization will fall victim to an information security breach is	1	2	3	4	5	6	7
27	The vulnerability of my organization to information security threats is	1	2	3	4	5	6	7

Part IV – Demographic Questions

28	Are you a Certified Information Security Manager (CISM)?	a. Yes b. No
29	How many years of experience do you have implementing BYOD?	a. None b. Less than 2 years c. Two years to less than 5 years d. Five years or more
30	How many users does your organization support?	a. Less than 50 users b. 50 to 249 c. 250 to 500 d. More than 500
31	What best describes your title?	a. CEO b. CIO c. CTO d. CISO e. Information Assurance Manager f. IT Director g. IT Manager h. IT Supervisor or Lead i. Other Director j. Other Manager k. None of the above
32	What is the primary business or industry of your organization?	a. Construction b. Education c. Energy/Utilities d. Financial Services/Banking e. Government f. State g. Health Care h. Information Technology- Services i. Information Technology-Manufacturing j. Manufacturing (non-IT) k. Professional, Technical, and Business Services (non-IT) l. Real Estate m. Retail n. Telecommunications o. Travel/Leisure/Hospitality p. Wholesale Distribution and Services q. Other

Appendix D: E-mail Invitation to Participate in Research

Date: [Insert Date]

Re: Invitation to Participate in a Research Study

Dear Recipient:

My name is Leslie DeShield and I am a doctoral student at Walden University, pursuing a Doctor of Information Technology degree (DIT). I am conducting a research study titled "The Challenges of Implementing Bring Your Own Device (BYOD)". I am writing you to request your participation in my study. Participation involves completing a brief online survey.

The goal of my study is to examine the relationship between security, compliance, and BYOD implementation. I would like to help information technology leaders develop strategies or a framework from which to implement BYOD successfully. If you are an information security manager with the Certified Information Security Manager (CISM) certification and are employed by a small to medium sized business in the eastern United States then your participation will be valuable to my research. You can participate by completing the online survey at: www.surveymonkey.com/xxxxx

Thanks for your consideration.

Sincerely,
Leslie DeShield
DIT Student, Walden University