


2017

Strategies to Prevent Security Breaches Caused by Mobile Devices

Tony Griffin
Walden University

Follow this and additional works at: <https://scholarworks.waldenu.edu/dissertations>

 Part of the [Databases and Information Systems Commons](#), and the [Library and Information Science Commons](#)

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact ScholarWorks@waldenu.edu.

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Tony Griffin

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. Timothy Perez, Committee Chairperson, Information Technology Faculty
Dr. Bob Duhainy, Committee Member, Information Technology Faculty
Dr. Steven Case, University Reviewer, Information Technology Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2017

Abstract

Strategies to Prevent Security Breaches Caused by Mobile Devices

by

Tony Griffin

MS, Kaplan University, 2013

BS, Grantham University, 2007

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2017

Abstract

Data breaches happen almost every day in the United States and, according to research, the majority of these breaches occur due to a lack of security with organizations' mobile devices. Although most of the security policies related to mobile devices currently in place may meet the guidelines required by law, they often fail to prevent a data breach caused by a mobile device. The main purpose of this qualitative single case study was to explore the strategies used by security managers to prevent data breaches caused by mobile devices. The study population consisted of security managers working for a government contractor located in the southeastern region of the United States. Ludwig von Bertalanffy's general systems theory was used as the conceptual framework of this study. The data collection process included interviews with organization security managers ($n = 5$) and company documents and procedures ($n = 13$) from the target organization related to mobile device security. Data from the interviews and organizational documents were coded using thematic analysis. Methodological triangulation of the data uncovered 4 major themes: information security policies and procedures, security awareness, technology management tools, and defense-in-depth. The implications for positive social change from this study include the potential to enhance the organizations' security policies, cultivate a better security awareness training program, and improve the organizations data protection strategies. In addition, this study outlines some strategies for preventing data breaches caused by mobile devices while still providing maximum benefit to its external and internal customers.

Strategies to Prevent Security Breaches Caused by Mobile Devices

by

Tony Griffin

MS, Kaplan University, 2013

BS, Grantham University, 2007

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 wife, Dr. Dana A. Griffin. I have achieved so much in this world with her help, guidance and support over the last 23 years. I am honestly, not sure where I would be today without her by my side through it all. And to my Mother, Jessie Griffin, who raised me from birth by herself doing everything she could to make sure that I had everything I needed to be a successful human being. I am the man I am today because of the support I received from my family and friends.

Acknowledgments

I would like to acknowledge the support I received from my Chair Dr. Timothy Perez, and my second committee member Dr. Bob Duhainy. With their support, guidance and dedication I was able to make it through this chapter in my life. This was by no means an easy journey and one I would have easily given up on without them helping me through this process.

Table of Contents

List of Figures	v
Section 1: Foundation of the Study.....	1
Background of the Problem	1
Problem Statement	1
Purpose Statement.....	2
Nature of the Study	3
Research Question	4
Interview Questions	4
Conceptual Framework.....	5
Definition of Terms.....	6
Assumptions, Limitations, and Delimitations.....	6
Assumptions.....	6
Limitations	6
Delimitations.....	7
Significance of the study.....	7
Contribution to Information Technology Practice	7
Implications for Social Change.....	8
A Review of the Professional and Academic Literature.....	9
Conceptual Framework.....	11
General Systems Theory	13
Supporting and contrasting Theories	27

Bring Your Own Device	29
Mobile Device Management.....	33
Defense in Depth.....	36
Transition and Summary.....	38
Section 2: The Project.....	40
Purpose Statement.....	40
Role of the Researcher	41
Participants.....	42
Research Method and Design	45
Research Method	45
Research Design.....	47
Population and Sampling	49
Ethical Research.....	52
Data Collection	54
Instruments.....	54
Data Collection Technique	56
Data Organization Techniques.....	59
Data Analysis Technique	60
Reliability and Validity.....	64
Dependability	66
Credibility	67
Transferability.....	68

Confirmability.....	68
Data Saturation.....	69
Transition and Summary.....	70
Section 3: Application to Professional Practice and Implications for Change	71
Overview of Study	71
Presentation of the Findings.....	72
Theme 1: Information Security Policies and Procedures.....	73
Theme 2: Security Awareness	77
Theme 3: Technology Management Tools	81
Theme 4: Defense-in-Depth.....	86
Applications to Professional Practice	89
Implications for Social Change.....	90
Recommendations for Action	91
Recommendations for Further Study	93
Reflections	94
Summary and Study Conclusions	94
References.....	96
Appendix A: Interview Protocol.....	123
Appendix B: Interview Questions.....	127

List of Tables

Table 1. Statistics for References in the Literature Review.....	9
Table 2. References to Information Security Policies and Procedures.....	73
Table 3. References to Security Awareness.....	78
Table 4. References to Technology Management Tools	82
Table 5. References to Defense-in-Depth.....	86

List of Figures

Figure 1. TISA: Layered trust information security architecture (Reprinted from de Oliveira et al., 2014)	20
Figure 2. BYOD multilevel security policy – organizational level, application level, and device level policies (Reprinted from Vignesh & Asha, 2015)	33
Figure 3. Functions of an MDM System (Reprinted from Rhee et al., 2013)	35
Figure 4. Defense-in-Depth Strategic Framework (Reprinted from U.S. Department of Homeland Security, 2016)	39

Section 1: Foundation of the Study

Background of the Problem

Data breaches happen almost every day in the United States and, according to the research reviewed for this study, the majority of these breaches occur due to a lack of security with organizations' mobile devices. Mobile technology has become a requirement for organizations to compete in the global workforce, however the problems with this technology are the associated risks and vulnerabilities this technology brings with it.

I used existing research on this topic to further enhance this qualitative single case study. In 2010, the researcher Rhonda G. Chicone did a similar study titled "An exploration of security implementations for Mobile Wireless Software Applications within Organizations". In this study, the researcher also utilized a qualitative case study that centered on computer security and more specifically on mobile device software application security (Chicone, 2010). One of the major findings of Chicone's research study was the lack of research around the topic of mobile technology and the implementation of security for these types of devices. Therefore, my main objective for this study was to explore the strategies security managers use to prevent data breaches caused by lost or stolen mobile devices.

Problem Statement

A younger, more mobile workforce, expecting to be able to use their own personal mobile devices while at work is pushing today's organizations (Earley, Harmon, Lee, & Mithas, 2014). As Tu, Turel, Yuan, and Archer (2015), pointed out, mobile

devices are vulnerable to a unique risk of loss or theft, which could potentially lead to the loss of confidential data or give the intruder access to the organization's enterprise network. As mobile devices continue to become progressively prevalent, so do the incentives for hackers. Liu, Musen, and Chou (2015), evaluated 949 data breaches affecting 29 million records between 2010 and 2013, and the majority of the breaches occurred via mobile devices. The general IT problem addressed in this study was that some organizations suffer data breaches due to lost or stolen mobile devices. The specific IT problem was that some security managers lack strategies to secure mobile devices to prevent a data breach.

Purpose Statement

The purpose of this qualitative single case study was to explore the strategies used by security managers to prevent data breaches caused by mobile devices. The target population consisted of security managers who utilize strategies to prevent data breaches caused by mobile devices. The security managers included in this study were sourced from a government contractor located in the southeastern region of the United States. This population was appropriate for this study as they represent the individuals responsible for implementing security strategies to protect the data stored on mobile devices, as well as the ones who will be held responsible if a data breach occurs.

This study may benefit not only the target organization but also the customer by protecting their confidential data from potential data breaches. In addition, this study outlines some strategies for preventing data breaches caused by mobile devices while still providing maximum benefit to its external and internal customers. Organizations will

continue to see the benefits from allowing its employees to use mobile technology while at the same time the customers of the organization will remain confident that their personal data is not at risk. Data from this research might provide security managers with strategies they can implement at their institutions to prevent data breaches caused by mobile devices.

Nature of the Study

I chose a qualitative methodology for this study based on a review and understanding of the available research methods. According to Morse and McEvoy (2014), researchers that utilize the qualitative approach have the ability to uncover a deeper understanding of what is yielded from a decision or a process. As the focus of this study was to take an in-depth look at strategies security managers use to prevent data breaches caused by mobile devices, the qualitative method was the best method to determine what works and what does not and why.

A quantitative method is the recommended approach when the researcher intends to acquire statistical data for hypothesis testing (Scrutton & Beames, 2015). Because I did not seek to test a hypothesis, a quantitative study was not a viable choice. As a mixed-methods approach is suitable when the purpose of the study is to utilize both qualitative and quantitative approaches (Siddiqui & Fitzgerald, 2014). Because the scope of this study did not involve a combination of numerical testing and participants' experiences, I did not choose the mixed-method approach.

I used a single case design for this study. Researchers that utilize a single case study design investigate a phenomenon in depth within a specific context to address a

specific research question (Stake, 1978). The single case study was best suited to my goals, as the focus of this study was to take an in depth look at strategies security managers use to prevent data breaches caused by mobile devices.

The ethnographic design is utilized when researchers wish to immerse themselves in the culture of the sample as active participants (Samnani & Singh, 2013). Because the intent of this study was not the observation of group cultures, an ethnographic design was not an appropriate method for this study. Based on a review of available literature, I chose not to utilize a phenomenological design. According to Hou, Ko, and Shu (2013), this type of design is used to derive new knowledge from participants' perceptions of their lived experiences, and the data is primarily collected via interviews. Because this study relied on a diverse set of data to meet the needs of the research question, the phenomenological design was not an appropriate choice.

Research Question

The following research question was used to guide this study: What strategies do security managers use to prevent data breaches caused by mobile devices?

Interview Questions

1. What strategies have you used to prevent data breaches caused by mobile devices?
2. What strategies have you used that failed to prevent a data breach caused by a mobile device?
3. What strategies have you used that succeeded to prevent a data breach caused by mobile devices?

4. What challenges did you face in implementing/using these strategies?
5. What additional information would you like to share about strategies to prevent data breaches caused by mobile devices?

Conceptual Framework

The conceptual framework for this study was driven by general systems theory. The scholar Ludwig von Bertalanffy initially proposed general systems theory in 1946 (Bertalanffy, 1968). As noted by von Bertalanffy (1968), at the center of systems theory are open systems and systems thinking. Researchers von Bertalanffy, Juarrero, and Rubino (2008), further built up Bertalanffy's work by stating that systems can be seen as both inputs and outputs working together to satisfy the objectives of the organism. Hammond (2010) stated the focal component of systems theory is the actual system, which is viewed as complete when all of its parts are functioning as designed.

Organizations are intricate systems composed of various components such as functions, activities and business units (Pushkarskaya & Marshall, 2010). The collaboration of business parts must function appropriately to bring about the accomplishment of organizational objectives. Information security is a critical business component of any organization. According to Coole and Brooks (2014) when security components do not function as a system a breakdown in the security defenses occurs. Systems theory drove this study by showing how the information security strategies presented in this study will help to bring about the accomplishment of the objectives of the system. I used systems theory to identify the key elements (objects) of the system, or the attributes of the system, while addressing the relationship of those elements in the

context of accomplishing the objectives.

Definition of Terms

The following terms were used throughout this study.

Mobile application: Software program developed to run on a mobile device (Serrano, Hernantes, & Gallardo, 2013).

Security managers: For the purpose of this study, security managers are the chief information security officers (CISO), chief technology officers (CTO), chief information officers (CIO), and/or information security managers of an organization (Ifinedo, 2012).

Assumptions, Limitations, and Delimitations

Assumptions

According to Lips-Wiersma and Mills (2014), assumptions are anything out of a researcher's control, however the researcher must consider these elements as relevant to the study. My main assumption was that the participants of this study provided open, honest and unbiased answers to the interview questions during the semistructured interviews.

Limitations

According to Madsen (2013), limitations are the potential shortcomings that may confine the extent of the research findings. The main limitation of this study was the use of a single case study design consisting of security managers from a government contractor located in the southeastern region of the United States.

Delimitations

Delimitations, as noted by Kongnso (2015), are the borders that guide the research study. In spite of the fact that organizations outside the selected industries might provide additional information to address the central research question, the geographical criterion restricted cooperation to individuals from a government contractor located in the southeastern region of the United States. Furthermore, the data collection instruments included semistructured interviews with organization security managers and a review of organization documents related to mobile device security. Another delimitation of this study was the population sample came from target organization located in the southeastern region of the United States.

Significance of the study

Although similar research on this topic exists, additional research on the specific topic related to strategies used by security managers to prevent data breaches caused by mobile devices would enhance the literature and practice in this area. Given the lack of research on this topic I expect this study to contribute to the practice and could lead to further research on the topic.

Contribution to Information Technology Practice

Mobile devices continue to rapidly change the global business landscape and how organizations conduct day-to-day operations. Mobile devices have become a permanent part of organizations and ultimately drive the way in which chief information officers ensure the IT department meets the needs of the organization. The information gathered might assist organizations around the world in the enhancement of its mobile security

framework by providing the security managers with some strategies that can be used to prevent data breaches caused by mobile devices. According to a recent study by Gartner, 70% of mobile professionals will conduct their work on personal mobile devices by 2018 (McClelland, 2014). This phenomenon, which is also known as Bring Your Own Device (BYOD), is one of the major contributing factors to this study. Data gathered from this study may assist organizations and security managers with identifying the best practices for dealing with BYOD while helping to minimize or prevent data breaches caused by mobile devices.

Implications for Social Change

This section of the study addresses how the findings of this study will contribute to positive social change. As indicated by Jewkes and Yar (2011), digital privacy protection has turned into a force for creativity and social change as innovation drives community engagement and cultivates corporate advancements. One recent study conducted by Intel and the Ponemon Institute revealed the loss of an estimated 86,000 laptops over a 1 year period, which caused an estimated \$2.1 billion dollars in damages in terms of data breaches, lost intellectual property, reduction in productivity, and legal and regulatory charges for 300 organizations in the United States (Macwillson, 2011).

The findings of this study may provide security managers with the knowledge to prevent these types of data breaches, which will in effect reduce the overall financial loss organizations face. Furthermore, by preventing these types of data breaches, organizations will protect consumers against the high costs of identity theft generally associated with these types of data breaches. Consumers will benefit from knowing that

organizations are taking steps to protect their data from unauthorized access while providing them with exceptional service through the use of mobile devices by the organization.

A Review of the Professional and Academic Literature

The literature review is an essential component of the study as its main purpose, according to Maier (2013), is to identify knowledge gaps/research needs in the problem domain/research area. The literature review also serves as a way for the researcher to build upon existing research in the problem domain/research area while providing the viewpoints of other researchers in an effort to promote further research around the study topic (Maier, 2013).

I gathered information for this literature review from multiple sources. Table 1 below breaks down the total number of references used in the literature review portion of this study.

Table 1

Statistics for References in the Literature Review

<i>Category</i>	<i>Result</i>
Total number of references	73
Total number of references published within the last 5 years	62
Total number of peer-reviewed references	61
Total number of doctoral dissertations	3
Percentage of peer-reviewed references including dissertations	88%
<u>Percentage of references published within last 5 years</u>	<u>85%</u>

Literature Search Strategy

This literature review encompassed a comprehensive search of the following online databases:

- EBSCOhost
- Thomson Gale Info Trac
- Emerald
- ProQuest Central
- Sage Premier
- Google Scholar
- Academic Search Complete/Premier

These databases contain a vast amount of books, dissertations, magazines, conference proceedings, and peer-reviewed scholarly articles. To narrow the scope and find sources relevant to this study. I used the following keywords or phrases in the search criteria: *mobile technology, bring your own device, BYOD, bring your own technology, BYOT, bring your own phone, BYOP, bring your own personal computer, BYOPC, BYOD challenges, mobile devices, information security, InfoSec, information assurance, mobile device management, MDM, data breaches, defense-in-depth, DiD, security management, information security management, security manager, systems theory, grey systems theory, general systems theory, and mobile security incidents.*

My extensive review of literature established a scholarly foundation for the study while providing a critical analysis of the body of knowledge related to the central research question for this study: What strategies do security managers use to prevent data breaches caused by mobile devices?

The literature review has been broken down into the following subsections:

- conceptual framework

- general systems theory
- supporting and contrasting theories
- bring your own device
- mobile device management
- defense-in-depth

Conceptual Framework

I chose general systems theory as the primary theory for this study based on an extensive review of literature and the central research question, which looks to uncover the strategies security managers use to prevent data breaches caused by mobile devices. The scholar Ludwig von Bertalanffy initially proposed general systems theory in 1946 (Bertalanffy, 1968). According to Rousseau (2015), one of the early goals of general systems theory revolved around the need for a theory to help bridge the divide between the subject-oriented and object-oriented disciplines. In essence, a theory that could be utilized to facilitate scientific discoveries in disciplines lacking exact theories. The key principles of systems theory include a continuous flow of information, some form of processing, and some form of output (Bertalanffy, 1972). These principles form the basis of the typical organization, which processes some form of information and generates some form of output.

Researchers have applied systems theory over the years to a diverse set of systems. According to Vikas and Dixit (2013), Miller utilized systems theory in the field of biology and Yourdon used it with information systems. As noted by von Bertalanffy (1968), at the center of general systems theory are open systems and systems thinking.

According to Nguyen and Bosch (2013), open systems interact with their environment and use it to adapt or determine the best fit. As most organizations are considered to be open systems, meaning they interact with their environment, this will help in determining which components of the system are not functioning as designed, thereby affecting the overall equifinality of the system. According to Laszlo and Krippner (1998), when viewed through the lens of systems theory, a business can be seen as a network of interconnected parts, each having a specific purpose and task. The strategies used by security managers to prevent data breaches caused by mobile devices in this equation can be seen as one of the many parts that make up an organization or system.

Another key tenet of systems theory is holism. As noted by von Bertalanffy (1968), a holistic approach should be used when designing any complex system. It is through this lens of holism that general systems theory drove this study by breaking down the parts of the target organization and how the strategies they use to prevent data breaches caused by mobile devices are just one element of the overall organization or system. Hammond (2010) contends the focal component of general systems theory is the actual system, which is viewed as complete when all of its parts are functioning as designed. General systems theory assisted in the identification of the key elements (objects) of the system, attributes of the system while addressing the relationship of those elements in the context of accomplishing the objectives of the system. The result of this study highlights why a holistic approach to information security is important with any system especially when it comes to strategies security managers use to prevent data breaches caused by mobile devices.

Entropy is another key tenet or principle of general systems theory. Entropy can be viewed as a measure of disorder or decay in a system (von Bertalanffy, 1968). In other words, a system will break down if not properly managed or controlled. According to Coole and Brooks (2014), as the entropy of a system increases, its capabilities decrease. This is based on the belief that systems rely on some form of order and cohesion to exist. At its core, an organization is composed of several subsystems which each have a unique function or objective.

In this study, I uncovered the strategies used to prevent data breaches caused by mobile devices, which is one of the main objectives of information security. In the next section of the literature review, I will take an in-depth look at the history of general systems theory and how it has evolved over the years into one of the main theories utilized by scientist and practitioners.

