THE EFFECTS OF INFORMATION TECHNOLOGY LEADERSHIP AND INFORMATION SECURITY GOVERNANCE ON INFORMATION SECURITY RISK MANAGEMENT IN USA ORGANIZATIONS

by

Henry I. Okonofua

SHAWON RAHMAN, PhD Faculty Mentor and Chair

GLENN BOTTOMLY, PhD, Committee Member

JELENA VUCETIC, PhD, Committee Member

Tonia Teasley, JD, Interim Dean

School of Business and Technology

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree of

Doctor of Philosophy

Capella University

October 2018

Abstract

This study addressed the topic of information security (IS) risk management in the context of information technology (IT) leadership and IS governance. Although organizations face continuously evolving IS risks, the scholarly literature is unclear as to whether transformational, transactional, and passive-avoidant leadership styles influence IS risk management. A similar gap exists concerning the correlation between IS governance and IS risk management. The purpose of the study was to ascertain the extent of the relationships between these variables. The research was also designed to determine whether IS governance mediated the relationship between IT leadership style and IS risk management. The study was conducted using a quantitative, non-experimental, descriptive research design. The sample consisted of senior IT leaders with a range of titles including Chief Information Officer (CIO), Chief Information Security Officer (CISO), Director of IT, and IT Manager. This population is characterized by extensive knowledge of IT and IS issues, and these individuals are generally responsible for directing an organization's approach to IS risk management. Data from 250 participant surveys were analyzed using the Pearson product-moment coefficient correlation and multiple regression analysis. The results of the analysis demonstrated that both IT leadership and IS governance were significantly related to IS risk management, but IT governance does not intervene with the relationship between IT leadership style and IS risk management. The multiple regression analysis indicated that together, IT leadership and IS governance accounted for 50% of the variance in IS risk management. The present study added to the current literature on IS risk management by demonstrating the importance of IT leadership and IS governance, but a more

robust analysis will facilitate the identification of the most effective leadership styles and governance frameworks.

Dedication

This dissertation is dedicated to the memory of my late father, Edward Iregbeyen Okonofua, for his influence in my life, my mother Elizabeth Aluede and my grandmother Grace Omamobo Ehikhuemhen for their inspiration, nurture, and impact in my life.

To the love of my life, Deborah Okonofua, I want to express my special and deep gratitude for your support and boundless patience. Your strength, comfort, and reassurance were my compass and what I needed. And my children, Sandra, Godswill, Joshua, and Joseph, thank you for your support, understanding and long-suffering. You forfeited a lot of quality time away from Dad while I was engrossed in this dissertation.

I also offer special thanks to my uncles Paul and Christopher Akhator for their help and guidance through school and life. Also, Matthew Okonofua for his love, support and care, and comforting words. To my brothers and sisters, Maggie, Emma, Precious, Tony, Omonigho, and Benedicta you make life worth living.

To my colleagues and men of God, thank you for your prayers and encouragement all the way. Finally, I thank God who is my helper, for the strength for the journey and for making this to happen.

Acknowledgments

It was a great pleasure and the honor of my life to work with this committee members Dr. Shawon Rahman (Chair), Dr. Alan Chmura (late), Dr. Glenn Bottomly, and Dr. Jelena Vucetic. Special thanks to Dr. Rahman for his prompt responses, advice, tremendous work ethic, and valuable insight. Your support and mentorship were invaluable throughout this process. Thanks to Dr. Bottomly and Dr. Vucetic for their insights, comments and early responses. Thanks to Dr. Jerry Luftman for the permission to use his instrument and for volunteering to be a member of the committee.

Table of Contents

List of Tables

List of Figures

CHAPTER 1. INTRODUCTION

Information security (IS) risk management has turned out to be an essential element of best practice in corporate governance (Adesemowo, Von Solms, & Botha, 2016; Agarwal, 2017). IS risk management is no longer being treated as an IT issue but as a critical component of general business practice in organizations (Knorst, Vanti, Andrade, & Johann, 2011). Supporting this observation, Bobbert and Mulder (2015) noted that IS risk management policy is decided at the board level and implemented by information technology (IT) leadership. Recognizing the central roles of both IT leaders and IS governance, the current study appraised the relationship between these factors and their influence on IS risk management in U.S.-based organizations.

Chapter 1 introduces some necessary contextual background information for the present study. The chapter sections following the background address the statement of the problem, and both the purpose and significance of the study. Following this, the next two sections introduce the research questions and provide definitions of key terms. Finally, a discussion of the research design and the assumptions and limitations of the present study is subject to be followed by an organizational summary of the remaining four chapters.