General Systems Theory

In 1937, Ludwig von Bertalanffy first presented his idea of a general systems theory at a philosophy seminar in Chicago (Wilson, 2012). However, it was not until 1946, when the first publication of a general systems theory was released to the public (Thomas, 2015). The section below outlines the aims of general systems theory:

von Bertalanffy (1968) defined the aims of the theory as follows:

- (1) There is a general tendency toward integration in the various sciences, natural and social.
- (2) Such integration seems to be centered in a general theory of systems.
- (3) Such theory may be an important means for aiming at exact theory in the nonphysical fields of science.
- (4) Developing unifying principles running

“vertically” through the universe of the individual sciences, this theory brings us nearer the goal of the unity of science. (5) This can lead to a much-needed integration in scientific education. (p. 38)

von Bertalanffy (1968), hypothesized that general systems theory can be applied to all of the sciences concerned with systems. Furthermore, von Bertalanffy (1972), posited that the relationships between the components of a system are more important when compared to the components themselves. According to Bernard, Paoline and Pare (2005), general systems theory made attempts at developing generalizations such as all systems have some common characteristics and that it was useful to understand these similarities in an effort to understand how all systems function.

Over the years, several contributing authors have expanded the theoretical model first proposed by von Bertalanffy. Researchers von Bertalanffy, Juarrero, and Rubino (2008), further built up von Bertalanffy's work, stating that systems can be seen as both inputs and outputs working in congruity to satisfy the objectives of the organism. According to Kast and Rosenzweig (1972), in the 19th and early 20th centuries, researchers revised systems theory to accommodate social systems, communication, and other forms of holistic thinking. A holistic view must be used with any organization to ensure that all of the components of the system are addressed.

This type of thinking forms the core of a security manager, as he or she must look at every element of the system/network and determine what is functioning as designed and what elements need to be modified to ensure the survival of the system. Kast and Rosenzweig (1972), addressed several key concepts put forth over the years by many of

the contributing authors (Benton, González-Jurado, Beneit-Montesinos, & Fernández, 2013):

- feedback
- open to environment
- homeostasis
- teleology or purpose
- input-transformation-output process
- interrelated subsystems
- equifinality
- entropy

Based on an extensive review of literature, the target organization of this study can be classified as an open system and viewed through the lens of general systems theory. Organizations are either simple or complex systems (von Bertalanffy, 1972). A complex system is one that includes several other microsystems. As noted by von Bertalanffy (1972), educational institutions such as universities and colleges can be characterized as being systems. Furthermore, Suter, Goldman, Martimianakis, Chatalasingh, DeMatteo and Reeves (2013) postulated that general systems theory addresses complex systems such as hospitals, schools, and organizations.

When security manager's views the organization as a complex system, several critical concepts comes into play, including synergy, open systems, and subsystems. According to Nguyen and Bosch (2013), open systems interact with their environment and use it to adapt or determine the best fit. As most organizations are considered to be

open systems, which means they interact with their environment, this will help in determining which components of the system are not functioning as designed thereby affecting the equifinality of the system.

As noted by Stephens (2013), most organizations contain several subsystems. With the use of general systems theory, the organization can be viewed as a purposeful system of interrelated subsystems working in conjunction with each other to achieve a common goal in an ever-changing environment (Wang, Shi, Nevo, Li, & Chen, 2015). Any change or deviation in one subsystem will impact the overall organization or system.

Another critical concept is synergy. As Ludovic-Alexandre and Marle (2012) point out, units or subsystems of the organization thrive more when they work together rather than independently. According to Johnson (2013), systems theory is made up of inputs, outputs, and processes that, when analyzed, bring about a better understanding of how to improve the system by making it more reliable and efficient. In essence, by using a systems theory approach, a researcher will be able to better understand the root of the problem the system is experiencing which in turn will lead to a solution that ultimately makes the system more reliable.

One final critical concept to systems theory is entropy. The second principle in thermodynamics refers to entropy in a closed system as a quantity that must increase to a maximum until it comes to a stop at a state of equilibrium (von Bertalanffy, 1968). Entropy is the measure of disorder or decay in a system (von Bertalanffy, 1968). According to Coole and Brooks (2014), the term entropy is hard to conceptualize and often misunderstood one central theme conveys how various components of a system

relate to each other towards producing a coherent whole. At the heart of any organization is the protection of its data.

In this section of the study, information security and its relationship to systems theory and the specific IT problem addressed in this study are synthesized for the reader. One of the primary goals of many technology organizations is information security. According to Knowles, Prince, Hutchison, Disso, and Jones (2015), information security--also referred to as InfoSec--encompasses the protection of information or data by the organization. The National Institute of Standards Technology (2013), further defined information security as “the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.” At the heart of information security is the protection of the organizations sensitive data from unauthorized access. One of the goals of the organization or system is information security. ISO/IEC 17799 establishes the guidelines for information security centered around three key elements (Anton & Nedelcu, 2015):

- 1) Confidentiality
- 2) Integrity
- 3) Availability

These three elements are part of the CIA triad (de Oliveira Albuquerque, García Villalba, Sandoval Orozco, Buiati, & Tai-Hoon, 2014). According to Wilson (2012), general systems theory has evolved from a purely biological concept to include organized entities such as technology all working to reach the established goals of the organization.

An integral part of an organizations business and IT strategy is the protection of its information assets (Knapp & Ferrante, 2012). Barr (2013) states that systems theory can be used by organizations to address complex business problems such as information security. According to Montgomery and Oladapo (2014), a general systems theory approach allows for an integrated approach or the examination of relationships between two or more systems. In other words, systems theory encourages the researcher to view the organization as a whole and not through the isolation of variables (Montgomery & Oladapo, 2014). Furthermore, systems theory enables the organization to function as a whole system made up of several integrated parts all working to achieve the organizations mission (Barr, 2013).

As organizations continue to embrace new technological advancements, the organization must embrace these new advancements. As noted by Hammond (2010), organizational components must function as one. To accomplish this goal, security managers must utilize strategies that not only meet the needs of the organization but also protect its information assets from internal and external threats. As noted by Anton and Nedelcu (2015), “the systemic approach to the management of information security is based on approaching the system as an integrated information security system, characterized by the achievement of steady state through the contribution of all the components of the system”. A system essentially consists of objects (physical or logical), attributes that describe the objects, relationships among the objects, and the environment in which the system is contained (Gutiérrez-Martínez, Núñez-Gaona, & Aguirre-Meneses, 2015). As Chai, Kim, and Rao (2011), points out, disruptions in an

organizations information system could threaten the survival of the organization or system. As organizations continue to evolve, security managers must take this into account to ensure the survivability of the system. As posited by Kira and van Eijnatten (2013), an on-going study is required to ensure the sustainability of any open system.

According to the researcher Thomas (2015), every business is an organization that contains multiple subsystems all working in harmony to meet the goals of the organization. In essence, at its core, every system has a defined goal. Hammond (2010) contends the focal component of systems theory is the actual system, which is viewed as complete when all of its parts are functioning as designed. In other words, a system can be characterized as any object of study that, despite the fact that comprising of various components commonly interconnected and communicating with each other or the external environment, reacts or evolves as a whole with its own general rules (Andretta, 2014). Furthermore, according to systems theory, nothing can be comprehended in isolation, but must be seen as part of a larger system (von Bertalanffy, 1968). In systems theory, complex systems are modeled as a hierarchy of levels of organization, each more complex than the one below, where a level is characterized by having emergent or irreducible properties (Young & Leveson, 2014). According to the authors of recent article current information security models being utilized by most organizations fail to properly manage the policies, risks, people and assets effectively (de Oliveira Albuquerque, García Villalba, Sandoval Orozco, Buiati, & Tai-Hoon, 2014). In the article, de Oliveira Albuquerque et al. (2014), outline the current issues with information security models and propose a new layered trust information security architecture (TISA)

model using a holistic approach to information security. As noted by von Bertalanffy (1968), a holistic approach should be used when designing any system. This new layered (TISA) model (see Figure 1) below, shows how all of the components are connected regarding information security and how all the security architecture elements interact with one another (de Oliveira Albuquerque et al., 2014).

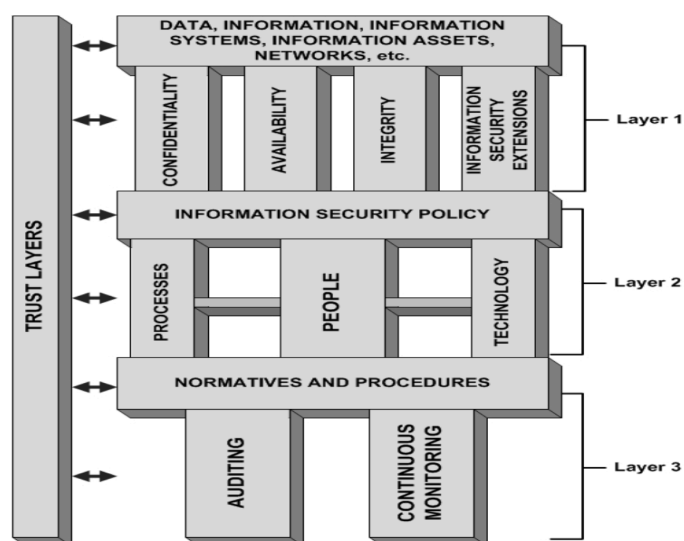


Figure 1. TISA: Layered trust information security architecture (Reprinted from de Oliveira et al., 2014)

Mobile devices and information security can be managed but only through the use of specific strategies employed by security managers. As Savola (2014), points out, the confidentiality, integrity and availability of data can be compromised through vulnerabilities, threats and attacks of the system which can be either intentional or unintentional. With the introduction of mobile devices into the equation, security managers must ensure these devices are included in their overall information security policy. Mobile devices which are vulnerable to a unique risk of loss or theft could

potentially lead to the loss of confidential data or give the intruder access to the organizations enterprise network (Tu, Turel, Yuan, & Archer, 2015). For several decades, network security was the main layer of defense for computer systems against malicious software and hackers (Basem, Ghalwash, & Sadek, 2015). As mobile devices continue to become progressively prevalent, so do the incentives for hackers, particularly when transactions conducted via a mobile device reached US\$630 billion dollars in 2014 and continue to climb (Bhattacharya, Yang, Guo, Qian, & Yang, 2014). Security managers must implement solutions and security strategies designed specifically for mobile devices to prevent information security breaches. To combat these new challenges introduced by mobile devices, organizations must make every effort to address the information security needs of the organization.

Overall, the introduction of mobile devices into the equation has changed the parameters for the types of information being accessed as well as how the information is accessed. Technological innovations such as the Internet, smartphones and other portable devices allow organizations around the world to interconnect to help streamline business communications. According to Silic and Back (2013), employees today are using their personal mobile devices to access organizational data as well as social media sites such as Facebook and Twitter which raises unprecedented threats to information security, the organization must address. Some organizations such as Hospitals and other Medical organizations are being mandated to ensure compliance with the enactment of federal laws designed to ensure the protection of consumer data. One recent article titled “The HIPAA conundrum in the era of mobile health communications”, highlights the need for

strategies healthcare organizations need to implement to protect healthcare data being accessed via mobile devices. According to the authors of the article, both physicians and patients use their own unsecured personal mobile devices to access electronic health records (Wand et, al, 2013).

The abundant list of studies reviewed for this literature indicates the need for strategies security managers can implement to prevent data breaches due to mobile devices is greater than ever. A recent article in the New England Journal of Medicine outlines several steps security managers can implement to protect and secure information when using mobile devices (Taitzman, Grimm, & Agrawal, 2013):

- The installation of encryption software on the mobile device
- Enforce some form of user authentication on the mobile device
- Prevent the use of file-sharing applications
- Ensure all security software updates are pushed to the device
- Remind employees to maintain physical and visual contact with their mobile devices at all times
- The installation of a firewall to prevent unauthorized access
- Enable remote wiping of any device being used for work purposes

As this section on information security has shown, at the heart of information security is the protection of the organizations sensitive data from unauthorized access. To accomplish this, security managers must implement strategies designed to mitigate the risks associated with mobile devices. As Alebrahim, Hatebur, Fassbender, Goeke, and Côté (2015) point out; one of the essential components in achieving information security

is risk analysis, which is an essential part of the ISO 27001 standard. The International Organization for Standardization (ISO) established the ISO/IEC 27001 standard in 2005, which outlines the requirements for implementing, establishing, operating, reviewing, monitoring, maintaining, and improving security management systems and overall security governance for the organization (Alebrahim, Hatebur, Fassbender, Goeke, & Côté, 2015). At its core, the security standard ISO 27001, identifies risks, vulnerabilities, and threats to the organization as the main objectives (Alebrahim et al., 2015).

In this section of the study, data breaches and its relationship to systems theory and the specific IT problem addressed in this study are synthesized for the reader. Although mobile devices offer organizations increased productivity, these devices also bring with them increased security risks for the user and ultimately the organization. As Kesh and Raghupathi (2013) point out, these new security risks can have far-reaching and significantly disruptive consequences for the organization. One of the biggest security risks these types of devices introduce is the data breach. As noted by Wikina (2014), data breaches represent the most prevalent privacy risk arising from loss of control of information in either electronic or paper form by an organization, its vendors (business associates), or a malicious third party. About 22% of security executives surveyed by the CSI and Federal Bureau of Investigation (FBI) indicated their organization had experienced some form of a data breach within the year (Zhao, Xue, & Whinston, 2013). Based on the CSI/FBI survey, exploring the strategies security managers' use to minimize data breaches is a business necessity.

Over the last three to five years, data breaches have become a serious problem

affecting organizations around the world. According to a recent study by Liu, Musen, and Chou (2015) a data breach has happened in every U.S. state including Puerto Rico and the District of Columbia, and five states California, Florida, New York, Illinois and Texas represented over a third of the total number of reported breach incidents. One of the highest profile data breaches of 2013 was against the retailer Target. Liu et al. (2015) stated that out of 949 data breaches that occurred between 2010 and 2013, where caused due to mobile devices such as laptop computer or other portable electronic devices. The significance of information security to a firm's strategy means leaders should view security breaches as a threat to organizational success (Fleming & Faye, 2013).

According to Ben-Asher and Gonzalez (2015), the protection of enterprise systems from vulnerabilities is the responsibility of security managers. To develop an effective security response plan, analysts need to detect and analyze data breaches to identify network threats and vulnerabilities that might lead to a data compromise (Ben-Asher & Gonzalez, 2015). As Densham (2015) points out, every organization must come to the realization and expect a data breach to happen. By doing this, the organization is prepared for the worst and has planned for the attack and the aftermath of the breach. Outlined below are three cyber-security strategies the security manager of the organization can use to mitigate the impact of a data breach (Densham, 2015):

- 1) Response in depth (RID) – this strategy is broken down into six steps:
 - a. Detection – this step involves the collection of log files
 - b. Aggregate – once the log files have been collected, the next step is to correlate and normalize the data

- c. Analyze – detailed analysis of the normalized log data
 - d. Identify – indicators of compromise (IOCs) will help to facilitate the identification of breach events and any other forms of malicious activity
 - e. Respond – this step is broken down into three sub steps: contain the breach, remediation, and finally recover any services that may have been affected during the breach
 - f. Improve – security team should meet and conduct an after-action review which includes the identification of any lessons learned
- 2) 360-degree security – this strategy encompasses the securing of networks, people and processes. Periodic and deliberate testing of the network, systems, applications and employees. Implementation of a governance process based on risk assessments, security governance, compliance/audit activities, and security awareness training. A holistic approach to monitoring that encompasses the environment, employees and security events.
- 3) The avocado and the coconut – this strategy calls for network segregation where the organization accepts a level of risk for the Internet connected part of the network while having a hardened core portion of the network that houses all of the organizations valuable data that is only accessible while connected to the corporate network.

One of the strategies outlined above, response in depth fits in with a systems thinking approach and how organizations should use systems theory to develop a proactive security strategy. As noted by Mangal (2013), four key areas that determine

how well systems function are:

- 1) self-organization
- 2) resilience
- 3) efficiency
- 4) hierarchy

Resilient systems are designed using a systems thinking approach to ensure the system is capable of recovering from a setback caused by internal or external forces (Mangal, 2013). One of the key concepts of general systems theory relates to hierarchy and the relationship between components of the system (Kast, & Rosenzweig, 1972). In the end, successful security managers use strategies to prevent data breaches caused by mobile devices that are designed using a systems thinking approach. One of the key tenets of systems theory is that systems contain many interconnected parts, which must be considered as a whole and not independently (Zenko, Rosi, Mulej, Mlakar, & Mulej, 2013). Which is why a defense-in-depth (DiD) approach to security is appropriate for complex organizations. The defense-in-depth (DiD) strategy is based on a decades old military strategy, which pushed for a defense that would seek to delay an attack while the military worked to stop the attacker (Stytz, 2004). The main concept behind defense-in-depth (DiD) is that layered security mechanisms increase the security of the system as a whole (Ibor, & Obidinnu, 2015). In other words, there is no one line of defense when it comes to the network or the assets being managed by the security managers of the organization. As Ibor and Obidinnu (2015) suggest, a DiD strategy should be implemented utilizing a systems approach based off of general systems theory. This

section of the study has explored the creation and advancement of general systems theory and reviewed some of the key tenets of the theory that will be used to drive this study.

Supporting and contrasting Theories

Due to the nature of this study, general systems theory was chosen for the conceptual framework to help understand the phenomena and to uncover the strategies used by security managers to prevent data breaches caused by mobile devices. The following section breaks down theories that either support or contrast the chosen theory for the study.

As there are many theories to choose from a researcher must look at each theory and determine if the theory will help to answer the central research question. One supporting theory is the high reliability theory, which emerged in 1987 out of the desire by researchers to understand why highly reliable organizations ranked very low in errors or failures (Chassin & Loeb, 2013). According to Chassin and Loeb (2013) one of the salient characteristics of highly reliable organizations is their drive to not be satisfied with the status quo of their current level of safety. Much like general systems theory which encourages the researcher to look at the organization and their environment as one whole and not as individual entities, high reliability theory involves the study of organizations capable of avoiding failures while providing operational capabilities under a wide range of environmental conditions (Karniouchina, Carson, Short, & Ketchen, 2013; Boin, & van Eeten, 2013). Both theories involve complex systems and how their environment affects the life cycle of the overall system. The only difference is high reliability theory deals primarily with nuclear power plants and air travel organizations,

which manage processes that could result in a major disaster (Chassin & Loeb, 2013) whereas general systems theory can be applied to a wide range of complex systems including the organization chosen for this study, a government contractor located in the southeastern region of the United States.

Another theory that was considered for this study but ultimately was not chosen, as it did not meet the needs was grey systems theory. In contrast to general systems theory a researcher could utilize grey systems theory, which was first proposed by Professor Julong Deng in 1982 (Deng, 1982). According to Deng (1982), a grey system is characterized as having knowns and unknowns. The ultimate goal for grey systems theory is to help bridge the gap between the natural science and the social sciences (Deng, 1982). With grey systems theory, the problem at hand is studied using small samples and or poor information (Sifeng, Liangyan, Naiming, & Yingjie, 2016). In essence, all of the pieces to the puzzle are unknown and the researcher must make assumptions and or draw conclusions based on partial information. According to Gilstrap (2013), as opposed to grey systems theory, systems theory could be used to identify problems and form patterns and relationships. In this study, all of the elements involved in the problem are known or available which is why general systems theory was chosen to drive the framework for this study.

Ultimately, general systems theory was selected to drive the conceptual framework of this study for the following reasons. First, it can be applied to the target organization of the study as it meets the criteria of being classified as an open system. Second, general systems theory encourages a holistic approach when researching any

problem which will help guide this study through the process of uncovering the strategies used by security managers to prevent data breaches caused by mobile devices. And finally, with the use of general systems theory, the organization can be viewed as a purposeful system of interrelated subsystems working in conjunction with each other to achieve a common goal in an ever-changing environment (Wang, Shi, Nevo, Li, & Chen, 2015). The next section of the study discusses the major themes uncovered during the review of literature for this study.