Background of the Problem

Risk management of information security breaches is now a regular matter of concern at Board level in U.S. organizations. Von Solms and Von Solms (2009) acknowledged this when they noted that by the end of the first decade of the new millennium, information security risk management had become the primary concern of corporate governance. By 1998, the

Information Systems Audit and Control Association (ISACA) formed the IT Governance Institute, whose 2006 guide for boards of directors and executive management noted that it was expected that boards of directors would treat information security as an intrinsic element within corporate governance efforts. As an essential component of corporate governance, information security must be aligned with the governance processes in place to oversee other critical functions within the organization (Brotby, 2006). Turel and Bart (2014) stated that in the years directly before their study that the involvement of boards of directors in IT matters had continued to increase to the point that their study was explicitly focused on the antecedents and consequences of board-level IT governance.

According to Nazareth and Choi (2015) managing information security risks is both challenging and critically important particularly given the increasing frequency, rapid evolution, and severity of threats to organizations. Galdies (2014) noted that such threats to organizations' information security stem from both internal and external actors and both unintentional and intentional actions on these actors parts. In practice, such threats may manifest as technical failures, systemic vulnerabilities, human error, fraud, and external events among others (Bojanc & Jerman-Blazic, 2013).

The establishment of timely and adequate information security governance (ISG) policies is the most appropriate way to bolster security processes and align said processes with the organization's objectives (Mellado, Sánchez, Fernández-Medina, & Piattini, 2013; Wu, Straub, & Liang, 2015). Furthermore, organizations' ISG policies must be structured to support and protect the confidentiality, integrity, and availability of the organization's assets (Von Solms & Van Niekerk, 2013). However, implementing ISG policies for information security risk management requires the deployment of the appropriate technologies, methods, methodologies, and processes, as well as appropriate human resources (Nazareth & Choi, 2015; White, 2013) In turn, to optimize, IS security outcomes based on the organization's governance policies and resources deployed to support them, requires effective leadership which has been linked by scholars to decreased systemic organizational security risks (Alqahtani, 2015; Apollonia, & Ihagh, 2016; Arslan, & Staub, 2013; Richard, Devinney, Yip, & Johnson, 2009).

While research links effective leadership to decreased systemic risks, the literature also provides numerous definitions of leadership (Antonakis & Day, 2017). The questions that engaged the researcher were first, what leadership style was most effective in the context of information security risk management (ISRM)? Second, how did the inter-relationships between information technology leadership, information security governance impact on organizational information security risk management?

To avoid the need to address a multiplicity of definitions of leadership while still being able to capture the perspectives of a full range of leadership styles, the theoretical framework was chosen to underpin the present study was Bass & Avolio's (1994) Full Range Leadership Theory. This theory is well supported and has been well validated (Avolio, 2011). There were additional reasons for choosing the FRLT as well. The first was that there was good empirical support for the validity of the FRLT in the context of IT (Thite, 2000). The second was that previous scholarship had found that CIOs were increasingly found at the board-level of organizations by the late 1990s (Armstrong & Sambamurthy, 1999) and that the interactions of CIOs with the rest of top management was stronger in organizations who exhibited transformational IT vision (Armstrong & Sambamurthy, 1999).

The full-range leadership model instantiates the FRLT, and the present study utilized the Multifactor Leadership Questionnaire (MLQ-5X) which is the most recent version of the instrument associated with the model. The MLQ was explicitly designed by Avolio & Bass (2004) to assess a full range of leadership styles. The MLQ utilizes nine scales to measure three overarching leadership styles: transformational, transactional and passive-avoidant. It also provides two scales that measure the actual outcomes of leadership (Avolio & Bass, 2004).

More rigorous research on the effects of leadership on effective information security risk management in organizations is needed (Hu, Dinev, Hart, & Cooke, 2012). The senior leaders create the organization-wide culture of safety and business competencies in the organization (Epstein, 2014). IT managers assist in the implementation of security programs and monitor information security management assurance in the organizations. According to Chen, Ramamurthy, and Wen (2015) leaders styles with detailed knowledge of the principles of IS governance enhance the understanding of governance principles and IS risk management.

Statement of the Problem

Research has demonstrated that organizations face continuously evolving risks, and as a result, IT leadership and governance practices related to organizational risk management must also continually evolve (Knorst et al., 2011). According to both Hargis, Watt, and Piotrowski, (2011), and Odumeru and, (2013) effective organizational leadership is integral to the management of both IS risks and regulatory compliance. Research has also established that IS governance can reduce system security risks (Alqahtani, 2015; Apollonia, & Ihagh, 2016; Arslan, & Staub, 2013). Leadership and governance differ in the sense that IS governance takes place at the board level, whereas IT technology leadership takes place at the level of line management (Bobbert & Mulder, 2015). There has been an increase in research on IT leadership and its importance to organizational success (Bobbert & Mulder, 2015; Latham, 2014; Meuser et al., 2016). However, there has been no evaluation of the effects of IT leadership and IS governance on IS risk management in U.S. organizations (Gbenle, 2013). The present study addressed that gap in the extant literature.