Bring Your Own Device

In the following section, Bring Your Own Device (BYOD) is synthesized for the reader. BYOD is becoming an increasingly common practice with organizations around the World as it allows the employees of the organization to use their own personal mobile devices to access the organizations network from any location with access to a cell tower or Wi-Fi hot spot (Chang et al., 2014). According to Longo (2013), BYOD is one of the most pervasive and fastest growing phenomenon security managers have to deal with in terms of security risks faced by organizations. The benefits of BYOD are huge with the biggest benefit being increased productivity for the organization. A recent IBM Flex workplace study showed increases in productivity of 20%, or the equivalent to an extra day of work per week (Chang et al., 2014). However, BYOD programs can introduce significant security risks such as data leakage, data loss and data breaches. As Patten and Harris (2013) point out, mobile devices, including BYOD and corporate issued devices, all pose new problems for IT professionals who do not quite know how to handle the problem yet. To effectively tackle data security and minimize data breaches, businesses

need to address what makes them vulnerable – BYOD, consumer technologies and out of date strategies for sharing and protecting data (Khanna, 2013). To help with the mitigation of these risks the organization must implement a comprehensive BYOD policy that includes a mobile device management (MDM) solution (Semer, 2013).

One alternative approach to BYOD is addressed in the following paragraph. Any organization opposed to BYOD may consider the so-called Corporate owned and personally enabled device, or COPE program (Feigelson, Jim, Serrato, & Jonathan, 2016). With any new program the security manager must do a comprehensive risk analysis to ensure which approach is the best for the organization. Although the COPE approach is considered a less risky option when compared to BYOD, it still does present the risks of commingling the employee's personal uses and data with the company's (Feigelson, Jim, Serrato, & Jonathan, 2016). In the end, the organization must consider the risks associated with allowing its employees to use corporate owned mobile devices for both work and personal matters.

BYOD represents a huge paradigm shift from past IT models. Past IT models typically revolved around the organization restricting access to the corporate network to only corporate owned devices (Pinchot & Poullet, 2015). With the use of VPN technology and a mobile device users can now connect to their organizations network using a personal tablet or smartphone. The younger more mobile workforce expects to be able to use his or her own personal devices at work (Earley et. al, 2014). These devices however, represent a huge vulnerability for the organization. As Mansfield-Devine (2014), points out, when an attacker goes after an organization the entry point is typically

the mobile device, once a sophisticated piece of malware has been injected into the mobile device this gives the attacker access to the rest of the organizations network.

BYOD is here to stay so security managers must be prepared and have a plan of attack. To address these risks security managers must adopt a comprehensive BYOD policy. As data security and privacy are key factors for the organization, the BYOD policy must address the risks associated with its employees using personally owned mobile devices for work purposes (de las Cuevas, Mora, Merelo, Castillo, García-Sánchez, & Fernández-Ares, 2015). Although most organizations feel BYOD policies are important, the majority of them fail to implement them. According to a recent survey conducted by the SAANS institute on BYOD policy use in organizations shows some alarming statistics (Vignesh & Asha, 2015):

- 36% of the organizations surveyed stated the organization had no formal BYOD policy in place
- 23% stated mobile devices are not permitted
- 14% of the organizations left it up to their employees to secure and monitor their own devices

Because BYOD is still a fairly new concept organizations are struggling to create comprehensive policies that can ensure the organizations sensitive data while providing the employee with the access they need to do their job. According to the authors of *Modifying security policies towards BYOD*, most BYOD policies currently in place are vague and generally immature (Vignesh & Asha, 2015). To address this risk, Vignesh and Asha (2015), have proposed a new 3-tier enhanced BYOD policy architecture, which

addresses the policies to be followed by the device, the applications and the organization. This new architecture (see Figure 2) below has been designed to address all of the required policies while not compromising the productivity these mobile devices bring to the organization.



Figure 2. BYOD multilevel security policy – Organizational level, Application level, and Device level policies (Reprinted from Vignesh & Asha, 2015)

As the figure above illustrates, an effective BYOD policy must not only address the mobile device but it must also incorporate the users applications, as well as permissions inside the organizations environment which are controlled by agreements and access control level list. As organizations come to the realization that BYOD is here to stay, security managers must take steps to develop and implement strategies the organization can use to prevent data breaches caused by these mobile devices.

Mobile Device Management

In the following section of the study, mobile device management (MDM) and its relationship to the specific IT problem is synthesized for the reader. In today's economy, to meet the needs of its customers as well as its employees, the organization must utilize some form of mobile device. As the number of mobile devices continues to increase, security managers must find ways to ensure the sensitive data stored or transmitted on these devices remains secure from both internal and external threats. As Chol-Un, Dok-Jun, and Song (2013) point out, with the massive use of mobile storage media for personal and confidential data by users a method of managing these devices is a necessity for organizations. In the summer of 2013, Check Point software technologies released its annual mobile-security report. According to the report, out of the 800 IT professionals surveyed, 42% stated they suffered a data breach due to a mobile device (Leavitt, 2013). With these types of numbers, security managers must incorporate strategies to help with the prevention of a data breach due to a mobile device.

One strategy security managers have started implementing to help with the administration of mobile devices in the organization is the use of some form of a mobile device management (MDM). Mobile device management (MDM) allows the organization to manage, monitor and secure the mobile devices used by its employees (Leavitt, 2013). MDM is typically implemented with the use of a third party software product that includes management features for particular vendors of the mobile devices. Security managers must come to the understanding that the organizations data no longer resides behind a corporate firewall, which is why an MDM system is such an invaluable tool for

the security manager. As Rhee, Won, Jang, Chae, and Park (2013), points out, an MDM system is used to manage smartphones, and other mobile devices remotely by monitoring their status and controlling their functions. Ultimately, the MDM system allows the organization the ability to ensure the organizations data remains safe and secure from both internal and external threats of the organization. Figure 2 below outlines some of the common functions an MDM will provide the organization.

Function	Description
Application Management	Install and uninstall enterprise applications Execute and stop enterprise and non-enterprise applications Update enterprise and non-enterprise applications Prevent uninstallation of enterprise applications Remove non-enterprise applications Install certificate
Device Management	Enable and disable camera, screen capture, Bluetooth, Wi-Fi, GPS, microphone, synchronization, etc. Control access point
Device inventory	Check assigned IP address, SIM state, OS information, application ID/name/version, Bluetooth status, Wi-Fi status, GPS status, phone number, IMEI, hardware resource information, data roaming setting, device type, etc.
Security Management	Remote device lock and unlock Remote device data wipe Remote device reset Push and remove configuration data Set password and password policies (combination, length, history, failure count, etc.) Encrypt and decrypt data Configure account (Exchange ActiveSync, e-mail, VPN, etc.)

Figure 3. Functions of an MDM System (Reprinted from Rhee et al., 2013)

The key to any strategy for preventing data breaches caused by mobile devices is to find a balance between what works and what doesn't. With every step the organization takes the security managers must look at the pros and cons of the strategy and determine if this new strategy will work for the organization and assist the IT team with the prevention of data breaches while at the same time allowing the users of the mobile

devices the ability to use their devices for work purposes. The key with mobile device management (MDM) is to find a balance between being too restrictive and too lenient. A recent article titled “Going beyond mobile device management” takes an in-depth look at how an organization should manage its mobile devices. As the author, Steiner (2013) points out, one question organizations have a hard time answering is, should the focus be on the protection of the mobile device or on the proprietary enterprise content being accessed by such devices? According to the author Steiner (2013), the answer is both. Four critical questions every security manager must address to ensure their organization is managing its mobile devices correctly are outlined below (Steiner, 2013, p. 20):

- 1) How are the employees authenticated?
 - a. The key here is ensuring you have adequate layers of protection in the form of authentication protocols
- 2) Who has access?
 - a. The goal here is to ensure only authorized employees have access to the organizations network. This can be accomplished with tight integration with LDAP and Active Directory.
- 3) How are files opened?
 - a. Key strategy here is that any files accessed via a mobile device are not stored locally as this can result in data duplication and unwanted data breaches.
- 4) How is data synched and stored?

- a. Continuous synching of data between the organizations network and the mobile device should be avoided as data in transit provides an ideal target for hackers.

Defense in Depth

In this section of the study, defense-in-depth is synthesized for the reader. With the proliferation of mobile devices the organization must now account for and manage not only its internal network but also the mobile devices its employees use while connected to external networks. With this, security managers must take every step to ensure these mobile devices remain secure and the organizations data remain safe from both internal and external threats. Unfortunately, there is no silver bullet when it comes to information security but there are strategies security managers can implement to help with the prevention of data breaches caused by mobile devices. One such strategy is a multi-layered defense-in-depth (DiD) approach. In a recent article titled “A new month, a new data breach”, the author German (2016) discusses defense-in-depth and how this approach that combines multiple layers of prevention and detection technologies is essential in the prevention of information security data breaches. According to Ahmad, Maynard, and Park (2014), information security systems should be designed using a layering approach where overlapping security measures are deployed so that if one layer is breached the next one takes over. As noted by von Bertalanffy (1968), a holistic approach should be used when designing any system. In essence, security managers must look at the organization as a system containing several subsystems all working together to achieve one common goal. In this case, the goal of information security and protecting

the organizations data. As noted earlier, a defense-in-depth strategy towards security requires the organization to take a holistic approach. A system should be viewed as a grouping of elements that are organized in a particular way (Mangal, 2013). As the key theme behind defense-in-depth focuses on the layering of defenses, systems thinking can be applied to ensure the strategy is organized to not only meet the needs of the business but also the protection of the organizations information from both internal and external threats. As noted by Sampemane (2015), with the continued use of mobile devices within organizations the security administrators must implement internal access controls when designing the system to limit the exposure of a hack to a single system and not the entire network. This is accomplished by using a DiD approach to information security or looking at the system as a whole and breaking it down into smaller components or subsystems. Implementing an effective DiD strategy will require taking a holistic approach that leverages all of the resources of the organization to provide effective layers of protection (U.S. Department of Homeland Security, 2009).

Figure 4 below shows the key elements of a defense-in-depth strategic framework, which addresses several key strategies organizations, should utilize to prevent data breaches caused by mobile devices:

- policies and procedures
- training and awareness
- personnel
- technology
- security controls

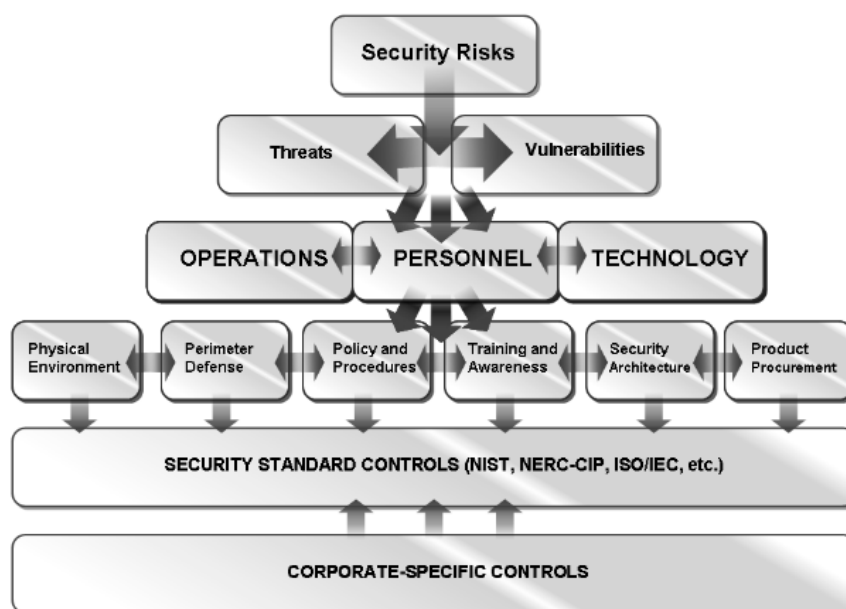


Figure 4. Defense-in-Depth Strategic Framework (Reprinted from U.S. Department of Homeland Security, 2016)

Transition and Summary

The purpose of this study was to explore the strategies security managers use to secure mobile devices to prevent a data breach. The extensive review of literature helped to establish a scholarly foundation for this study while providing a critical analysis of the body of knowledge related to the research question. The literature review was broken down by theme to help guide the reader through the extensive amount of research on the study topic.

Section two of the study will explain the rationale for using a qualitative single case study to explore the strategies security managers use to secure mobile devices to prevent a data breach. In addition, section two will also be described in detail, the role of the researcher, participant selection, population and sampling, data collection and

analysis and finally how this study was completed to ensure the reliability and validity of the study.

Section 2: The Project

The objective of this study was to explore strategies security managers use to prevent data breaches resulting from lost or stolen mobile devices. This section of this study also includes the purpose statement, role of the researcher, participants, the research method and design, population and sampling, and data collection, including organization and analysis, reliability and validity.

Purpose Statement

The purpose of this qualitative single case study was to explore strategies security managers use to secure mobile devices to prevent a data breach. The target population consisted of security managers who utilize strategies to prevent data breaches caused by mobile devices from an organization located in the southeastern region of the United States. The security managers participated in semistructured interviews to explore the strategies they currently use to prevent data breaches caused by mobile devices.

The findings of this study may ultimately benefit not only the organization but also the customer by protecting their confidential data from potential data breaches. In addition, this study outlines some strategies for preventing data breaches caused by mobile devices while still providing maximum benefit to its external and internal customers. Organizations may continue to see the benefits from allowing its employees to use mobile technology while at the same time the customers of the organization will remain confident their personal data are not at risk. Data from this research could potentially provide security managers with some strategies they can implement at their institutions to prevent data breaches caused by mobile devices.

Role of the Researcher

I was the main data collection instrument for this qualitative study. As posited by Pezalla, Pettigrew, and Miller-Day (2012), in a qualitative study, one of the researcher's roles in the study is that of the data collection instrument. For this study, I collected all of the data utilized to answer the central research question. Data collection for this study included conducting semistructured interviews and reviewing of the organizational documents from the target organization.

My experience in the IT industry was key in understanding the concepts presented and the data collected for this study. Although I do work for the same organization where the participants were sourced, I work in a different department with no ties to any of the participants selected for this study. Furthermore, I had no contact with participants occurred prior to receiving official approval from the Walden University IRB.

To further ensure an ethically sound study, I completed the National Institute of Human web-based training course and adhered to all of the ethical protocols outlined in the Belmont report, which include the protection of all participants of the study through the use of protocols designed to ensure the privacy and confidentiality of all participants, by eliminating or reducing the potential risk faced by participants, and finally by providing full disclosure to all participants (U.S. Department of Health and Human Services, 1979).

There is a potential for bias in any study and it must be addressed to ensure an ethically sound study. As Bernard (2013) stated, a researcher's cultural background and/or ideologies may contain biases that could affect the study. This may happen during

the data collection process. Strategies for reducing bias on the part of the researcher throughout the data collection and analysis include writing memos, maintaining a reflective journal, and finally engaging in interviews with an outside third party (Lamb, 2013). I maintained a reflective journal throughout the interview process to help mitigate any bias. To further help mitigate bias member checking was also utilized in this study.

I conducted all of the semistructured interviews for this study utilizing an interview protocol (see Appendix A). Furthermore, every participant of the study was asked the same initial interview questions(see Appendix B) to ensure consistency. I utilized a semistructured interview protocol throughout this study to help mitigate any researcher bias and to aid in the fostering of a relationship between the interviewer and the participant. As posited by Doody and Noonan (2013), researchers typically use an interview protocol to make the participants of the study feel more comfortable or at ease with the research process. In the end, the use of an interview protocol helped foster a relationship with the participants of the study and aided in the mitigation of bias during the semistructured interviews.

Participants

The participants in this study included security managers with experience in the implementation and use of strategies to prevent data breaches caused by mobile devices. For this study to be effective, participants were required to meet specific criteria. As noted by Draper (2015), participants of a research study should have experience with the research topic. I selected the target organization based on its use of mobile devices for organizational purposes. To be eligible for this study, I required every participant of the

study to meet specific eligibility criteria, which according to Strom et al. (2014) refers to the parameters (e.g., job title, and experience) set down by the researcher to ensure all participants qualify for participation in the study.

Each participant of the study selected from the target organization had no less than 10 years of experience as a security manager, had expertise in the implementation of strategies to prevent data breaches caused by mobile devices, and every participant of the study was required to agree to all of the terms in the informed consent prior to participation in the study. According to Limburgh et al. (2013) eligible participants of a study are defined as having knowledge of or experience with the phenomenon under investigation. The rationale for selecting security managers as the participants of this study was that they are typically involved with the creation and enforcement of information security policies for the organization related to mobile devices.

Before the collection of data began, I used census sampling to obtain suitable participants that met all of the eligibility criteria required for this study. According to McAreevery and Das (2013), gaining access to participants requires approval from gatekeepers who regulate access to the groups or organizations a researcher is targeting. A request to cooperate was emailed to the target organization human resources department seeking approval to reach out to potential participants for the study.

According to Cacari-Stone, Wallerstein, and Minkler (2014), participants are more likely to agree to participate in a study if the research problem is relevant to their field of study and may result in helping their organization policy wise. Once a signed copy of the letter of cooperation had been received from the target organization, I reached

out to the CIO of the organization to obtain contact information for all prospective participants. Using the list provided to me by the CIO all prospective participants of the study received an invitation to participate in the study via e-mail. This invitation outlined the purpose of the study along with the potential benefits participants of the study may gain, which includes possible enhancements to their own organizational security policies. All participants were required to sign a consent form prior to data collection to ensure the study met IRB requirements outlined by Walden University.

Building a solid working relationship with the participants of the study was key. According to Anyan (2013), a participant's willingness and openness to divulge quality data is driven by the relationship of the interviewer and the interviewee. To ensure honest and open feedback during the data collection process I formed a solid working relationship with all participants of the study. I treated every participant of the study as a professional in the IT field with the knowledge needed to complete this study. Doody and Noonan (2013) argued that building a good rapport with the participants of the study encourages the participant to be more open to the questions.

One method of building a good rapport with the participants was to conduct the interviews in their office or in another suitable location at their place of work. Seidman (2013) stated that building trust with the respondents could be accomplished by assuring them the results of the study will remain confidential. I formed an open relationship with the participants of the study by keeping the lines of communication open, establishing the confidentiality of the study at the beginning of the interview and throughout the process while acknowledging any and all concerns raised before, during or after the interview. I

reminded all participants of the study the data collected would remain 100% confidential and if any questions arose, to feel free to contact either the Walden University IRB or myself.

Research Method and Design

There are three main types of research methods: qualitative, quantitative, and mixed methods. The method selected for any research study should be chosen based on the goals of the study and the central research question (Hayes, Bonner, & Douglas, 2013). The focus of this study was to explore, from the perspective of security managers, strategies used to prevent data breaches caused by mobile devices.

Research Method

I chose the qualitative approach for this research study based on extensive review of the available research methods. Qualitative research involves the collection of data and the interpretation of that data based on patterns and traits exclusive to the participants of the study (Daigneault, 2014). As the focus of this study was to understand the patterns and traits of the strategies used by security managers to prevent data breaches caused by mobile devices, I selected the qualitative approach as the most appropriate. Researchers typically employ a qualitative approach when they seek to create themes from the analysis of data collected through semistructured interviews (Robinson, 2014). Anyan (2013) pointed out that a researcher should utilize a qualitative approach when the research problem cannot be easily measured or quantified. As the main focus of this study was not to determine the number of strategies in use but which ones are currently in use and why, I selected the qualitative approach as the best method to help answer the

research question. As noted by Bernard (2013), when a researcher utilizes the qualitative method, the participants of the study are provided with a venue to convey their points of view. Because the main focus of this study was solely on the participants' experiences. I chose to utilize the qualitative approach as the research method. The qualitative method enabled me the opportunity to explore the strategies used by security managers at the target organization to prevent data breaches caused by mobile devices.

I did not select a quantitative approach for this study, as this is typically a more objective approach. Quantitative research is ideal for studies seeking to answer research questions looking at how many as opposed to how or why (Venkatesh, Brown, & Bala, 2013). Furthermore, researchers typically utilize the quantitative method to solve a problem or formulate a hypothesis by looking at variables and their relationships (Frels & Onweugbuzie, 2013).

As the main purpose of this study was to explore strategies security managers use to prevent data breaches caused by mobile devices, the quantitative method could not meet my needs. Reviewing statistical information was not appropriate for this study as the intent of this study was to acquire rich, in-depth qualitative information to address the main research question.

I did not select a mixed-methods approach for this study as this method employs the use of both the qualitative and quantitative approach. A mixed-methods approach was initially considered for this study, however according to Hayes et al. (2013), a mixed-methods study uses a combination of both quantitative and qualitative methods, which was not a feasible option for this study. The analysis of variables would not have

provided the knowledge needed to address the research question for this study. As Petticrew et al. (2013) pointed out, a mixed-methods approach is suitable for synthesizing approaches wherein the data from a single study encompasses both qualitative and quantitative data collection. The purpose of this study was to explore the strategies used by security managers to prevent data breaches caused by mobile devices; thus, the qualitative approach alone was sufficient to answer the central research question.

Research Design

There are several qualitative study designs a researcher can choose from: case study, phenomenological, and ethnographic design. For this research study, I selected a single case study design. As Dresch, Lacerda, and Cauchick Miguel (2015) pointed out, a case study will provide the researcher with an understanding of a certain phenomena in-depth; thus, I chose to utilize a case study design as it provided me the tools needed to explore the types of strategies used by security managers to prevent data breaches caused by mobile devices.

According to Ketokivi and Choi (2014), a case study design encourages the use of diverse data sources while exploring phenomena within an existing context. Data for this study was sourced from multiple areas to include semistructured interviews, an extant review of literature and organizational documents gathered from the target organization. Sugar (2014) argues researchers using a case study design are able to engage in real world situations and make decisions using contextual clues described in the specific case. Therefore, the case study design was determined to be the most appropriate choice for exploring strategies security managers use to prevent data breaches caused by mobile

devices through the use of semistructured interviews and the review of organizational documents from the target organization.

The reasoning for not choosing a phenomenological design is outlined below. A phenomenological design is appropriate when the researcher seeks to study the meaning of lived experiences of a group of people around a specific phenomenon (Hunt, 2014). As the focus of this study did not revolve around lived experiences, rather around exploring a phenomenon within an existing context, a phenomenological design was not a suitable design. According to Wagstaff and Williams (2014), researchers who utilize a phenomenological design collect their data primarily through interviews, which has the potential to weaken the preferred depth and scope of the study. Furthermore, phenomenology is concerned with providing a direct description of human experience (Wells, 2013). Because the focus of this study did not revolve around the exploration of lived experiences, and this study sought to gather data from diverse sources a phenomenological design was not chosen.

And finally, an ethnographic design was not chosen for this study based on a comprehensive review of available literature. Researchers seeking to understand a culture in-depth will utilize an ethnographic design (Murthy, 2013). As the focus of this study was not centralized around the understanding of a workplace culture, the ethnographic design was not a suitable choice. Ethnographic research can be time consuming as the essence of ethnographic field research is to come to understand the framework of the people one is studying (Wilcox, 2012), which is not appropriate for this study, as the main goal of this study was not to get an in-depth understanding of security managers,

rather it was to explore the strategies security managers use to prevent data breaches caused by mobile devices. According to Agar (2014), an ethnographic design typically necessitates the researcher to become a part of the cultural group being studied. This study will not revolve around any specific cultural group, which is why the ethnographic design was not selected.

Population and Sampling

This section of the study describes the population, discusses the sampling method, addresses how data saturation will be achieved and discusses the setting for the semistructured interviews. The population for this research included security managers working for the target organization located in the southeaster region of the United States. Security managers were selected for the population as they have the knowledge and experience necessary to answer the central research question.

The three sampling strategies considered for this study where purposeful, convenience, and the census sampling technique. Due to the general nature of the research question, which sought to explore the strategies used by security managers to prevent data breaches caused by mobile devices, the design of the sample must seek a census across the participants. Therefore this study utilized the census sampling technique. According to Cleary, Horsfall, and Hayter (2014), in a qualitative study, the researcher must determine which participants will be a part of the population while ensuring a credible study. By utilizing the census sampling technique, I was able to quickly and efficiently identify potential participants for this study. According to Najafi, Alimadadi, Arastoo, Motamed, Khodadad, Fallahi, and Doroudian (2014), census

sampling involves the identification of the sample and then the collection of research data from all participants in the population. Participants of a research study selected using census sampling are typically chosen for a specific purpose, and the rationale for using census sampling in this study is to work with a specific population to help answer the research question. As noted by O'Reilly and Parker (2013), sampling for the study should take into consideration resource availability and the nature of the topic. Census sampling was used to include all security managers in the target organization that met all of the eligibility criteria.

The following section breaks down the number of participants interviewed for this study. Generally speaking qualitative studies do not typically have a set sample size as the ideal sample size for the study is driven by the purpose of the study and the overarching research question (Elo et al., 2014). For this study, participants included security managers working for the target organization located in the southeastern region of the United States that met all of the eligibility criteria. The credibility of the research is partially dependent on the researcher obtaining an adequate sample size of participants (Marshall et al., 2013). Because this study utilized a census sample from the target organization, obtaining enough participants to answer the central research question was not a factor. According to Duxbury (2012), the optimum sample size of participants for case study research ranges from three to ten participants. The sample for this study included five security managers from the target organization.

The following section breaks down how data saturation was achieved in this study. Data saturation in research occurs when no new or relevant information can be

captured with additional interviews (Galvin, 2014). According to O'Reilly and Parker (2013), data saturation is achieved when the same answer is given with no variation in the interviews by the researcher. Data analysis software was used to help tie back participant responses to each interview question. When no new constructs within themes can be achieved, data saturation has been reached within the study (Heslehurst, Russell, McCormack, Sedgewick, Bell, & Rankin, 2013). Data saturation in this study was achieved through the collection of multiple sources of data, which included interviews and organization documents focused on strategies used to prevent data breaches caused by mobile devices. Member checking interviews with each participant of the study also ensured data saturation was reached as each participant of the study was given a chance to review and verify my interpretations of the collected data during a follow up member checking session. All of the follow up member checking sessions were conducted over the phone.

The semistructured interviews were conducted in a quiet and conducive environment to ensure an open dialogue during the interview process. The setting for interviews should be free of distractions, enjoyable, and one that encourages open responses from the interviewees, according to Schiebe, Reichelt, Bellmann, and Kirch (2015). The interviews were conducted at the participant's place of business or a mutually agreed upon location free of distractions. As noted by Doody & Noonan (2013), the location and setting for the interview can affect data collection; therefore, the chosen location should be convenient and comfortable. The locations of the interviews were convenient for the participant. Anyan (2013) posited that the process of conducting

interviews is made easier by choosing a quiet and comfortable environment as this encourages participants to share. The preferred interview location was on site at the participant's place of business in a designated meeting area free from distractions unless the participant chose to meet at another mutually agreed upon location. The participants also had the option to choose a telephone interview. All of the interviews were conducted at the target organization in a designated conference room.

Ethical Research

After receiving IRB approval 08-17-17-0511068 from Walden University, I invited potential participants an opportunity to participate in the study via e-mail. This e-mail contained a copy of the informed consent, the purpose of the study and a list of the interview questions along with my contact information. As noted by Chiumento, Khan, Rahman, and Frith (2015), the informed consent process is designed to ensure the rights of all participants are not violated in anyway. According to Crockett et al (2013), the informed consent process involves the providing of information to the participant, ensuring the participant understands the information and finally advising the participant that participation in the study is 100% voluntary. The consent form outlined (a) the purpose of the study, (b) criteria for participating in the study, (c) the researchers role in the study, (d) the process for withdrawing from the study, (e) data safeguards, (f) disclosure of incentives, and (g) the publication intent of findings. Every participant in the study was required to read and sign the informed consent form prior to participation in the study.

All participants of the study were advised that participation in the study was 100% voluntary and that they may withdraw from the study at any time with no repercussions as outlined in the informed consent form. I ensured every participant of the study clearly understood his or her rights to formally withdraw from the study at any time as outlined in the informed consent form. A critical component of every research study is the informed consent of every participant (Nishimura et al., 2013). Furthermore, each participant of the study was advised that no incentives would be offered to any participant of the study. As noted by Robinson (2014), researchers who offer incentives to participants for participation in their study can have adverse effects on the data. Therefore, participants of this study did not receive any incentives, rewards or payments to participate in this study.

To ensure no harm or risks came to the participants of this study all of the IRB legal and ethical requirements outlined by Walden University were strictly followed. The identities of all participants and the organization of the study will be kept confidential. According to Lohle and Terrell (2014), one method to protect the identities of participants involves measures to disguise identities. To ensure the participants and their collected data remain confidential, each participant was given a unique pseudonym (e.g., P1, P2). As noted by Gibson, Benson, and Brand (2013), confidentiality can be achieved by assigning each participant of the study a generic code. In addition, no identifiable markers such as the name of the participant or the target organization were used throughout this study.

And finally to ensure the data remains secure and meets all of the IRB requirements outlined by Walden University, all of the research data collected will be stored in a locked file cabinet. All of the electronic data will be stored on a password protected encrypted external hard drive. Five years from the date of publication of this study, the external hard drive and all of its contents will be permanently destroyed as well as any and all audio recordings, journals, and paper documentation.

Data Collection

In the section below, the data collection instruments that were used to gather evidence for this single case study are identified. As noted by Yin (2013), the types of data collected in a case study will typically include the review of documentation, the review of archival records, interviews, a review of physical artifacts and the direct observation of participants and or events.

Instruments

Data for this case study were collected from organizational documents relating to mobile device security and through semistructured interviews. According to Marbach (2013), the researcher is the primary data collection instrument in qualitative studies. I served as the main data collection instrument for this study as outlined in the role of the researcher, in charge of gathering all of the required sources of data. As noted by Barrett (2007), the researcher's wisdom, perception and subjectivity in the data collection process are pivotal for the study. My understanding of the research topic in conjunction with the conceptual framework helped drive the collection of the necessary data necessary to answer the central research question. Haahr, Norlyk, and Hall (2014)

underlined, researchers must perceive themselves as central instruments in the research process. As the main data collection instrument, I ensured all of the necessary data was collected during the study.

Interview data for this study was collected using a semistructured interview protocol (see Appendix A). Irvine, Drew, and Sainsbury (2013) expressed, semistructured interviews are the best method for gathering information for qualitative research due to the adaptability in outlining and refining the interview protocols and in conducting the interviews. The semistructured interviews enabled me an opportunity with each participant to ask follow-up clarifying questions that ultimately contributed to the collection of rich data. As noted by Yin (2013), documentation can be used to further expand and confirm the data collected from the interviews; thus, the organizational documents were used to augment the findings of the data collected during the interview process. Organizational documents used for the study included all of the organizations policy and procedure documents related to mobile device security, and information security. As noted by Frels and Onwuegbuzie (2013), the most predominant form of data collection in qualitative research comes from interviews. According to Rowley (2012), semistructured interviews encourage the interviewee to reflect on personal experiences, ideas and insights. The interviews coupled with the organizational documents assisted in the obtainment of enough rich data to answer the central research question of the study.

Member checking was used in this study to minimize participant response interpretation errors. According to Morse (2015), member checking is crucial for establishing the validity and the reliability in qualitative research studies. Each participant

of the study was provided with an opportunity to verify interpretation of the collected data during a follow-up interview session. This was an iterative process that continued until no new data was presented during the follow up member checking session. By utilizing member checking, the researcher eliminates the possibility of taking the interviewees' responses out of context (Stack, Sahni, Mallen, & Raza, 2013). The goal of the member checking session was to give each participant an opportunity to either confirm or deny the interpretation of the data. As noted by Kipulei (2013) the dependability of any research study is a measure of the consistency of the research approach.

Data Collection Technique

Interview data for this study were collected utilizing an interview protocol (see Appendix A). Lewis (2015), characterized the interview protocol as a type of subjective information gathering by which the researcher coordinates the interview and records data given by the interviewee. I conducted all of the semistructured interviews in an approved location by the participant. Hunter (2012) posited that interview protocols, guide the researcher in the creation of procedures and methods for conducting interviews. The data collection approach for this study allowed the participants the freedom of expression to convey their own personal views on the matter while providing reliable and comparative qualitative data. Interviews for this study utilized open-ended interview questions. According to O'Cathain et al. (2014) interviews are the recommended approach when dealing with professionals.

According to Yin (2013), case study research often includes the review of documentation by the researcher, as it is specific, inconspicuous and stable. Organizational documents from the target organization were reviewed to help augment the findings of the interview data and to add any new themes into the equation. The focuses of the documents reviewed for this study were related to strategies security managers use to prevent data breaches caused by mobile devices. Organizational documents were collected from the CISO of the organization. This documentation included all of the policies and procedures used by the organization related to mobile device security and information security.

To enhance the reliability and validity of the data collection instrument, member checking was used for this study. According to Houghton, Casey, Shaw, and Murphy (2013), member checking includes talking with members to gather information, deciphering and translating the interview data, and providing participants copies of the translated data to guarantee the exactness of information captured during the interview. A follow up member checking session was held with every participant of the study to provide him or her with an opportunity to verify my interpretation of the collected interview data. Furthermore, Morse (2015) posited that member checking is a crucial step in establishing the validity and reliability in a qualitative study. As noted by Andraski, Chandler, Powell, Humes, and Wakefield (2014), researchers use member checking as an opportunity to verify the researcher's interpretation of the collected interview data and to ensure the validity and reliability of the research. Ultimately, the member checking process helped to enhance the reliability and validity of the study.

As with any data collection technique there are advantages and disadvantages the researcher must consider. Listed below are a few of the advantages a researcher gains by conducting semistructured interviews with the participants of a study. One advantage to utilizing semistructured interviews in a research study is the ability to ask additional questions and it gives the participants of the study an opportunity to seek clarification (Doody & Noonan, 2013). During the interview process new data may be uncovered during the interview session, which may be beneficial to the research study. Another benefit of utilizing semistructured interviews as a type of data gathering technique are that they concentrate specifically on the case study topic and may provide perceived casual inferences (Verner, & Abdullah 2013). Ultimately, the semistructured interviews provided a platform to meet with the participants of the study to ask them specific questions about the research topic. And one final advantage a researcher gains by conducting semistructured interviews is the opportunity to observe nonverbal communication from the participants (Irvine, Drew, & Sainsbury, 2013).

However, with any type of data gathering there are disadvantages to using a semistructured interview. According to Baskarada (2014), researcher bias and the misrepresentation of data collected during the interview could potentially skew the results of the study, which is why it is very important to ensure no bias affects the process and that the participants are given a chance to verify the data has been represented accurately during a follow-up member checking session. Another possible disadvantage to using a semistructured interview is that it requires the interviewer to provide their full attention to ensure the data collected is accurate (Irvine et al., 2013). Again, misinterpretation of the

data can skew the study, which is why member checking was used to ensure the reliability and validity of the study. One final disadvantage to using semistructured interviews is that bias can be introduced into the study when the researcher attempts to lead the interviewees' responses (Tufford & Newman, 2012). To ensure this did not happen, the interview protocol was used with every participant of the study.

Data Organization Techniques

The organization of data in a case study requires the use of certain techniques due to the amount of information and evidence collected during the study. To ensure the validity and reliability of a study and to uncover patterns and themes a researcher uses research notes, research logs and interview transcriptions (Yin, 2013). Throughout this study a research log was utilized to facilitate the organization of the data and to contribute to the validity, reliability and conformability of the study. As noted by Wagstaff, Hanton, and Fletcher (2013), a researcher utilizes a research log to capture data to examine assumptions and actions thematic in a study. The log was used to keep track of research notes, observations from the interview, potential themes, as well as steps taken during the study, which were used during the data analysis. According to Georgiou, Marks, Braithwaite, and Westbrook (2013) the research log can also be used as an audit tool for conformability enabling the researcher to identify and reflect on challenges that could occur during the study. And finally, Green (2014) posits that research logs help the researcher minimize potential bias throughout a study. The research log helped to ensure no bias was introduced into the study, and it gave me a platform for reflection to capture not only the challenges that occurred during the study but also the positive outcomes.

Data collected from the interviews were transcribed using the Microsoft word application. The identification of citations and references for this study were done using the Mendeley citation manager, and finally the NVivo software tool application was used to store, file and organize the research data. To mask the identities of the participants of this study, each participant was assigned a unique alphanumeric code. Examples of participant codes used in the study: P1, P2, P3, etc.

All of the electronic data collected during the study will be stored on a password protected encrypted external hard drive for a period of five years from the date of publication. The physical hard drive will be stored in a locked cabinet in a home office along with any paper documentation collected or generated during the study, after which all of the contents stored on the hard drive along with any paper documentation will be permanently destroyed.

Data Analysis Technique

The following section of the study outlines the specific data analysis technique utilized for this research study. For this study, the chosen data analysis technique was thematic analysis. Thematic analysis encompasses the identification of, the analysis of, and the reporting of themes or patterns found in the collected data (Cruzes, Dyba, Runeson, & Host, 2014). Thematic analysis is frequently used in qualitative research to uncover the major themes.

Methodological triangulation was used to validate the findings of this single case study. To ensure the confirmability, reliability and credibility of a research study, researchers will use some form of triangulation (Houghton, Casey, Shaw, & Murphy,

2013). Data collected for this study were sourced from the semistructured interviews along with organizational documents provided by the CISO of the organization. By using multiple sources of data a researcher is able to triangulate the data more accurately (Onwuegbuzie, Leech, & Collins, 2012; Yin, 2013). All of the documentation was organized accordingly and uploaded into the NVivo software application tool for processing. As noted by Yilmaz (2013), researchers will use methodological triangulation to help validate the findings of a study. Methodological triangulation of the transcribed interview data coupled with the organizational documentation helped increased the overall validity of the study and helped uncover trends during the data analysis.

The analysis of the data focused on the uncovering of key concepts from the raw data. According to Vaismoradi, Turunen, and Bondas (2013), thematic analysis involves six stages: gaining a comprehensive understanding of the data, the generation of initial codes, uncovering themes within the data, becoming familiar with the themes, further refinement of the themes, and producing a final report.

The first stage of the data analysis encompassed gaining a comprehensive understanding of the collected research data. This included the reviewing of each interview transcript and each member checking transcript to gain a thorough understanding of the raw data. In addition, the organizational documents provided by the CISO were thoroughly reviewed during this phase to gain a comprehensive understanding of the policies and procedures used by the organization in relation to mobile device security and information security. During the review of these documents research notes were captured that were used later in the generation of initial codes. The

interpretation and the understanding of the collected data during this phase was key in the generation of the initial codes and the key themes. The next phase of the analysis breaks down the process I used in the coding of the data.