Purpose of the Study

The purpose of this quantitative, non-experimental, descriptive study was to examine the effects of IT Leadership and IS Governance on IS Risk Management in U.S. organizations. The significance of leadership in organizations has been under considerable scrutiny since the formation of groups and organizations. The growing diversity of leadership theories pose several challenges to the advancement of leadership (Langley, Smallman, Tsoukas, & Van de Ven, 2013; Meuser et al., 2016), and the understanding of its applications and practice (Latham, 2014).

Effective IT leadership should decrease information risk and allow information to be exchanged reliably (Flores, Antonsen, & Ekstedt, 2014; Tu & Yuan, 2014). This study provided insights into how leadership styles were related to IS risk management and how IS governance influences that relationship. Thus, the study’s findings allow researchers, managers, and IT leaders to apply leadership skillsets that reduce risk and create an awareness of the significance of efficient IS risk management in organizations. This study also evaluated the correlation between IT leadership and IS governance in organizations and explored the influence of these different levels of oversight on the protection of organizational assets.

Significance of the Study

This study’s significance is explained in the following section. First, IT leadership, IS governance and IS risk management constitute crucial topics for modern organizations (McFadzean, Ezingeard, & Birchall, 2011; Williams, Hardy, & Holgate, 2013). Scholars have noted that the industry is challenged by the lack of knowledge related to the influence that IT leadership has in improving IS risk management in organizations (Landis, Hill, & Harvey, 2014). Furthermore, Nichols (2016) noted that there are differences in IT leadership traits which are useful in the analysis of leadership qualities and the resultant impact on IS risk management. The present research contributed to the understanding of how different leadership styles (i.e., transformational, transaction, and passive-avoidant) are related to IS governance and how the interaction of these elements affects IS risk management in organizations. It was expected that the present study's findings would underscore the importance of governance strategies in the field of IS (see Jadric, Cukusic, & Garaca, 2016).

The study was also significant in that it added to the literature on IT leadership by widening the scope of inquiry. The use of behavioral theories offers a unique perspective that focuses on the behaviors of the leaders rather than their cognitive, biological, or social traits (Gajendran, & Brewer, 2012). Thus, with the development of leadership theories, researchers should be concerned with a better understanding of how certain fundamental aspects of leadership can create an environment conducive for system thinking and value creation for organizations (Latham, 2014; Safa, Von Solms, & Furnell, 2016). Consequently, effective leadership abilities can be cultivated if research can identify which leadership styles are most effective at promoting positive risk management behaviors. This study aimed to make a significant contribution related to the understanding of IT leadership styles in relation to both IS governance practices and IS risk management in U.S. organizations.

Research Questions

This research was originated to study the relationships between IT leadership styles, IS governance, and IS risk management in U.S. institutions. The study was guided by an overarching research question that asked:

Overarching Research Question: To what extent are IT leadership style and IS governance related to IS risk management in U.S. organizations?

The primary research question was answered by asking two specific subquestions:

Subquestion 1: To what extent are IT leadership style and IS governance individually related to IS risk management in U.S. organizations?

Subquestion 2: To what extent does IS governance mediate the relationship between IT leadership style and IS risk management in U.S. organizations?

Definition of Terms

The following terms are defined to clarify their use in this research.

Communications. One of the components of the variable IS governance. Luftman, Ben-Zvi, Dwivedi, and Rigoni (2012) noted that communications refer to the goals and the objectives set between IT and business departments within an organization. Communications are essential for information sharing within the institution to allow the parties to efficiently function and understand the business environment (Luftman et al., 2012).

Competency/value. One of the components of the variable IS governance. Competency/value is used to validate IT's contribution to the organization in relation to management (Luftman et al., 2012).

Governance. One of the components of the variable IS governance. Governance is defined as the processes for making decisions and the individuals with authority to make business decisions and set IT priorities within an organization (Luftman et al., 2012).

IS governance. The mediating variable in the present study. IS governance defined as the set of frameworks and tools as well as decisions that an organization institutionalizes to meet its operational and institutional objectives (Stair, & Reynolds, 2010). IS governance is comprised of six components: (a) communications, (b) competency/value, (c) governance, (d) partnership, (e) scope and architecture, and (f) skills (Luftman et al., 2012). IS governance provides tactical direction, satisfies organizational objectives, manages risks, and ensures the responsible use of corporate resources while monitoring the enterprise security program (Williams et al., 2013). Enterprises need a comprehensive set of policies, processes, and systems for the effective risk management of information assets, ensuring acceptable levels of information security risk (Parra Reyes, 2015).