The second stage of the data analysis encompassed the generation of initial codes from the raw data. Coding was based on words and phrases related to mobile device security (e.g. encryption, BYOD, and mobile device management). Coding of the data to uncover themes was accomplished using the NVivo™ software application. The coding of the data immediately followed the interview and assisted in separating and distinguishing the participant responses. The NVivo™ software application is a program that allows researchers to code themes, which assist with the analysis of the data. According to Campbell et al. (2013), coding is a valuable tool used by researchers to uncover themes in the collected data. The NVivo™ software tool was used to identify recurring themes and associate them with the answers provided by the participant. Axial coding was also used during this stage of the analysis as recommended by Weidmann (2015), which involves the linking of the data, classification of the data, the establishment of major and minor categories, and uncovering any associations between the identified categories.

The third stage of the data analysis involves the uncovering of themes within the coded data. The coded data collected is organized into themes using the coding technique (Pierre & Jackson, 2014; Rosenfeld, Gatten & Scales, 2013). Software analysis tools such as NVivo™ aid the researcher with the analysis of the collected data (Woods et al., 2015). Combining of the codes into broader categories or themes while visually

displaying the occurrences of key themes was accomplished through the use of the NVivo™ software tool. As noted by Emmel (2015) the selection of themes during the data analysis phase is a fundamental task of the researcher. The researcher can use the following steps to help with the selection of themes (Emmel, 2015): focus on commonly used words by participants, narrow down the themes, develop a hierarchy of themes, and finally link the themes back to the conceptual framework and the research question. The process outlined by Emmel was used during this phase of the study to help with the generation of themes. In the next phase of the data analysis, the uncovered themes were analyzed further and compared to the literature review and the conceptual framework.

The fourth stage of the analysis encompasses the familiarization with the uncovered themes from the previous stage. Once the data had been analyzed using the NVivo™ software, themes were linked with the literature review and the conceptual framework. As noted by Yin (2013), the conceptual framework of a study is linked to the theories, literature and methodology of the study. Once initial themes had been uncovered through the use of the NVivo™ software tool, a comprehensive data analysis of the emergent themes was performed. An iterative analysis of the uncovered themes was done to uncover the major themes presented in section three of the study.

The fifth stage of the analysis involved the refinement of identified themes. According to Ganapathy (2016), once the coding process is complete, the next phase in the analysis is the process to uncover the major themes, which are essentially the aggregated codes. Key themes were uncovered during this stage of the analysis by reviewing the frequency of the theme and comparing the themes with the extant literature

review and the conceptual framework. To gain a clear understanding of which themes were repeated, the identified major themes were compared to each interview question. The extensive review of literature uncovered the following themes related to mobile devices and data breaches: security policies and procedures, security awareness, technology management tools and defense-in-depth.

The final stage of the analysis involves the generation of a report, which includes the major and minor themes, and how each theme ties back to the literature review and the conceptual framework of the study. The NVivo™ software tool was key during this phase of the analysis as key features such as the ability to create word clouds, tree maps and a cluster analysis helped in the generation of the final report. This presentation of findings will be explored further in section three of the study.

Reliability and Validity

The following section of the study breaks down how data validity and reliability was addressed in the study. The reliability and validity of this study was accomplished by ensuring data saturation occurred during the interview phase of the study by providing each participant of the study with copies of the transcribed interview data for member checking. According to Barry, Chaney, Piazza-Gardner, and Chavarria (2014), a study is considered to be reliable if the results are repeatable and the establishment of data validity refers to the accuracy of the data. The research logs and journals used during the study were crucial in ensuring a valid study. According to Georgiou, Marks, Braithwaite, and Westbrook (2013) the research log is used as an audit tool for conformability enabling the researcher to identify and reflect on challenges that may occur during the

study. The research log utilized during this study helped keep track of the challenges I faced throughout this study. Morse (2015) expressed when outlining, breaking down, and judging the quality of a study, qualitative researchers should seek to address validity and reliability. Qualitative researchers conceptualize the ideas of validity and reliability in research as meticulousness, trustworthiness, and quality (Titze, Schenck, Logoz, & Lehmkuhl, 2014).

Interviews and member checking were used until no new information was presented. According to Yin (2013), the reliability and validity of a case study can be ensured with proper documentation of the research approach and the steps taken by the researcher throughout the research process. Two very important areas of any research study are the reliability and the validity of the study. A research study is considered reliable when another researcher can repeat the study and obtain similar or the exact results (Cope, 2014; Singh, 2015). As noted by Yin (2013), a researcher should clarify any bias as early as possible so that readers of the study will be able to identify any bias or assumptions made by the researcher in the study. Researchers can also mitigate bias in a study by using multiple or different sources of data, investigators, data collection methods and theories (Podsakoff, MacKenzie, & Podsakoff, 2012). As noted by Kipkulei (2013), the instrument a researcher uses is valid if it measures what the researcher intends to measure. Internal and external are the two types of validity in research (Kipkulei, 2013; Seyal, 2015). Internal validity refers to the researcher's ability to form inferences (Laksmi & Mohideen, 2013). On the other end of the spectrum is external validity. External validity occurs when the findings of the study can be applied to larger

populations, settings or groups (Sikorskii & Noble, 2013). Credibility, transferability, confirmability and dependability were achieved through methodological triangulation and member checking.

Dependability

The dependability of this study is addressed in the following section. In qualitative research, reliability and internal validity are synonymous with credibility and dependability (Munn, Porritt, Lockwood, Aromataris, & Pearson, 2013). A dependable study is one in which other researchers can understand and follow the trail of decisions (Crowe, Inder, & Porter, 2015). According to Houghton et al. (2013) readers of a study may not agree with how the research was interpreted; however, the study is considered dependable if the reader is able to comprehend how the researcher was able to derive the findings of the study.

Dependability in this study was addressed through the use of member checking. One technique researchers use for establishing dependability in qualitative research is member checking of data interpretation (Welch, Grossaint, Reid, & Walker, 2014). Each participant of the study was given an opportunity to check the interpretation of the collected interview data. According to Houghton et al. (2013), member checking is used to ensure the interpretation of the collected data and the intent aligns. As noted by Beck (2014) the misrepresentation of data can affect the validity of a study; therefore member checking will be utilized in this study. Member checking was utilized in this study by asking each participant during a follow up interview session to verify my interpretations of their answers to ensure the collected data was an accurate representation. Any new

data presented during the follow up member checking session meant additional member checking sessions were conducted until no new information was presented.

Credibility

Member checking is one method of ensuring the credibility of a study. According to Cheng (2014), member checking not only enhances the credibility of a study but it also helps in the building of a trusting relationship between the interviewee and the interviewer. One method employed by researchers to ensure the credibility of their study is member checking. When used properly, member checking can increase the trustworthiness of the study while adding credibility to the study (Becher & Weiling, 2015). Member checking was utilized for this study by giving the participants a chance to correct any errors or misinterpretations of the data gathered during the interview process (Siddiqui, Ramesh, Manoharan, Hussein, Jawad, & Hussain, 2014). As noted by Power and Gendron (2015), the researcher is in constant dialog between the views of the participants of the study and the interpretations made by analyst. Member checking helped to ensure the data collected was an accurate representation of the participant's views.

In addition to using member checking for this study, methodological triangulation was also utilized. According to McNulty, Zlattoni, and Douglas (2013), triangulation is necessary to increase the validity and rigor of a study. Koc and Boz (2014) noted, the findings of a study obtained through triangulation would increase the validity and credibility of the study. Furthermore, triangulation may provide stronger evidence for the researcher, which will increase the credibility of the study (Koc & Boz, 2014).

Triangulated data for this study came from the interviews, procedure documents, organizational policies, and standard operating procedures used by the target organization.

Transferability

One important aspect of any study is transferability. Transferability is achieved when the findings of the study have meanings to individuals not involved in the study (Barnes, 2015). The transferability of a study is evident when the outcome of that study can be used within a different context or broader group (Rapport, Clement, Doel, & Hutchings, 2015). According to De Ceunynck, Kusumastuti, Hannes, Janssens, and Wets (2013), the responsibility of a researcher is to provide the readers of the study with detailed descriptions that will enable them to make an informed decision regarding whether the study's outcome is transferable to their specific contexts. Transferability in this study was accomplished by following all of the prescribed protocols for qualitative research, which included providing detailed information the readers of this study can use to determine the study's transferability.

Confirmability

The following section addresses confirmability in a research study. Confirmability can be demonstrated by way of describing how conclusions and interpretations have been established, and exemplifying that the findings were derived directly from the collected data (Cope, 2014). According to Erlingsson and Brysiewicz (2013), trustworthiness and confirmability can be accomplished by meticulously describing the methodologies of the steps in a study. Researcher may utilize respondents to judge the trustworthiness of a

study in an effort to confirm the validity of the conclusion. Andraski, Chandler, Powell, Humes, and Wakefield (2014) referred to this type of authenticity and validity as member checking. Each participant of the study was given an opportunity during a follow up member checking session to either confirm or augment the interpretation of his or her responses.

Data Saturation

Another important area of any qualitative research study involves whether or not the researcher achieved data saturation. Data saturation is achieved when the information being collected becomes repetitive or reveals no new data (Roy, Zvonkovic, Goldberg, Sharp, & La Rossa, 2015). As noted by Onwuegbuzie and Byers (2014), data saturation is present when there is sufficient data for the researcher to conduct a comprehensive and credible analysis of the research topic. Data saturation happens when there is redundancy in the data being collected during the interview process (Marshall, Cardon, Poddar, & Fontenot, 2013). Data saturation in this study was accomplished through the gathering of data from organizational documents and interviews, the verification of the interpretation of that data through the use of member checking, through the use of census sampling to ensure an appropriate sample population and finally through the use of methodological triangulation. As noted by Erlingsson and Brysiewicz (2013) member checking is used to reduce the number of errors before the analysis of the data occurs and to help achieve validity in the study. Data saturation, validity and the reliability in a study can be achieved through the use of member checking (Andraski et al., 2014). When the researcher incorporates member checking into the study, data saturation occurs when no

new information is during the data collection phase of the study (Unluer, 2012). Follow up interviews were held with every participant of the study to provide him or her with an opportunity to clarify the interpretation of the collected data as outlined in the interview protocol (see Appendix A).

Transition and Summary

In section 2 of this study, the main purpose of the study, the target participants, population and sampling, and the methods and processes that were used to collect and analyze the research data have all been explored. The purposes of this qualitative single case study was to explore the strategies security managers use to prevent data breaches caused by mobile devices. Methodological triangulation was utilized to ensure the credibility of this qualitative study. Section 3 of the study encompasses the presentation of findings, implications for social change, a discussion regarding the applicability to professional practice, recommendations for action and further research, reflections, and the conclusion of the study.

Section 3: Application to Professional Practice and Implications for Change

This section of the study includes an overview of the study and a presentation of the major themes uncovered during the data analysis phase. This section also includes potential implications for social change, recommendations for action, areas of interest for future research, personal reflections, and a study conclusion.

Overview of Study

The purpose of this qualitative single case study was to explore the strategies utilized by security managers use to secure mobile devices to prevent a data breach. The data for this study came from two main areas: the semistructured interviews and the organizational documents related to mobile device security used by the target organization. I conducted semistructured interviews with five security managers working for a government contractor located in the southeastern region of the United States. In addition, I collected and analyzed 13 organizational documents during the data analysis phase of the study. All of the participants of the study had experience with the implementation of strategies to prevent data breaches caused by mobile devices, and every participant had no less than ten years of experience as a security manager.

Four major themes emerged during the data analysis phase of this qualitative single case study: (a) security policies and procedures, (b) security awareness, (c) technology management tools, and (d) defense-in-depth. The findings from this study are comparable to the findings uncovered in the literature review. Additionally, the findings from this study support the use of von Bertalanffy's general systems theory as the

conceptual framework. In the following section, the four key themes uncovered during the data analysis phase will be explored and synthesized for the reader.

Presentation of the Findings

The central research question used to drive this study was: What strategies do security managers use to prevent data breaches caused by mobile devices?

This section of the study breaks down the four major themes uncovered during data analysis phase of the study. I used methodological triangulation to analyze the data collected from the semistructured interviews and the organizational documents related to mobile device security used by the target organization. The interview transcripts, member checking transcripts, and organizational documents were all uploaded into the NVivo software tool where the analysis of the data produced four major themes: (a) information security policies and procedures, (b) security awareness, (c) technology management tools and (d) defense-in-depth. As noted by Edwards-Jone (2014), software tools such as NVivo allow the researcher to visually analyze and code the data into themes. The development of themes during the data analysis phase tied back to the literature review and the conceptual framework.

In the following section, the four major themes that emerged during the data analysis phase are compared to the extant review of literature and tied back to von Bertalanffy's general systems theory, which served as the conceptual framework for this study.

Theme 1: Information Security Policies and Procedures

The theme information security policies and procedures was the first prominent theme to emerge during the data analysis phase of the study. An integral part of an organizations business and IT strategy is the protection of its information assets (Knapp & Ferrante, 2012). Every IT department must ensure its information security policies and procedures are in alignment with the organization. Furthermore, these security policies should cover every asset that touches organizational data.

The second of half of the information security equation encompasses procedures. This includes both proactive and reactive procedures. The next section of the study discusses the findings and how the data supports the theme. Table 2 below highlights the number of references related to the theme information security policies and procedures.

Table 2

References to Information Security Policies and Procedures

Major Theme	Participant		Document	
	Count	References	Count	References
Information Security Policies and Procedures	5	38	8	56

Information security policies and procedures form the backbone of the organization's approach to information security according to participant P1. Participant P4 highlighted the below security policies and procedural documents the organization currently has in place:

- Information security policy
- BYOD security policy

- AUP policy
- End user IT asset management standard
- Communications security standard
- Access control standard
- Encryption standard

Participant P5 stated, “our goal is first to ensure a security breach doesn’t occur, but if one does, our security team will be prepared for it”. The key with any effective IT organization is to be prepared for the worst. Participant P3 stated most security managers do not look at the overall footprint of the business when creating effective security policies and procedures, which could lead to lapses in data security. As technology continues to evolve so must organizations and this starts with effective information security policies and procedures according to participant P1. With the introduction of mobile devices into the security equation, security managers must account for these devices in their overall information security model. According to Participant P2, the organization distributes a monthly information security newsletter to all employees that outlines recent security threats and encourages employees to review the current organizational policies related to information security. This type of communication keeps information security at the forefront of the organization and its employees by reminding them they must stay vigilant and adhere to all of the outlined security policies and procedures currently in use by the organization.

All of the participants of the study agreed that the success of any organization depends on information security. Furthermore, four of the five participants stated lapses

in data security are the result of security policies and procedures that are not in alignment with the objectives of the business. Data collected from the semistructured interviews and the organizational documents support the theme of information security policies and procedures as one of the key strategies a security manager should utilize to prevent a data breach caused by a mobile device.

The findings of this study demonstrate how information security policies and procedures are in alignment with existing literature. According to Allassani (2014), the protection of an organizations IT assets starts with the implementation of comprehensive information security policies and procedures. As noted by the participants of the study, these documents form the foundation of information security and they must address the entire footprint of the organization. According to the authors of a recent article, current information security models being utilized by most organizations fail to properly manage the policies, risks, people and assets effectively (de Oliveira Albuquerque, García Villalba, Sandoval Orozco, Buiati, & Tai-Hoon, 2014). As noted by participant P3, a data breach typically occurs because the organization failed to properly manage its assets effectively. Although mobile devices offer organizations increased productivity, these devices also bring with them increased security risks for the user and ultimately the organization. Organizations can reduce expenses related to data breaches through the communication, and enforcement of its information security policies (Knapp & Ferrante, 2012). The extant literature that I reviewed for this study is in alignment with the findings of the study by highlighting the importance of information security.

Recent literature further supports the theme information security policies and procedures as a strategy security managers can use to prevent data breaches caused by mobile devices. According to Di Modica, and Tomarchio (2016), security managers should ensure the security policies and procedures in use are compliant with well-established security specifications. According to participant P4, every year our department reviews our current security policies and procedures to determine if changes need to be made. As noted by Bauer, Bernroider, and Chudzikowski (2017) the organization must ensure their information security policies and procedures are up to date but also that the employees of the organization are in compliance and actively following them. Furthermore, effective security policies and procedures encompass not only the prevention of security breaches but also how the organization responds to a security breach. In today's technology landscape, every organization should accept the fact they may be the target of a data breach; however if their information security policies and procedures are up to date they will be prepared to respond accordingly.

When viewed through the lens of general systems theory, an organization with effective information security policies and procedures will contribute to the overall success of the organization. According to Coole and Brooks (2014) when security components do not function as a system, a breakdown in the security defenses occurs. Participant P4 noted, a successful security model ensures a breach will not occur and this is only possible if all of the elements of the model are functioning as designed. General systems theory drove this study by showing how the information security strategies presented in this study will help to bring about the accomplishment of the objectives of

the organization. As noted by von Bertalanffy et al. (2008), organizations are intricate systems composed of various components such as functions, activities and business units. The collaboration of business parts must function appropriately to bring about the accomplishment of the organizational objectives and according to all of the participants of the study; information security is a critical component of any organization. The majority of the participants indicated information security policies and procedures that are not aligned with the business could create lapses in information security, which could lead to a data breach. The findings of this study show that through proper alignment with the objectives of the business and utilizing a systems theory approach to information security, the security managers of the organization can ensure the organizations data remains safe and secure from both internal and external threats.

Theme 2: Security Awareness

The second major theme to emerge during the data analysis phase was the concept of security awareness. Security awareness is the first line of defense for any organization. At its core, security awareness is the attitude and knowledge an employee of the organization has about information security. Every organization should consider security awareness an essential element of its information security model. By using security awareness learning tactics, an organization can minimize the possibility of a data breach due to mobile devices. Table 3 below highlights the number of references related to the theme security awareness.

Table 3

References to Security Awareness

Major Theme	Participant		Document	
	Count	References	Count	References
Security Awareness	5	33	7	51

Participant P5 stated, security awareness is at the forefront of the organization and is emphasized from the moment a new employee gets hired by the organization. Two effective methods for creating security awareness within the organization include education and training as these highlight the responsibilities every employee must assume to ensure the protection of the organizations IT assets (Mishra et al., 2014). All of the participants of the study echoed Mishra et al., stating the majority of security lapses within an organization occur due to a lack security awareness by the organization and its employees. According to Participant P4, government policies and regulations related to information security has assisted the security managers within the organization in championing a security culture that ensures the organization's confidential data is secure. Furthermore, according to Participant P1, the organization requires every employee to complete annual security trainings. Participants revealed their perception of information security changed shortly after the organization started mandating yearly security awareness training sessions. Every employee must also acknowledge he or she has read the latest information security policy by digitally signing an electronic document sent out quarterly by the human resources department. The responses to the interview questions by the participants were in alignment with Mishra et al.'s (2014) statement that a positive mindset toward information security is possible through proper education and training.

The literature supports the theme of security awareness as a key strategy in the prevention of data breaches caused by mobile devices. The findings of the following studies align with the participants' responses to the interview questions. According to Mishra, Caputo, Leone, Kohun, and Draus (2014), implementing an effective and comprehensive security program begins with creating awareness around information security. According to participant P4, every organization should look at this as one of its fundamental objectives as this ensures information security is at the forefront of every employee that works for the organization. At the heart of information security awareness is the reduction of the risks the organization faces, which is accomplished by focusing on the user and not the device. In essence, the goal of information security awareness is to create a culture of security within the organization.