IS risk management. The dependent variable in the present study. IS risk management was defined as the adoption of a comprehensive set of policies, processes, and systems to manage information asset risks and ensure acceptable levels of information security risk (Parra Reyes, 2015). Fadun (2013) noted that risk management is not focused on evading or eliminating risk, but instead is focused on managing an organization's operational risk through the reduction of threats and the maximization of opportunities. IS risk management was measured based on an organization's use of ISO/IEC 27001/27002 standards, which offers specifications for implementing and maintaining IS management systems (Ristov & Gusev, 2013).

IT leadership style. The independent variable in the present study. IT leadership style was defined as either transactional, transformational, or passive-avoidant. Hussain and Hassan (2016) noted that leadership refers to the ability to persuade followers to adopt goals or objectives and work toward them collectively. Antonakis and Day (2017) characterized leadership as the ability to motivate others to achieve an outcome.

Partnership. One of the components of the variable IS governance. Partnership gauges the trust relationship between IT and business elements within an organization (Luftman et al., 2012).

Passive-avoidant leadership style. A leadership style that fluctuates and allows subordinates to operate with limited management or oversight (Avolio & Bass, 2004). The passive-avoidant leadership style is laissez-faire, absent-minded, and unchallenging (Badshah, 2012). Under this leadership style, projects fail when the leaders do not provide communication or direction (Badshah, 2012).

Scope and architecture. One of the components of the variable IS governance. Scope and architecture determine the level of integration within an organization (Luftman et al., 2012). The scope of IT usage is directly linked to business-IT alignment.

Skills. One of the components of the variable IS governance. Skills measure the human resource practices associated with hiring, training, and career advancement (Luftman et al., 2012). Skills help determine adaptability in the face of changing management styles.

Transactional leadership style. A leadership style that uses positive and negative reinforcement to motivate followers (Avolio & Bass, 2004). This form of leadership allows leaders to achieve their goals by emphasizing extrinsic rewards, avoiding risks, and focusing on an organization's goals (McCleskey, 2014). Transactional leadership is criticized as an unyielding style because it utilizes rewards and punishments, and as a result, it does not encourage creativity or the accountability of employees for actions within the organization (Tyssen, Wald, & Spieth, 2014).

Transformational leadership style. A leadership style in which the leader employs charisma and enthusiasm to inspire his followers (Avolio & Bass, 2004). Transformational leaders obtain management positions due to their personalities, and they develop vision and direction for the organization (Odumeru & Ifeanyi, 2013). Transformational leaders inspire and motivate workers to greater heights by continually challenging them.

Research Design

This research employed a quantitative, non-experimental, descriptive research design to examine the relationship between IT leadership style, IS governance, and IS risk management in U.S. organizations. Quantitative research clarifies a phenomenon by gathering measurable information that can be examined using numerical techniques (Creswell, 2014; Muijs, 2010). The present study was characterized as non-experimental because the variables were not manipulated, modified, or controlled (see Swanson, & Holton, 2005). The primary intent was to test associations between IT leadership styles, IS governance, and IS risk management in U.S. organizations based on their use of ISO/IEC 27001/27002 standards.

This study used a deductive framework for the variables and research questions based on theory. The goal of the research was to determine the type of correlation between the independent variable of IT leadership style and the mediating variable of IS governance (see Gbenle, 2013). These variables were examined in relation to their ability to influence or explain the dependent variable, use of the ISO/IEC 27001/27002 standards. The research contributed to the existing literature on relationships between IT leadership style and IS governance and their impact on IS risk management.

A descriptive survey instrument was used to collect and data from participants. The data were then analyzed using correlation and multiple regression techniques. This approach was consistent with existing studies in the literature which noted that the goal of descriptive studies is to explain phenomena and their features (Gall, Gall, & Borg, 2007; Nassaji, 2015). Figure 1 presents a diagram of the relationship between the study's variables.

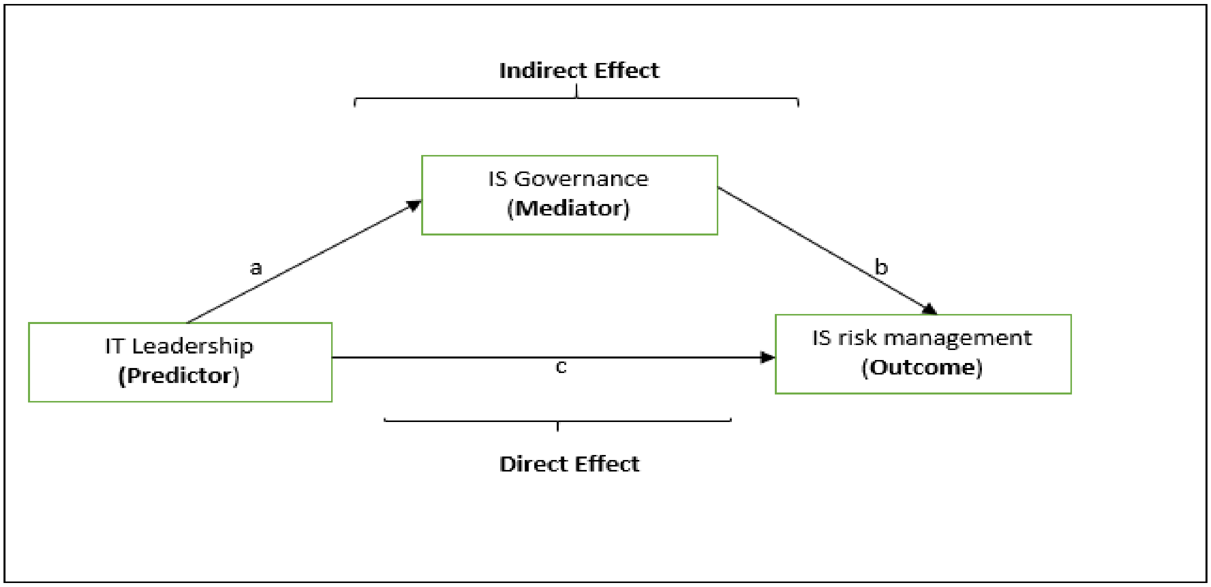

Figure 1. Relationships between the variables.

Assumptions and Limitations

Assumptions

Several topical assumptions were made during the design of this study. For example, it was assumed that the participants in this study (e.g., IT Directors, Managers, CIOs, and CISOs) had knowledge of the leadership and governance processes within their organizations. The researcher assumed that the sample frame selected for this study was an accurate representation of the population of IT leaders responsible for addressing IS risks in U.S. organizations. IT leaders such as CIOs, CISOs, and IT directors and managers have both leadership skills and knowledge of IS risk management. Thus, it was assumed that the participants would answer the survey questions based on their technical skills and knowledge of IT and IS.

From a methodological perspective, it was assumed that the research questions and the variables could be measured on a scale and their values could be subjected to statistical analysis and interpretation. As the research employed methods frequently used by previous researchers, the researcher deemed this assumption to be reasonable. Furthermore, the instruments used in this study had been previously developed and tested using a peer-review process, and as a result, the researcher assumed that the scales adequately addressed the complex topics explored within this study.

Limitations

The present research had several inherent limitations. First, the study was limited by its quantitative nature. Quantitative research has many advantages and allows researchers to predict and measure relationships between variables (Muijs, 2010). However, when using quantitative methodologies, researchers accept that the scope of their research will be limited in the sense that participants do not have an opportunity to share observations about a phenomenon in their own words. Additionally, the researcher's selection of specific instruments and theories limits the perspective of the study. For example, only three types of leadership styles were examined (i.e., transactional, transformational, and passive-avoidant). These limitations mean that the study cannot widely explore all possible explanations for outcomes related to IS risk management in U.S. organizations. These limitations are, however, necessary to ensure that the scope of the study was within the ability of the research to complete in a timely and thorough fashion.

The methodological approach also limited the researcher's ability to draw conclusions from the results. The researcher used an online survey to collect cross-sectional data. Online surveys can be limitations in the sense that a researcher is not able to observe participants as they complete the survey or offer any clarification if questions are misunderstood (DeSimone, Harms, & DeSimone, 2014). Furthermore, the use of a single survey to collect data did not allow the researcher to measure changes in the variables over time or measure IS risk management outcomes in companies where IT leadership styles have changed.

Organization of the Remainder of the Study

This study is made up of five chapters. Chapter 1 provided the background of the research problem, which examines the effect of IT leadership and IS governance on IS risk management in U.S. organizations. Chapter 2 provides a review of existing literature relating to the study’s theoretical framework and the variables of interest, specifically: IT leadership, IS governance and IS risk management. Chapter 3 explains the research design and the procedures used to conduct the study. Chapter 4 contains the results of the statistical analysis. The results of the respondents’ characteristics and the collected data are presented as well as an assessment of the validity and reliability of the scales. Chapter 5 contains a discussion of the findings along with implications and recommendations for future research.

CHAPTER 2. LITERATURE REVIEW

This chapter starts with a review of literature related to IT leadership, IS governance and their impact on IS risk management in US organizations. This study examines the full range of leadership styles made up of the transformational, transactional, and passive-avoidant leadership styles (Avolio & Bass, 2004). The IS governance practices involve skills, governance, value, communications, partnership, scope, and architecture (Luftman, 2003) in a relationship with IS risk management in US organizations. A variety of the IS governance researchers identify information security as a leadership problem (Barrick, Thurgood, Smith, & Courtright, 2015; Von Solms & van Niekerk, 2013). The subject matter is primarily prescriptive and offers little practical guidance (Williams et al., 2013). Though literature indicates that IT leadership enhances IS governance (Gbenle, 2013), there is a gap in determining which leadership style is more effective in governing the security of organizations.