As noted by Tsohoua, Karydab, and Kokolakis (2015), the focus of most security awareness programs is on the content and processes as opposed to how the employees of the organization make decisions around security. Therefore, one key goal for security managers is to create not only awareness but to also encourage outside the box thinking the employees can use. According to Kim (2014), after attending a security awareness seminar at a local college, the attitude of the students toward information security changed significantly. The findings related to security awareness align with the literature by showing that through the act of providing the employees of the organization some form of security training, the organization can have an impact on that employee's mindset related to information security. In the end, a security managers' main goal is to drive the

pulse of the organization through the creation of an information security culture, which is at the heart of information security awareness.

More recent literature further supports the theme of security awareness in relation to the prevention of data breaches caused by mobile devices. As noted by Bitton, Finkelstein, Sidi, Puzis, Rokach, and Shabtai (2017), when compared to the PC domain, security awareness among users is relatively high and significantly higher than the mobile platform. These devices are attractive to attackers because they hold valuable information an organization cannot afford to have leaked. Therefore, security managers must ensure some form of security awareness training is available to all of the employees of the organization.

One method of increasing security awareness in the organization is to create a culture of security. As noted by Rocha Flores and Ekstedt (2016), information security culture is defined as “An employee's individual perception of shared beliefs and values among colleagues in the work environment” (p. 31). As noted by participant P1, the security culture within our organization is strong and effective because we actively encourage it because we know first-hand how effective it is in the prevention of data breaches. A successful security culture starts with the employees of the organization (Gerhold, Bartl, & Haake, 2017). It is hard to change individual behavior, but if you push an organizational culture, employees will influence each other.

The theme security awareness is in alignment with general systems theory, which served as the conceptual framework for this study. One of the key tenets of general systems theory is the concept of holism. As noted by von Bertalanffy (1968), a holistic

approach should be used when designing any complex system. As noted earlier, at the heart of information security and one of the central components of an information security model is security awareness. According to participant P2, we are not just thinking of our internal network when we design security awareness initiatives, we look at the entire technology landscape of the organization, especially mobile devices, as these devices typically operate outside of the corporate network. To this end, security managers must focus on all of the components of the organization when designing security awareness initiatives.

One of the components of a successful organization, according to Chandrashekhar, Gupta, and Shivaraj (2015), is information security awareness. When viewed through the lens of general systems theory, an organization with an effective security awareness program will contribute to the overall success of the organization.

Based on the findings of this study, a successful security awareness program will take into consideration all of the components of the system and will be in alignment with the needs of the organization. To accomplish this, security managers must take a holistic approach to information security, which serves as one of the key tenets of general systems theory.

Theme 3: Technology Management Tools

The third major theme uncovered during the data analysis phase of the study revolved around the concept of technology management tools. Technology management tools as a theme centers on how organizations must utilize every tool at its disposal to ensure the security of the organization's assets. The ever-changing technology

landscape means organizations must take a proactive stance to security by staying up-to-date with the latest trends, vulnerabilities and threats. The introduction of mobile devices into the equation calls for the use of tools the organization can use to manage these devices. To this end, technology management tools when used properly can assist in the prevention of data breaches caused by mobile devices. Table 4 below highlights the number of references related to the theme technology management tools.

Table 4

References to Technology Management Tools

Major Theme	Participant		Document	
	Count	References	Count	References
Technology Management Tools	5	29	7	46

All of the participants noted, the organization uses several technology management tools to ensure the protection of the organizations IT assets. Some of the technology management tools specifically used by the target organization to manage the mobile devices are discussed here further. According to four of the five participants interviewed, the organization uses a third party mobile device management or MDM tool to help ensure the organization's data remains safe and secure from both internal and external threats. Participant P1 noted the MDM software the organization utilizes is a valuable tool that allows us to not only monitor the phone but it also gives us the capability of a bricking a phone remotely. The MDM tool in use by the organization is just one of the technology management tools they use to manage the mobile devices in use by the employees of the organization. According to Participant P3, the organization also utilizes Microsoft Exchange ActiveSync to help with the management of the mobile

devices. This tool according to Participant P3 lets you synchronize users exchange email account with their mobile device. In addition, Exchange ActiveSync includes the following security features:

- secure socket layer encryption between the mobile device and the exchange server
- enhanced mobile device security through password policy
- the ability to remote wipe a lost or stolen device
- the ability to control which types of mobile devices with your organization's exchange server

All of the participants of the study agreed, the key with ensuring security for these types of mobile devices is accomplished through the use of current and up to date technology management tools outlined above. In addition to the data collected from the semistructured interviews, and the organizational documents reviewed during the data analysis phase of the study all support the theme of technology management tools. Seven of the organizational documents reviewed highlight specific tools used by the organization for information security specifically related to mobile devices. The data collected for this study all support the theme of technology management tools.

The next section of the study ties the theme technology management tools back to the extant literature reviewed for this study as well as recently published studies. As Chol-Un, Dok-Jun, and Song (2013) point out, with the massive use of mobile devices for personal and confidential data by users, a method of managing these devices is a necessity for organizations. One strategy security managers have started implementing to

help with the administration of mobile devices in the organization is the use of some form of MDM software. As Rhee, Won, Jang, Chae, and Park (2013), points out, an MDM system is used to manage smartphones, and other mobile devices remotely by monitoring their status and controlling their functions. According to Yang, Lee, Park, and Eom (2015), to keep up with the latest threats and vulnerabilities, organizations must be proactive when it comes to security to keep up with the constant changes in the technology landscape. To do this, security managers must ensure all of the technology management tools currently in use stay up to date with the latest patches and security fixes and that they are in alignment with the business needs of the organization. MDM allows the organization to manage, monitor and secure the mobile devices used by its employees (Leavitt, 2013). As noted by participant P5, our MDM software allows us the capability to remotely monitor all of our mobile devices as well as the ability to brick a phone if necessary. To this end, security managers must come to the understanding that the organizations data no longer resides behind a corporate firewall, which is why an MDM system is such an invaluable tool for the security manager.

More recent literature further supports the theme of technology management tools as a strategy security managers can utilize to prevent data breaches caused by mobile devices. A recent study by Luke, Christian, and Gordon (2016) further solidifies the need for organizations to use some form of MDM software to ensure the organizations data remains safe and secure from both internal and external threats. Any organization currently allowing its employees to use mobile devices for both work and personal needs must come to the conclusion that these devices bring with them added vulnerabilities.

However, with proper management tools such as MDM software, the data on these devices can be secured. The analysis of seven organizational documents during the data analysis phase allowed for methodological triangulation and confirmed the importance of this theme. In the end, the findings of this study align with recent research, which encourages the use of up to date technology management tools by the security team to keep up with the ever-changing technology landscape.

The next section of the study ties the findings to the conceptual framework, general systems theory. According to Montgomery and Oladapo (2014), a general systems theory approach allows for an integrated approach or the examination of relationships between two or more systems. In today's complex organization, the IT department is responsible for multiple systems utilized by the organization that may interact with external third party systems. As noted by participant P3, the days of living behind a corporate firewall are in the past. According to Laszlo and Krippner (1998), a business when viewed through the lens of systems theory can be seen as a network of interconnected parts, each having a specific purpose and task. The strategies used by security managers to prevent data breaches caused by mobile devices in this equation can be seen as one of the many interconnected parts that make up an organization or system. In essence, security managers must look at the organization as a system containing several subsystems all working together to achieve one common goal. At its core, this goal is the protection of the organizations IT assets. All of the participants interviewed actively push for a holistic approach when making or designing any new system. Security managers who utilize a systems theory approach to security are able use a holistic

approach and account for all of the interconnected parts that make up a typical organization.

Theme 4: Defense-in-Depth

The fourth and final theme to emerge during the data analysis phase of the study related to the concept of defense-in-depth or DiD. The premise behind the theme DiD is that it encourages 360-degree security and incorporates all of the organizations IT assets including mobile devices, which often connect to unsecured networks outside the organization. As noted by German (2016), a DiD approach combines multiple layers of prevention and detection technologies and is essential in the prevention of information security data breaches. The findings of this study coupled with that of existing literature support this theme and show how a DiD approach to information security is a key strategy in the prevention of data breaches caused by mobile devices. Table 5 below highlights the number of references related to the theme defense-in-depth.

Table 5

References to Defense-in-Depth

Major Theme	Participant		Document	
	Count	References	Count	References
Defense-in-Depth	5	41	8	43

The participant responses to the semistructured interview questions echoed Germans (2016) conclusion. All of the participants of the study highlighted their approach to security for the organization utilized a DiD approach. According to Participant P3, our DiD strategy encompasses multiple layers and involves several members of the security team. The goal here, according to Participant P1 is to ensure we

have every component of the organization covered in case of an attack and that we have a plan in place if an attack occurs. Four of the five participants stated although the organization has never actually suffered a data breach, there have been a few close calls, however because of our DiD strategy the threat was contained quickly and efficiently. Eight of the organizational documents analyzed for this study make reference too or specifically address how a DiD approach should be used to protect the organizations assets from both internal and external threats. According to participant P5 the organization reviews these documents on an annual basis to ensure they are in alignment with the needs of the business and are addressing all elements of the infrastructure utilizing a DiD approach. The findings of this study, which included the collection of data from multiple sources all, support the theme of defense-in-depth as one of the key strategies a security manager can utilize to prevent a data breach caused by a mobile device.

The next section of the study ties the theme to the extant literature reviewed for this study as well as to recent literature. According to Ahmad, Maynard, and Park (2014), information security systems should be designed using a layering approach where overlapping security measures are deployed so that if one layer is breached the next one takes over. With the proliferation of mobile devices, the organization must now account for and manage not only its internal network but also the mobile devices its employees use while connected to external networks. As noted by participant P4, organizations that do not utilize a DiD approach are just asking for a security breach. A recent paper which focuses on cybersecurity for distributed electric power systems calls for a layered defense

framework consisting of cyber systems designed to protect against malicious intrusions (Li, Shahidehpour, & Aminifar, 2017). Recent literature aligns with the findings of the study and supports the DiD theme, which pushes for a layered approach to security or a DiD approach, which accounts for all of the components of the organization. As noted by Sampemane (2015), with the continued use of mobile devices within organizations the security managers must implement internal access controls when designing the system to limit the exposure of a hack to a single system and not the entire network. This is accomplished by using a DiD approach to information security or looking at the system as a whole and breaking it down into smaller components or subsystems. All of the participants of the study agreed with Sampemane. According to Mansfield-Devine (2016), the key to using a DiD approach is to view the organization as an ecosystem of technologies and to integrate them all together which will drive how the organization approaches security. The findings of these studies encourage the use of a DiD approach to security, which is in alignment with the participants' responses to the interview questions and the organizational documents reviewed.

General systems theory which served as the conceptual framework for this study aligns with the findings of this theme of utilizing a DiD approach to help with the prevention of data breaches caused by mobile devices. Organizations that utilize a DiD approach to security are following one of the key tenets of systems theory, which states a system is made up of many interconnected parts. To ensure the overall security of the organization's data, security managers must focus on all of the components of the organization. According to participant P2, as a security manager, you have to address the

threats and vulnerabilities of every IT asset the organization utilizes. As noted by von Bertalanffy (1968), a complex system when designed using a holistic approach will be more effective when compared to one that does not use a holistic approach. In essence, security managers must look at the organization as a system containing several subsystems all working together to achieve one common goal. Furthermore, a system should be viewed as a grouping of elements that are organized in a particular way (Mangal, 2013). As the key theme behind DiD focuses on the layering of defenses, systems thinking can be applied to ensure the strategy is organized to not only meet the needs of the business but also the protection of the organization's information assets from both internal and external threats.

All of the identified themes align with current research and highlight the fact that effective IT organizations utilize strategies that are in alignment with the business objectives of the organization while protecting the organization's data from malicious threats. The strategies outlined in this study are in alignment with existing literature and can be tied back to general systems theory, which served as the conceptual framework for this study. Using a systems theory approach, security managers may implement the recommended actions below combined with the strategies uncovered in the literature review section of the study to prevent data breaches caused by mobile devices.

Applications to Professional Practice

The specific IT problem I sought to address in this study was the perceived lack of strategies used by security managers to prevent data breaches caused by mobile devices. Other security managers around the world to help enhance and maximize their

strategies used to prevent data breaches caused by mobile devices could utilize the strategies uncovered in this study. The majority of the participants interviewed for this study noted their participation in this study has contributed to the enhancement of their existing strategies which they plan to share with other security managers in the IT industry.

The findings of this study may contribute to the reduction in the number of data breaches caused by mobile devices, which would decrease the costs an organization would incur from responding to a data breach. According to the 12th annual cost of a data breach study which is sponsored by IBM, the average cost of a data breach is roughly \$3.62 million or \$141 for each lost or stolen record containing sensitive or confidential information (IBM & Ponemon Institute, 2017). In addition to the costs associated with data breaches, organizations could also face a decrease in revenue due to the fallout from the data breach. In the end, the findings of this study may benefit security managers around the world by providing them with a few key strategies uncovered in this study, which could be used to form the blueprint for their new and improved security approach.

Implications for Social Change

The findings of this study indicate that there can be improvements to the strategies used by security managers to prevent data breaches caused by mobile devices, which can lead to a decrease in the overall number of data breaches affecting organizations around the world. As indicated by Jewkes and Yar (2011), digital privacy protection has turned into a force for creativity and social change as innovation drives community engagement and cultivates corporate advancements. Through the

implementation of strategies to prevent data breaches caused by mobile devices, the organization will protect consumers against the high costs of identity theft associated with these types of data breaches. Furthermore, data breaches can have a negative impact on the organizations stock prices, which may affect the value of employee stock options, retirement plans, as well as pension plans (Hinz, Nofer, Schiereck, & Trillig, 2015). In the end, consumers as well as employees of the organization will benefit knowing organizations are taking steps to protect their data from unauthorized access while still providing them with exceptional service through the use of mobile devices by the organization.

Recommendations for Action

The findings of this study could benefit security managers around the world by providing them with some strategies they could implement related to mobile device security. The first recommendation calls for security managers to conduct a strategic planning session with their security team that looks at their existing policies and procedures in place to prevent data breaches caused by mobile devices and determines if they align with the ones presented in this study. Also, security managers should also reach out to other security managers working in other industries, which could prove to be beneficial to both organizations. Furthermore, any organization currently operating with no existing strategies should review this study and determine if the ones uncovered in this study could work for their organization.

The second recommendation is for security managers to take an in-depth look at how they are currently creating security awareness within the organization. As this study

has shown, one of the key strategies security managers use to prevent data breaches caused by mobile devices is through security awareness. Every security manager should look at how their organization achieves security awareness within the organization, as this will help them uncover any areas of improvement.

The third recommendation calls for security managers to do a comprehensive review of the technology management tools they currently utilize for mobile devices. This review will assist them in determining if the current tools in place are effective or if additional tools or modifications need to be made to ensure the organization is keeping up with technology. Four of the five participants interviewed stated that every security manager should do an annual audit of the technology management tools currently in use within the organization. This audit allows them the opportunity to look at new and improved tools and determine end of life for older technology tools no longer needed.

The fourth and final recommendation calls for security managers to have a third party security firm do an audit of their current information security program to determine if they are utilizing a defense-in-depth approach. This audit will give them concrete evidence of how they currently have security setup to determine if they are addressing all of the interconnected parts of the organization using a layered approach. By following these four recommendations, security managers will feel confident their information security approach is addressing all of the components of the organization.

Dissemination of the findings of this study will be accomplished using multiple approaches. Once I have received CAO approval, every participant of the target organization will be provided with a two-page summary of my findings. The study will

also be available in the ProQuest database, which has active partnerships with more than 700 Universities around the world. Furthermore, I plan on pursuing publication of my research in other scholarly journals, industry publications, and conferences, which will expand the target audience to IT professionals outside of the University community.

Recommendations for Further Study

This study has uncovered some of the strategies used by security managers to prevent data breaches caused by mobile devices. However, further research around this study topic could be beneficial for every organization that utilizes some form of mobile device for day-to-day operations. The main limitation of this study was the focus on strategies used by security managers working for a government contractor located in the southeastern region of the United States. Recommendations for further research include similar studies using other industries in different regions of the United States. Also, I would also recommend a multiple case study, which looks at multiple organizations to determine if they have similar approaches to this IT problem.

Additional research conducted using a different design or method may also be beneficial. For example, a quantitative study may examine the relationship between the use of personal mobile devices and the support the organization must provide to ensure security. This type of study would be able to determine the relationship between BYOD and the support of the organization. In the end, this study has contributed to the literature but additional research involving mobile device use within organizations may prove to be beneficial to the IT industry.

Reflections

This research study was one of the hardest academic endeavors I have ever undertaken. In the end, this study has changed my perception of how academic research is accomplished and increased my overall respect and admiration for anyone attempting to or has obtained the title of researcher. Throughout this study I focused all of my attention on ensuring this would be a credible study by utilizing techniques to mitigate personal biases from controlling the direction of the study. As the main instrument for not only collecting the data but also reviewing it, I considered my individual bias throughout the study. To further ensure a credible study, I strictly followed the interview protocol with every participant of the study and provided every participant of the study an opportunity to verify the accuracy of my interpretations during a follow-up member checking session. Furthermore, the organizational documents were triangulated with the interview and member checking transcripts.

Several positive outcomes came from this study. The first relates to how the participants in this study were eager to share their experience and knowledge of the types of strategies they currently use to prevent data breaches caused by mobile devices. The second one relates to both my excitement to have finally finished this study and my need to explore more. In the end, this study has opened my eyes up to the possibility of additional research studies I would like to undertake in the near future.

Summary and Study Conclusions

The objective of this qualitative single case study was to explore the strategies security managers to prevent data breaches caused by mobile devices. The organization

selected for this study was a government contractor located in the southeastern region of the United States. Methodological triangulation of the interview transcripts, member checking transcripts, and the organizational documents helped to answer the central research question of the study. During the data analysis phase of this study, three key themes related to the strategies used by security managers to prevent data breaches caused by mobile devices emerged. These three prominent themes (a) policies and procedures, (b) security awareness training and (c) technology, indicate a need for security managers to champion strategies related to the prevention of data breaches caused by mobile devices. As Densham (2015) points out, every organization must come to the realization and expect a data breach to happen. By doing this, the organization is prepared for the worst and has planned for the attack and the aftermath of the breach.

References

- Adderley, S., & Mellor, D. (2014). Who's influencing whom? Developing sustainable business partnerships. *EuroMed Journal of Business*, 9(1), 60-74.
doi:10.1108/EMJB-06-2013-0033
- Ahmad, A., Maynard, S., & Park, S. (2014). Information security strategies: towards an organizational multi-strategy perspective. *Journal Of Intelligent Manufacturing*, 25(2), 357-370. doi:10.1007/s10845-012-0683-0
- Alebrahim, A., Hatebur, D., Fassbender, S., Goeke, L., & Côté, I. (2015). A pattern-based and tool-supported risk analysis method compliant to ISO 27001 for cloud systems. *International Journal of Secure Software Engineering*, 6(1), 24-46.
doi:10.4018/ijssse.2015010102
- Allassani, W. (2014). Determining factors determinants of bank employees' reading habits of information security policies. *Journal of Information Systems and Technology Management*, 11, 533-548. doi:10.4301/S1807-17752014000300002
- Andraski, M. P., Chandler, C., Powell, B., Humes, D., & Wakefield, S. (2014). Bridging the divide: HIV prevention research and black men who have sex with men. *American Journal of Public Health*, 104, 708-714. Retrieved from <http://ajph.aphapublications.org/>
- Andretta, M. (2014). Some considerations on the definition of risk based on concepts of systems theory and probability. *Risk Analysis*, 34(7), 1184-1195.
doi:10.1111/risa.12092

- Anton, N., & Nedelcu, A. (2015). The Systemic Approach to Information Protection in Relation to Risk in an Integrated Information Security System. *Applied Mechanics & Materials*, 760689. doi:10.4028/www.scientific.net/AMM.760.689
- Anyan, F. (2013). The influence of power shifts in data collection and analysis stages: A focus on qualitative research interview. *Qualitative Report*, 18, 130-136.
Retrieved from <http://www.nova.edu/ssss/QR/index.html>
- Barnes, J. (2015). Qualitative research from start to finish (2nd edn.). *Neuropsychological Rehabilitation*, 1–3. doi:10.1080/09602011.2015.1126911
- Barr, H. (2013). Toward a theoretical framework for inter professional education. *Journal of Interprofessional Care*, 27(1), 4-9. doi:10.3109/13561820.2012.698328
- Barrett, J. R. (2007). The researcher as instrument: learning to conduct qualitative research through analyzing and interpreting a choral rehearsal. *Music Education Research*, 9, 417-433. doi:10.1080/14613800701587795
- Basem, B., Ghalwash, A., Z., & Sadek, R., A. (2015). Multilayer secured SIP based VoIP architecture. *International Journal of Computer Theory and Engineering*, 7, 453-462. doi:10.7763/IJCTE.2015.V7.1002
- Baskarada, S. (2014). Qualitative case study guidelines. *Qualitative Report*, 19(40), 1-25.
- Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, 68145-159. doi:10.1016/j.cose.2017.04.009

- Becher, E. H., & Wieling, E. (2015). The intersections of culture and power in clinician and interpreter relationships: *A Qualitative Study*, 21, 450-457.
doi:10.1037/a0037535
- Beck, C. D. (2014). Antecedents of servant leadership: A mixed methods review. *Journal of Leadership & Organizational Studies*, 21, 299-314.
doi:10.1177/1548051814529993
- Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, 48, 51-61.
doi:10.1016/j.chb.2015.01.039
- Benoot, C., Hannes, K., & Bilsen, J. (2016). The use of purposeful sampling in a qualitative evidence synthesis: A worked example on sexual adjustment to a cancer trajectory. *BMC Medical Research Methodology*, 1621.
doi:10.1186/s12874-016-0114-6
- Benton, D. C., González-Jurado, M. A., Benoit-Montesinos, J. V., & Fernández P. (2013). Use of Open Systems Theory to Describe Regulatory Trends. *Journal Of Nursing Regulation*, 4(3), 49-568p
- Bernard, R. H. (2013). *Social research methods: Qualitative and quantitative approaches (2nd ed.)*. Thousand Oaks, CA: Sage
- Bernard, T. J., Paoline, E. I., & Pare, P. (2005). General systems theory and criminal justice. *Journal Of Criminal Justice*, 33(3), 203-211.
doi:10.1016/j.jcrimjus.2005.02.001

- Bhattacharya, P., Yang, L., Guo, M., Qian, K., & Yang, M. (2014). Learning Mobile Security with Labware. *IEEE Security & Privacy Magazine*, 12(1), 69.
doi:10.1109/MSP.2014.6
- Bitton, R., Finkelstein, A., Sidi, L., Puzis, R., Rokach, L., & Shabtai, A. (2017). Taxonomy of mobile users' security awareness. *Computers & Security*,
doi:10.1016/j.cose.2017.10.015
- Boin, A., & van Eeten, M. G. (2013). The resilient organization. *Public Management Review*, 15, 429-445. doi:10.1080/14719037.2013.769856
- Cacari-Stone, L., Wallerstein, N. G., & Minkler, M. (2014). The promise of community-based participatory research for health equity: A conceptual model for bridging evidence with policy. *American Journal of Public Health*, 104, 1615-1623.
doi:10.2105/AJPH.2014.301961
- Chai, S., Kim, M., & Rao, R. H. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems*, 50, 651-661. doi:10.1016/j.dss.2010.08.017
- Chandrashekhar, A. M., Gupta, R. K., & Shivaraj, H. P. (2015). Role of information security awareness in success of an organization. *International Journal of Research*, 2(6), 15-22. Retrieved from <http://internationaljournalofresearch.org/>
- Chang, J. M., Ho, P., & Chang, T. (2014). Securing BYOD. *IT Professional*, 16(5), 9-11.
doi:10.1109/MITP.2014.76

- Chassin, M., & Loeb, J. M. (2013). High-reliability health care: Getting there from here. *Milbank Quarterly*, 91, 459-490. doi:10.1111/1468-0009.12023
- Cheng, F. (2014) Using focus groups with outsider and insider approaches: Preparation, process, and reflections. SAGE Research Methods Cases. London, United Kingdom: SAGE Publications, Ltd. doi: 10.4135/978144627305014528633
- Chicone, R. G. (2010). *An exploration of security implementations for mobile wireless software applications within organizations* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database. (UMI No. 3394802).
- Chiumento, A., Khan, M. N., Rahman, A., & Frith, L. (2015). Managing ethical challenges to mental health research in post conflict settings. *Developing World Bioethics*. doi:10.1111/dewb.12076
- Chol-Un, K., Dok-Jun, A., & Song, H. (2013). A Security Protocol for the Identification and Data Encrypt-Key Management of Secure Mobile Devices. *Journal Of Theoretical Physics And Cryptography*, (1), 21.
- Cleary, M., Horsfall, J., & Hayter, M. (2014). Data collection and sampling in qualitative research: does size matter? *Journal of Advanced Nursing*, 70, 473- 475. doi:10.1111/jan.12163
- Coole, M., & Brooks, D. J. (2014). Do security systems fail because of entropy? *Journal of Physical Security*, 7(2), 50-76. Retrieved from <http://www.anl.gov/>
- Cope, D. G. (2014). Computer-assisted qualitative data analysis software. *Oncology Nursing Forum*, 41, 322-323. doi:10.1188/14.ONF.322-323

- Cope, D. G. (2014). Methods and meanings: Credibility and trustworthiness of qualitative research. *Oncology Nursing Forum*, 41, 89-91. doi:10.1188/14.ONF.89-91
- Crockett, D., Downey, H., Firat, A, Ozanne, J., & Pettigrew, S. (2013). Conceptualizing a transformative research agenda. *Journal of Business Research*, 66, 1171-1178. doi:10.1016/j.jbusres.2012.08.009
- Crowe, M., Inder, M., & Porter, R. (2015). Conducting qualitative research in mental health: Thematic and content analysis. *Australian & New Zealand Journal of Psychiatry*, 49, 616-623. doi:10.1177/0004867415582053
- Cruzes, D. S., Dyba, T., Runeson, P., & Host, M. (2014). Case studies synthesis: A thematic, cross-case, and narrative synthesis worked example. *Empirical Software Engineering*, 20, 1634–1665. doi:10.1007/s10664-014-9326-8
- Daigneault, P. (2014). Taking stock of four decades of quantitative research on stakeholder participation and evaluation use: A systematic map, *Evaluation and Program Planning*, 45, 171-181. doi:10.1016/j.evalprogplan.2014.04.003
- de las Cuevas, P., Mora, A., Merelo, J., Castillo, P., García-Sánchez, P., & Fernández-Ares, A. (2015). Corporate security solutions for BYOD: A novel user-centric and self-adaptive system. *Computer Communications*, 6883-95. doi:10.1016/j.comcom.2015.07.019
- Deng, J. (1982). Grey systems control. *Systems & Control Letters*, 1, 288-294. doi:10.1016/S0167-6911(82)80025-X
- Densham, B. (2015). Three cyber-security strategies to mitigate the impact of a data breach. *Network Security*, 20155-8. doi:10.1016/S1353-4858(15)70007-3

- de Oliveira Albuquerque, R., García Villalba, L. J., Sandoval Orozco, A. L., Buiati, F., & Tai-Hoon, K. (2014). A Layered Trust Information Security Architecture. *Sensors* (14248220), 14(12), 22754-22772. doi:10.3390/s141222754
- Di Modica, G., & Tomarchio, O. (2016). Matchmaking semantic security policies in heterogeneous clouds. *Future Generation Computer Systems*, 55176-185. doi:10.1016/j.future.2015.03.008
- Doody, O., & Noonan, M. (2013). Preparing and conducting interviews to collect data. *Nurse Researcher*, 20, 28-32. doi:10.7748/nr2013.05.20.5.28.e327
- Draper, J. (2015). Ethnography: Principles, practice and potential. *Nursing Standard*, 29(36), 36– 41. doi:10.7748/ns.29.36.36.e8937
- Duxbury, T. (2012). Towards more case study research in entrepreneurship. *Technology Innovation Management Review*, 9-17. *Advanced online publication*. Retrieved from <http://timreview.ca>
- Earley, S., Harmon, R., Lee, M. R., & Mithas, S. (2014). From BYOD to BYOA, Phishing, and Botnets. *IT Professional*, 16(5), 16-18. doi:10.1109/MITP.2014.69
- Elo, S., Kaariainen, M., Kanste, O., Polkki, T., Utriainen, K., & Kyngas, H. (2014). *Qualitative content analysis: A focus on trustworthiness*. *SAGE Open*, 4, 1-10. doi:10.1177/2158244014522633
- Erlingsson, C., & Brysiewicz, P. (2013). Orientation among multiple truths: An introduction to qualitative research. *African Journal of Emergency Medicine*, 3, 92-99. doi:10.1016/j.afjem.2012.04.005

- Ernst & Young. (2013). *Bring your own device: Security and risk considerations for your mobile device program*. Retrieved from <http://www.ey.com/Publication/>
- Ernst & Young. (2013). *Under cyber-attack: EY's global information security survey 2013*. Retrieved from <http://www.ey.com/Publication/>
- Feigelson, J., Jim, P., Serrato, J. K., & Jonathan, M. (2016). New Federal Guidance on Cybersecurity for Mobile Devices. *Intellectual Property & Technology Law Journal*, 28(3), 25-26.
- Fleming, R. S., & Faye X., Z. (2013). Meeting service level challenges through proactive strategies. *Business Renaissance Quarterly*, 8, 77-88. Retrieved from <http://www.brqjournal.com/>
- Frels, R. K., & Onwuegbuzie, A. J. (2013). Administering quantitative instruments with qualitative interviews: A mixed research approach. *Journal of Counseling & Development*, 91, 184-194. doi:10.1002/j.1556-6676.2013.00085.x
- Ganapathy, M. (2016). Qualitative Data Analysis: Making it Easy for Nurse Researcher. *International Journal Of Nursing Education*, 8(2), 106-110. doi:10.5958/0974-9357.2016.00057.X
- Georgiou A, Marks A, Braithwaite J, et al. (2013) Gaps, disconnections, and discontinuities: the role of information exchange in the delivery of quality long-term care. *The Gerontologist*. 53(5): 770–779.
- Gerhold, L., Bartl, G., & Haake, N. (2017). Security culture 2030. How security experts assess the future state of privatization, surveillance, security technologies and risk awareness in Germany. *Futures*, 50. doi:10.1016/j.futures.2017.01.005

- German, P. (2016). Feature: A new month, a new data breach. *Network Security*, 201618-20. doi:10.1016/S1353-4858(16)30029-0
- Gibson, S., Benson, O., & Brand, S. (2013). Talking about suicide: Confidentiality and anonymity in qualitative research. *Nursing Ethics*, 20(1), 18-29.
doi:10.1177/0969733012452684
- Gilstrap, D. L. (2013). Leadership and decision-making in team-based organizations: A model of bounded chaotic cycling in emerging system states. *Emergence: Complexity & Organization*, 15(3), 24-54. Retrieved from http://emergentpublications.com/ECO/about_eco.aspx?AspxAutoDetectCookieSupport=1
- Gutiérrez-Martínez, J., Núñez-Gaona, M., & Aguirre-Meneses, H. (2015). Business Model for the Security of a Large-Scale PACS, Compliance with ISO/27002:2013 Standard. *Journal Of Digital Imaging*, 28(4), 481-491. doi:10.1007/s10278-014-9746-4
- Haahr, A., Norlyk, A., & Hall, E. O. (2014). Ethical challenges embedded in qualitative 120 research interviews with close relatives. *Nursing Ethics*, 21, 6-15.
doi:10.1177/0969733013486370
- Hayes, B., Bonner, A., & Douglas, C. (2013). An introduction to mixed methods research for nephrology nurses. *Renal Society of Australasia Journal*, 9, 8-14. Retrieved from http://www.renalsociety.org/RSAJ/index_nl.html
- Heslehurst, N., Russell, S., McCormack, S., Sedgewick, G., Bell, R., & Rankin, J. (2013). Midwives perspectives of their training and education requirements in maternal

obesity: A qualitative study. *Midwifery*, 29, 736-744.

doi:10.1016/j.midw.2012.07.007

Hammond, D. (2010). *Science of synthesis: Exploring the social implications of general systems theory*. Boulder, CO: University Press of Colorado.

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management*, 52, 337-347. doi:10.1016/j.im.2014.12.006

Hou, W. L., Ko, N. Y., & Shu, B. C. (2013). Recovery experiences of Taiwanese women after terminating abusive relationships: A phenomenological study. *Journal of Interpersonal Violence*, 28, 157-175. Doi:10.1177/0886260512448851

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigor in qualitative casestudy research. *Nurse Researcher*, 20, 12-17. doi:10.7748/nr2013.03.20.4.12.e326

Hunt, L. (2014). In defense of qualitative research, *Journal of Dental Hygiene*, 88(2), 64-65. Retrieved from <http://jdh.adha.org>

Hunter, M.G., 2012. Creating qualitative interview protocols. *International Journal of Sociotechnology and Knowledge Development*, 4(3), 1-16.

doi:10.4018/jskd.2012070101

IBM & Ponemon Institute (2017). *2017 cost of data breach study: United States*.

Retrieved from <http://www-03.ibm.com/security/data-breach/>

Ibor, A. E., & Obidinnu, J. N. (2015). System hardening architecture for safer access to critical business data. *Nigerian Journal Of Technology*, 34(4), 788-792.

doi:10.4314/njt.v34i4.17

- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31, 83-95. doi:10.1016/j.cose.2011.10.007
- Irvine, A., Drew, P., & Sainsbury, R. (2013). Am I not answering your questions properly? Clarification, adequacy and responsiveness in semistructured telephone and face-to-face interviews. *Qualitative Research*, 13, 87-106. doi:10.1177/1468794112439086
- Johnson, N. (2013). *Primary care physicians' perception of caring for the uninsured* (Doctoral dissertation). Available from ProQuest Dissertation and Theses database (UMI No. 3550359)
- Jones, P., Beynon-Davies, P., Pickernell, D., & Packham, G. (2014). An exploration of the attitudes and strategic responses of sole-proprietor micro-enterprises in adopting ICT. *International Small Business Journal*, 32, 285-306. doi:10.1177/0266242612461802
- 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, 1010-1018. doi:10.1002/smj.2042
- Kast, F., & Rosenzweig, J. (1972, December). General systems theory: Application for organization and management. *Academy of Management Journal*, 15(4), 447-464.
- Kesh, S., & Raghupathi, W. (2013). Managing information security risks: An examination of multiple risk perspectives. *Journal of American Business Review*, Cambridge, 2(1), 35-41. Retrieved from <http://www.jaabc.com/jabrc.html>

- Ketokivi, M., & Choi, T. (2014). Renaissance of case research as a scientific method. *Journal of Operations Management*, 32, 232–240. doi:10.1016/j.jom.2014.03.004
- Khanna, R. (2013). Feature: Data breaches: the enemy within. *Computer Fraud & Security*, 20138-11. doi:10.1016/S1361-3723(13)70071-X
- Kipkulei, K. (2013). *Effects of information technology on reducing perishable waste in supermarkets* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3560427)
- Kira, M., & van Eijnatten, F. M. (2013). Socially sustainable work organisations: A debate. *Systems Research and Behavioral Science*, 30, 506-509. doi:10.1002/sres.2164
- Knowles, W., Prince, D., Hutchison, D., Disso, J. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal On Critical Infrastructure Protection*, 952-80. doi:10.1016/j.ijcip.2015.02.002
- Koc, E., & Boz, H. (2014). Triangulation in tourism research: A bibliometric study of top three tourism journals. *Tourism Management Perspectives*, 12, 9-14. doi:10.1016/j.tmp.2014.06.003
- Kongnso, F. (2015). *Best practices to minimize data security breaches for increased business performance* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3739769)
- Knapp, K. J., & Ferrante, C. J. (2012). Policy awareness, enforcement, and maintenance: Critical to information security effectiveness in organizations. *Journal of*

Management Policy & Practice, 13(5), 66-80. Retrieved from <http://www.na-businesspress.com/jmppopen.html>

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/>

Lamb, D. (2013). Promoting the case for using a research journal to document and reflect on the research experience. *Electronic Journal of Business Research Methods*, 11(2), 84-92. Retrieved from <http://www.ejbrm.com/main.html>

Leavitt, N. (2013). Today's Mobile Security Requires a New Approach. *Computer*, 46(11), 16-19. doi:10.1109/MC.2013.400

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice*, 16, 473-475. doi:10.1177/1524839915580941

Li, Z., Shahidehpour, M., & Aminifar, F. (2017). Cybersecurity in Distributed Power Systems. *Proceedings Of The IEEE*, 105(7), 1367-1388. doi:10.1109/JPROC.2017.2687865

Limburgh, C., van Schalkwyk, G., Lee, K., Buys, C., De Kock, M., Horn, M., ... van Schalkwyk, S. (2013). Cutting to the chase: Participation factors, behavioral effects, and cultural perspectives of participants in an adult circumcision campaign. *AIDS Care*, 25, 1278-1283. doi:10.1080/09540121.2013.764392

- 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, V., Musen, M. A., & Chou, T. (2015). Data breaches of protected health information in the United States. *JAMA: Journal Of The American Medical Association*, 313(14), 1471-1473 3p. doi:10.1001/jama.2015.2252
- Lohle, M. F., & Terrell, S. R. (2014). Real projects, virtual worlds: Coworkers, their avatars, and the trust conundrum. *The Qualitative Report*, 19(8), 1-35. Retrieved from <http://nsuworks.nova.edu/tqr/>
- Longo, B. (2013). Learning on the Wires: BYOD, Embedded Systems, Wireless Technologies and Cybercrime. *Legal Information Management*, 13(2), 119-123. doi:10.1017/S1472669613000285
- Ludovic-Alexandre, V., & Marle, F. (2012). A systems thinking approach for project vulnerability management. *Kybernetes*, 41, 206-228. doi:10.1108/036849212
- Luke, C., Christian, C., & Gordon J., P. (2016). Device-Centric Monitoring for Mobile Device Management. *Electronic Proceedings In Theoretical Computer Science*, 205, 31-44. doi:10.4204/EPTCS.205.3
- Macwillson, A. (2011). *Rethinking cybersecurity in a mobile world*. Retrieved May 27, 2016, from <http://www.securityweek.com/rethinking-cybersecurity-mobile-world>
- Madsen, A. K. (2013). Virtual acts of balance: Virtual technologies of knowledge management as co-produced by social intentions and technical limitations.