The objective of this chapter is to review how leadership styles and actions of IS governance support IS risk management in organizations. Leaders manage the short and long-term goals of development, examination, execution, and maintenance of the organization's security program. As security risks are continually changing (Allam, Flowerday, & Flowerday, 2014), the administration of an organization’s IS governance programs can help reduce threats and allow for the reliable sharing of information and computer data (Flores et al., 2014; Tu, & Yuan, 2014). The review of the effects of IT leadership and IS governance on IS risk management is based on the decision-making process of leaders (Caudle, 2013) and the execution of a range of governance programs leading to successful prevention and management of IS risks (Rid & Buchanan, 2015).

The theoretical framework that precedes this study is the study developed by Gbenle (2013), which investigated the relationship between IT Governance and IT leadership. This study as shown in Figure 1, utilized Luftman's (2003) Strategic Alignment Maturity Model (SAMM) and the Multifactor Leadership Questionnaire (MLQ-5X). SAMM is a widely accepted experimental assessment tool for determining business and IT alignment. Business and IT is one of the leading concerns by senior management in organizations (Hiekkanen, 2015). Strategic alignment is a significant precursor of IT business performance in determining whether organizations and IT are aligned and make the best use of IT investments for decision making (Luftman et al., 2012).

Bass (as quoted by Landis et al., 2014) argued that "If a theory of leadership is to be used for diagnosis, training, and development, it must be a theory grounded in the concepts and assumptions that are acceptable to and used by managers, officials, and emergent leaders" (p. 98). According to Landis et al. (2014) to provide a review of the critical research on leadership, the crucial parts of the theories and their implications must be studied including a review of IS governance programs and the alignment of IT-business in organizations. Next, is a brief description of IS risk management and standards for measuring effective ISRM.

Methods of Searching

The researcher utilized a combination of data searches performed at Capella University's library and utilizing Google scholar. The researcher searched specific databases such as Sage Journals Online, Business Source Complete, and Applied Sciences Complete. Two tools provided by the library and used in the present search were (a) Summon and (b) the Journal and Book Locator.

A keyword search was performed, and it included, but was not limited to, such terms as IT Leadership, IS governance, FRLT, FRLM, transformational leadership, transactional leadership, passive-avoidant leadership, security framework, and security standards, ISO, NIST, and FFIEC. Additionally, the researcher utilized the Capella library guides pages to assist in searching additional databases such as the ABI/INFORM Collection, Academic Search Premier, Credo Reference Dissertations @ Capella, Dissertations and Thesis Global, EBSCO host, and ERIC. Throughout the dissertation process, Google Scholar was utilized to monitor the literature on an ongoing basis for new studies on topics relevant to the present study.

Theoretical Orientation for the Study

The theoretical orientation of the present study rests on the full range leadership theory (FLRT). Bass and Avolio (1994) developed the FRLT based on work by Burns (1978) who first conceived of the idea of transformational authority. Bass and Avolio used the notion of transformational authority to develop their concept of transformational leadership. In terms of the FRLT,

> “There are three types of leadership behaviors, represented by nine distinct factors. These are Transformational (idealized influence attributed to charisma, idealized influence behavior attributed to beliefs and values, inspirational motivation, intellectual stimulation, individualized consideration). Transactional (contingent rewards, management-by-exception passive, management-by-exception). Non-transactional laissez-faire.~~.~~” (Avolio, 2011, p. 7)

The full-range leadership model (FLRM) instantiates the FLRT. Avolio (2011) noted that it is fundamental to the FLRM that “...every leader displays each style to some degree.” (p. 67) The FRLM does not provide a continuum of behaviors that go from bad to good. Instead, the

FRLM represents a continuum that progresses from less to more effective leadership behaviors, and that effectiveness is dependent on circumstances. A full-range leader chooses the leadership style that best suits the circumstances (Avolio, 2011).

Like other forms of leadership, IT leadership can be characterized based on the styles leaders use when interacting with subordinates. The three leadership styles examined in the present study are the transformational, transactional and passive-avoidant as understood by Bass and Avolio's (1994) FRLT. Scholars have identified many leadership styles; however, not all are appropriate in any given context or industry. The present study utilizes the FRLT as empirical research has shown its applicability to IT leadership.