- Electronic Journal of E-Government*, 11, 183-197. Retrieved from <http://www.ejeg.com/main.html>
- Maier, R. H. (2013). What constitutes a good literature review and why does its quality matter? *Environmental Modeling & Software*, 43, 3-4.
doi:10.1016/j.envsoft.2013.02.004
- 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(1), 117-133. Retrieved from <http://www.ijbcnet.com/>
- Mansfield-Devine, S. (2014). Mobile security: it's all about behaviour. *Network Security*, 2014(11), 16-20. doi:10.1016/j.diin.2010.05.010
- Mansfield-Devine, S. (2016). Feature: The death of defence in depth. *Computer Fraud & Security*, 201616-20. doi:10.1016/S1361-3723(15)30048-8
- Marbach, E. (2013). Towards a phenomenological analysis of fictional intentionality and reference. *International Journal of Philosophical Studies*, 21, 428-447.
doi:10.1080/09672559.2013.801631
- Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does sample size matter in qualitative research? A review of qualitative interviews in is research. *Journal of Computer Information Systems*, 54, 11-22. Retrieved from <http://www.iacis.org/jcis/jcis.php>
- McAreavey, R., & Das, C. (2013). A delicate balancing act: Negotiating with gatekeepers for ethical research when researching minority communities. *International*

- Journal of Qualitative Methods*, 12(1), 113-131. Retrieved from <https://ejournals.library.ualberta.ca/>
- McNulty, T., Zattoni, A., & Douglas, T. (2013). Developing corporate governance research through qualitative methods: A review of previous studies. *Corporate governance: An International Review*, 21, 183-198. doi:10.1111/corg/12006
- Mealer, M., & Jones, J. (2014). Methodological and ethical issues related to qualitative telephone interviews on sensitive topics. *Nurse Researcher*, 21, 32-37. doi:10.7748/nr2014.03.21.4.32.e1229
- Mishra, S., Caputo, D. J., Leone, G. J., Kohun, F. G., & Draus, P. J. (2014). The role of awareness and communications in information security management: A health care information systems perspective. *International Journal of Management & Information Systems (Online)*, 18, 139-138. Retrieved from <http://cluteinstitute.com/ojs/index.php/IJMIS>
- 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, 173-189. Retrieved from <http://www.jbsq.org>
- Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research*, 25, 1212-1222. doi:10.1177/1049732315588501
- Morse, A., & McEvoy, C. (2014). Qualitative research in sport management: Case study as a methodological approach. *The Qualitative Report*, 19(17), 1-13. Retrieved from <http://ssrn.com/abstract=2458106>

- Murthy, D. (2013). Ethnographic research 2.0. *Journal of Organizational Ethnography*, 2(1), 23-36. doi:10.1108/JOE-01-2012-0008
- Najafi, M., Alimadadi, H., Arastoo, L., Motamed, F., Khodadad, A., Fallahi, G., Doroudian, R. (2014). The clinical manifestations, treatment efficacy and adverse drug reactions in 62 Iranian children with Wilson disease. *International Journal of Pediatrics*, 2, 25-29. Retrieved from <http://ijp.mums.ac.ir/>
- National Institute of Standards Technology. (2013). *Glossary of key information security terms*. Retrieved from <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>
- Nguyen, N. C., & Bosch, O. H. (2013). A systems thinking approach to identify leverage points for sustainability: A case study in the Cat Ba Biosphere Reserve, Vietnam. *Systems Research & Behavioral Science*, 30, 104-115. doi:10.1002/sres.2145
- Nishimura, A., Carey, J., Erwin, P. J., Tilburt, J. C., Murad, M. H., & McCormick, J. B. (2013). Improving understanding in the research informed consent process: a systematic review of 54 interventions tested in randomized control trials. *BMC Medical Ethics*, 14. doi:10.1186/1472-6939-14-28
- O'Cathain, A., Goode, J., Drabble, S. J., Thomas, K. J., Rudolph, A., & Hewison, J. (2014). Getting added value from using qualitative research with randomized controlled trials: A qualitative interview study. *Trials*, 15(1), 1-20. doi:10.1186/1745-6215-15-215

- Onwuegbuzie, A. J., & Byers, V. T. (2014). An exemplar for combining the collection, analysis, and interpretation of verbal and nonverbal data in qualitative research. *International Journal of Education*, 6, 183-246. doi:10.5296/ije.v6i1.4399
- O P, M., Vikas, k., & Dixit, G. (2013). JIT supply chain; an investigation through general system theory. *Management Science Letters*, 3(3), 743-752.
- O'Reilly, M., & Parker, N. (2013). Unsatisfactory saturation: A critical exploration of the notion of saturated sample sizes in qualitative research. *Qualitative Research*, 13, 190-197. doi:10.1177/1468794112446106
- Patten, K. P., & Harris, M. A. (2013). The Need to Address Mobile Device Security in the Higher Education IT Curriculum. *Journal Of Information Systems Education*, 24(1), 41-52.
- Petticrew, M., Refuess, E., Noyes, J., Higgins, J., & Mayhew, J. (2013). Synthesizing evidence on complex interventions: How meta-analytical, qualitative, and mixed-method approaches can contribute. *Journal of Clinical Epidemiology*, 66, 1230-1273. doi:10.1016/j.jclinepi.2013.06.005
- Pezalla, A. E., Pettigrew, J., & Miller - D ay, M. (2012). Researching the researcher - as - instrument: An exercise in interviewer self - reflexivity. *Qualitative Research*, 12(2), 165-185. doi:10.1177/1468794111422107
- Pinchot, J., & Pullet, K. (2015). Bring Your Own Device to Work: Benefits, Security Risks and Governance Issues. *Issues in Information Systems*, 16(3), 238-244.
- Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual*

Review of Psychology, 63, 539-569. Retrieved from

<http://www.annualreviews.org/toc/psych/63/1>

- Rapport, F., Clement, C., Doel, M. A., & Hutchings, H. A. (2015). Qualitative research and its methods in epilepsy: Contributing to an understanding of patients' lived experiences of the disease. *Epilepsy & Behavior*, 45, 94-100.
doi:10.1016/j.yebeh.2015.01.040
- 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(3), 243-256. doi:10.1007/s10660-013-9121-4
- 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
- Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, 5926-44. doi:10.1016/j.cose.2016.01.004
- Rousseau, D. (2015). General Systems Theory: Its present and potential. *Systems Research And Behavioral Science*, 32(5), 522-533. doi:10.1002/sres.2354
- Rowley, J. (2012). Conducting research interviews. *Management Research Review*, 35, 260-271. doi:10.1108/01409171211210154
- Royset, J. O. (2013). On sample size control average approximations for solving smooth stochastic programs. *Computational Optimization and Applications*, 55, 265-309.

- Roy, K., Zvonkovic, A., Goldberg, A., Sharp, E., & La Rossa, R. (2015). Sampling richness and qualitative integrity: Challenges for research with families. *Journal of Marriage and Family*, 77, 243-260. doi:10.1111/jomf.12147
- Rudnick, A. (2014). A Philosophical Analysis of the General Methodology of Qualitative Research: A Critical Rationalist Perspective. *Health Care Analysis*, 22(3), 245-254 10p. doi:10.1007/s10728-012-0212-5
- Samnani, A., & Singh, P. (2013). Exploring the fit perspective: An ethnographic approach. *Human Resource Management*, 52, 123-144. doi:10.1002/hrm.21516
- Sampemane, G. (2015). Internal Access Controls. *Communications Of The ACM*, 58(1), 62-65. doi:10.1145/2687878
- Sangestani, G., & Khatiban, M. (2013). Comparison of problem-based learning and lecture-based learning in midwifery. *Nurse Education Today*, 33, 791-795. doi:10.1016/j.nedt.2012.03.010
- Savola, M. J. (2014). Towards measurement of security effectiveness enabling factors in software intensive systems. *Lecture Notes on Software Engineering*, 2, 104-109. doi:10.7763/LNSE.2014.V2.104
- Scheibe, M., Reichelt, J., Bellmann, M., & Kirch, W. (2015). Acceptance factors of mobile apps for diabetes by patients aged 50 or older: A qualitative study. *Medicine 2.0*, 4, E1. doi:10.2196/med20.3912
- Seidman, I. (2013). *Interviewing as qualitative research: A guide for researchers in education and the social sciences*. New York, NY: Teachers College Press.

- Semer, L. (2013). Auditing the BYOD program: the growing business use of personal smartphones and other devices raises new security risks. *Internal Auditor*, 1, 23.
- Serrano, N., Hernantes, J., & Gallardo, G. (2013). Mobile Web Apps. *IEEE Software*, 30(5), 22-27. doi:10.1109/MS.2013.111
- Seyal, A. H. (2015). Examining the role of transformational leadership in technology adoption: Evidence from Bruneian technical & vocational establishments (TVE). *Journal of Education and Practice*, 6(8), 32-44. Retrieved from <http://www.iiste.org>
- Siddiqui, N., & Fitzgerald, J. A. (2014). Elaborated integration of qualitative and quantitative perspectives in mixed methods research: A profound enquiry into the nursing practice environment. *International Journal of Multiple Research Approaches*, 8, 137-147. doi:10.5172/mra.2014.8.2.137
- Siddiqui, S., Ramesh, A., Manoharan, K., Hussein, A., Jawad, A. M., & Hussain, F. (2014). Developing a framework for the internationalization of British healthcare institutes: A qualitative dual case study analysis. *International Journal of Healthcare Management*, 7, 14-20. doi:10.1179/2047971913Y.0000000059
- Sifeng, L., Liangyan, T., Naiming, X., & Yingjie, Y. (2016). On the New Model System and Framework of Grey System Theory. *Journal Of Grey System*, 28(1), 1-15.
- Sikorskii, A., & Noble, P. C. (2013). Statistical considerations in the psychometric validation of outcome measures. *Clinical Orthopedics and Related Research*, 471, 3489-3495. doi:10.1007/s11999-013-3028-1

- Silic, M., & Back, A. (2013). Factors impacting information governance in the mobile device dual-use context. *Records Management Journal*, 23(2), 73-89.
doi:10.1108/RMJ-11-2012-0033
- Singh, J. S. (2015). Narratives of participation in autism genetics research. *Science, Technology & Human Values*, 40, 227-249. doi:10.1177/0162243914542162
- Smith, R. A., Colombi, M. J., & Wirthlin, R. W. (2013). Rapid development: A content analysis comparison of literature and purposive sampling of rapid reaction projects. *Procedia Computer Science*, 16, 475-482.
doi:10.1016/j.procs.2013.01.050
- Stack, R. J., Sahni, M., Mallen, C. D., & Raza, K. (2013). Symptom complexes at the earliest phases of rheumatoid arthritis: A synthesis of the qualitative literature. *Arthritis & Rheumatism*, 65, 1916-1926. doi:10.1002/acr.22097
- Stake, R. E. (1978). The case study method in social inquiry. *Educational Researcher*, 7(2), 5-8.
- Steiner, P. (2014). Feature: Going beyond mobile device management. *Computer Fraud & Security*, 201419-20. doi:10.1016/S1361-3723(14)70483-X
- Stephens, A. (2013). Principled success. *International Journal of Managing Projects in Business*, 6, 199-209. doi:10.1108/17538371311291099
- Strom, D., Sears, K., Kelly, K. (2014). Work engagement: The roles of organizational justice and leadership style in predicting engagement among employees. *Journal of Leadership & Organizational Studies*, 21(1), 71-82.
doi:10.1177/1548051813485437

- Suter, E., Goldman, J., Martimianakis, T., Chatalalsingh, C., DeMatteo, D. J., & Reeves, S. (2013). The use of systems and organizational theories in the interprofessional field: Findings from a scoping review. *Journal of Interprofessional Care*, 27(1), 57-64. doi:10.3109/13561820.2012.739670
- Taitsman, J. K., Grimm, C. M., & Agrawal, S. (2013). Protecting Patient Privacy and Data Security. *New England Journal Of Medicine*, 368(11), 977-979. doi:10.1056/NEJMp121528
- Thomas, S. (2015). *Exploring Strategies for Retaining Information Technology Professionals: A Case Study* (Doctoral dissertation). Ann Arbor, MI: UMI Dissertation Publishing. Retrieved from ProQuest Dissertations and Theses database. (UMI No. 3681815)
- Titze, K., Schenck, S., Logoz, M., & Lehmkuhl, U. (2014). Assessing the quality of the parent-child relationship: Validity and reliability of the child-parent relationship test (ChiP-C). *Journal of Child & Family Studies*, 23, 917-933. doi:10.1007/s10826-013-9749-7
- Tsang, E. W. K. (2013). Case study methodology: Causal explanation, contextualization, and theorizing. *Journal of International Management*, 19, 195 – 202. doi:10.1016/j.intman.2012.08.004
- Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management*, 52(4), 506-517. doi:10.1016/j.im.2015.03.002

- Tufford, T., & Newman, P. (2012). Bracketing in qualitative research. *Qualitative Social Work*, 11, 80-96. doi:10.1177/1473325010368316
- Unluer, S. (2012). Being an insider researcher while conducting case study research. *The Qualitative Report*, 17, 58. Retrieved from <http://www.nova.edu/ssss/QR/index.html>
- U.S. Department of Health and Human Services.(1979). *The Belmont Report*. Retrieved from <http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html>
- U.S. Department of Homeland Security. (2016). *Recommended Practice: Improving industrial control systems cybersecurity with defense-in-depth strategies*. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
- Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences*, 15, 398-405. doi:10.1111/nhs.12048
- Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods. *MIS Quarterly*, 37, 21-54. Retrieved from <http://www.misq.org>
- Verner, J. M., & Abdullah, L. M. (2013). Exploratory case study research: Outsourced project failure. *Information and Software Technology*, 54, 866-886. doi:10.1016/j.infsof.2011.11.001

- 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. (1968). *General systems theory: Foundations, development, application* (Revised ed.). New York, NY: George Braziller.
- von Bertalanffy, L., Juarrero, A., & Rubino, A., C. (2008). An outline of general system theory. *Emergence: Complexity & Organization*, 10, 103-123. Retrieved from <http://www.isce.edu/index-2.html>
- von Bertalanffy, L. (1972). The history and status of general systems theory. *Academy of Management Journal*, 15, 407-426. doi:10.2307/255139
- Wagstaff, C. R. D., Hanton, S. and Fletcher, D. (2013). Developing emotion abilities and regulation strategies in a sport organization: An action research intervention. *Psychology of Sport and Exercise*, 14(1), 476-487.
- Wang, C. J., & Huang, D. J. (2013). The HIPAA conundrum in the era of mobile health and communications. *JAMA: Journal Of The American Medical Association*, 310(11), 1121-1122. doi:10.1001/jama.2013.219869
- Wang, Y., Shi, S., Nevo, S., Li, S., & Chen, Y. (2015). The interaction effect of IT assets and IT management on firm performance: A systems perspective. *International Journal Of Information Management*, 35580-593.
doi:10.1016/j.ijinfomgt.2015.06.006
- Weidmann, N. B. (2015). A closer look at reporting bias in conflict event data. *American Journal of Political Science*, n.p. doi:10.1111/ajps.12196

- Welch, D., Grossaint, K., Reid, K., & Walker, C. (2014). Strengths-based Leadership Development: Insights from expert coaches. *Consulting Psychology Journal: Practice & Research*, 66(1), 20-37. doi:10.1037/cpb0000002
- Wikina, S. B. (2014). What Caused the Breach? An Examination of Use of Information Technology and Health Data Breaches. *Perspectives In Health Information Management*, 1-16 16p.
- Williams, L., Burton, C., & Rycroft-Malone, J. (2013). What works: a realist evaluation case study of intermediaries in infection control practice. *Journal of Advanced Nursing*, 69, 915-926. doi:10.1111/j.1365-2648.2012.06084.x
- Wilson, C. V. (2012). *Postimplementation planning and organizational structure of enterprise resource planning systems*. (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database. (UMI No. 3512581)
- Wisdom, J. P., Cavaleri, M. A., Onwuegbuzie, A. J., & Green, C. A. (2012). Methodological reporting in qualitative, quantitative, and mixed methods health services research articles. *Health Services Research*, 47, 721-745. doi:10.1111/j.1475-6773.2011.01344.x
- Yang, J. S., Lee, H. J., Park, M. W., & Eom, J. H. (2015). Security threats on national defense ICT based on IoT. *Advanced Science and Technology Letters*, 97, 94-98. doi:10.14257/astl.205.97.16
- Yin, R. (1981). The case study crisis: some answers. *Administrative Science Quarterly*, 26, 58-65.

- Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation*, 19, 321-332. doi:10.1177/1356389013497081
- 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
- Zenko, Z., Rosi, B., Mulej, M., Mlakar, T., & Mulej, N. (2013). General systems theory completed up by dialectical systems theory. *Systems Research and Behavioral Science*, 30, 637-645. doi:10.1002/sres.2234
- 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, 123-152. Retrieved from <http://www.jmis-web.org/issues>

Appendix A: Interview Protocol

Interview: Strategies to Prevent Security Breaches Caused by Mobile Devices?

Participant ID: _____ Date: _____ Starting Time: _____

- A. The interview will start with introductions and an overview of the topic.
- B. I will thank each participant for agreeing to participate in the study.
- C. I will remind the participant the interview is being recorded and that all information will remain strictly confidential.
- D. I will start the recording, announce the participants alphanumeric code and the date and time.
- E. Each interview will last approximately 30 - 45 minutes or until all of the interview questions and any follow-up questions have been answered.
- F. At the conclusion of the interview, I will explain the concept and overall plan for member checking.
- G. Once answers have been confirmed to the satisfaction of the participants, the interview will conclude with a thank you for participating in the study.

Interviewing:

- Each response from the participant will be paraphrased to ensure accuracy (e.g., so from what I heard; in essence you mean).
1. What strategies have you used to prevent data breaches caused by mobile devices?

Comments:

--

2. What strategies have you used that failed to prevent a data breach caused by mobile devices?

Comments:

3. What strategies have you used that succeeded to prevent a data breach caused by mobile devices?

Comments:

4. What challenges did you face in implementing/using these strategies?

Comments:

5. What additional information would you like to share about strategies to prevent data breaches caused by mobile devices?

Comments:

--

Closing time: _____

Interview Follow-Up

Script: Thank you for taking this time for a follow-up phone call to go over my interpretation and give you the opportunity to correct any mistakes or to add any additional detail you see fit.

Interview Question	Did I interpret your response correctly? Or is there anything you would like to add?
What strategies have you used to prevent data breaches caused by mobile devices?	Interpretation:
	Comments:
What strategies have you used that failed to prevent a data breach caused by mobile devices?	Interpretation:
	Comments:
What strategies have you used that succeeded to prevent a data breach caused by mobile devices?	Interpretation:

	Comments:
What challenges did you face in implementing/using these strategies?	Interpretation:
	Comments:
What additional information would you like to share about strategies to prevent data breaches caused by mobile devices?	Interpretation:
	Comments:

Appendix B: Interview Questions

Interview Questions

1. What strategies have you used to prevent data breaches caused by mobile devices?
2. What strategies have you used that failed to prevent a data breach caused by mobile devices?
3. What strategies have you used that succeeded to prevent a data breach caused by mobile devices?
4. What challenges did you face in implementing/using these strategies?
5. What additional information would you like to share about strategies to prevent data breaches caused by mobile devices?