Thite (2000) conducted a seminal study on IT leadership styles and found that no one leadership style was suitable in all situations. Instead, Thite discovered that an amalgamation of behaviors blending transformational and technical leadership styles enhanced transactional leadership effectiveness. This combination of leadership styles led to superior outcomes characterized by high rates of project success. Thite's research provided empirical validation that transformational and transactional leadership theories are a good fit with leadership in ICT. Furthermore, Thite's study provided support for Bass and Avolio's (1994) work on transformational leadership and the development and use of the FRLT within the domain of ICT management.

IT leadership comprises of directors and executive management concerned with IT and IS governance at the strategic level of an organization and senior and middle management at the tactical level who are concerned with implementing the IT and IS policies adopted and enforced by the strategic level of management (Von Solms & Von Solms, 2009). A key component of IT leadership at the tactical or line management level of organizations is IT security management (Von Solms & Von Solms, 2009).

IT leadership is often represented at board level by a Chief Information Officer (CIO). Armstrong and Sambamurthy (1999) studying the phenomenon of the arrival of CIO's in top management teams, found that CIO interaction with top management was stronger in firms with transformational IT vision. Table 1, below summarizes the functions of governance versus management.

Table 1. *Responsibilities of Governance Versus Management*

Governance	Management
Oversight	Implementation
Authorizes decision rights	Authorized to make decisions
Enact policy	Enforce policy
Accountability	Responsibility
Strategic planning	Project planning
Resource allocation	Resource utilization

From Confluence Spaces, Retrieved from https://spaces.at.internet2.edu/display/2014infosecurityguide/Information_Security_Governance. Adapted with permission.

Review of the Literature

Scholars have noted that effective IT leadership leads to superior outcomes for organizational IS risk management (Adesemowo et al., 2016; Agarwal, 2017). IS governance provides overall direction to IT leadership, characterized in modern organizations by the board-level adoption of an IT risk framework (Agarwal, 2017; Fitzgerald, 2012). The actual execution of IS risk management is the domain of the line managers in an organization who execute the vision and policies provided by IT leadership (Fitzgerald, 2012).

This literature review commences with discussions of IT leadership in the analytical context of the FRLT, IS governance, and IS risk management. Within IT leadership, transformational, transactional, and laissez-faire leadership styles are evaluated. The IS governance literature focuses on the role of IS governance professionals and present security frameworks and standards. The information security risk management portion of the literature review provides context on the interrelationships between policy, management, and implementation. Table 2 provides a summary of the three FRLT leadership styles

IT Leadership and the FRLT

Thite's (2000) seminal empirical research strongly linked transformational and transactional leadership to effective IT leadership practice. Scholars have found that the FRLT has strong explanatory power. The three key leadership behaviors captured by the FLRT are discussed in detail in the three following sections. Figure 2 depicts the spectrum of leadership styles with their associated behavioral dimensions.

Passive avoidant/laissez-faire leadership. Passive-avoidant leadership is a nontransactional laissez-faire leadership style characterized by some scholars as a non-leadership style. Scholars often define passive-avoidant leadership as leadership that relinquishes responsibilities evade making decisions (Robbins, Judge, & Sanghi, 2007). Indeed, scholars such as Shao, Feng, and Liu (2012) equated passive-avoidant leadership with a refusal to lead. Key characteristics of passive-avoidant leaders are their propensity to vacillate and their desire to avoid making decisions, particularly critical or high-priority decisions (Hinkin & Schriesheim, 2008; Yukl & Mahsud, 2010). Often viewed as uninvolved, passive-avoidant leaders are frequently withdrawn and uncaring or unconcerned about the goals of the project or organization to which they are associated (Hinkin & Schriesheim, 2008).

Table 2. *FRLT Leadership Styles*

Basis for Comparison	Transactional Leadership	Transformational Leadership	Passive-Avoidant Leadership
Meaning	A leadership style that employs rewards and punishments for motivating followers is Transactional Leadership.	A leadership style in which the leader employs charisma and enthusiasm to inspire his followers is Transformational Leadership.	A leadership style that vacillates and allows subordinates room to operate without interference is Passive-avoidant
Concept	Leader emphasizes his relationship with followers.	Leader emphasizes the values, ideals, morals, and needs of the followers.	The leader emphasizes freedom and skills.
Nature	Reactive	Proactive	Consultative
Best suited for	Settled Environment	Turbulent Environment	Poorly defined roles. Feedback and consultation
Works for	Developing the existing organizational culture.	Changing the existing organizational culture.	Independent and carefree.
Style	Bureaucratic	Charismatic	Highly skilled
How many leaders are there in a group?	Only one	More than One	One to Many
Focused on	Planning and Execution	Innovation	Skills and motivation
Motivational tool	Attracting followers by putting their own self-interest in the first place.	Stimulating followers by setting group interest as a priority.	High level and intrinsic motivation

Comparison of the leadership styles. Key differences between transactional, transformation and passive-avoidant leadership. Adapted with permission from Surbhi.

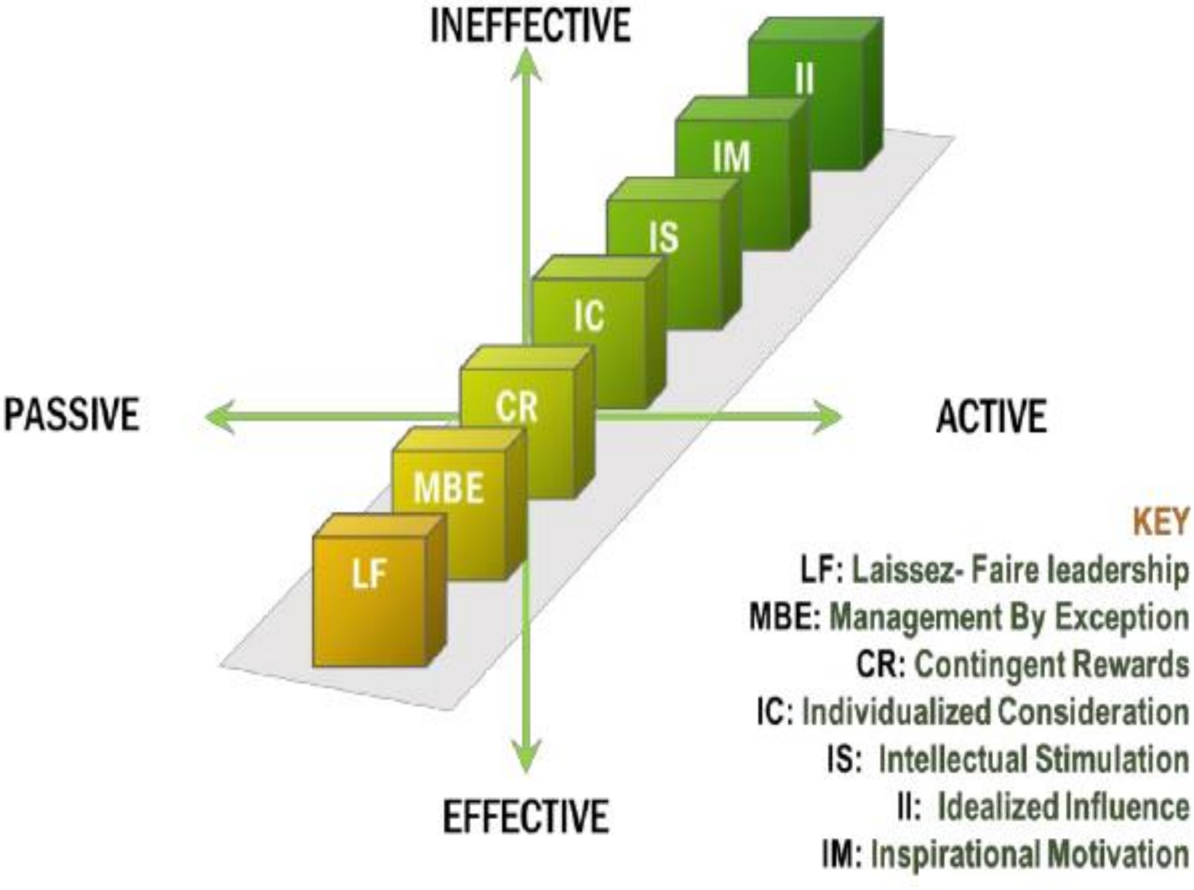
INEFFECTIVE
II
IM
IS
IC
PASSIVE
CR
ACTIVE
MBE
LF
KEY
LF: Laissez- Faire leadership
MBE: Management By Exception
CR: Contingent Rewards
IC: Individualized Consideration
IS: Intellectual Stimulation
II: Idealized Influence
IM: Inspirational Motivation
EFFECTIVE

Figure 2. Schematic-Representation-of-Full-Range-Leadership. With permission from Renjith.

One notable consequence of passive-avoidant behavior is that the leaders that exhibit such behaviors negatively impact the cohesion of the teams they lead (Hinkin & Schriesheim, 2008). In addition to the negative characteristics that earlier scholars have ascribed to passive-avoidant leaders, Salter, Harris, and McCormack (2014) found that there was also a negative correlation between moral reasoning and passive-avoidant leadership. Passive-avoidant leaders do not convey a strong moral identity to their followers. Without the ability to convey a strong moral dimension in communications with followers, a key facet in the process of inspiring and influencing followers is lost.

Avolio (1999) noted that FRLM represents a spectrum of behaviors by leaders and that what is of note is how often a leader exhibits a given behavior. Thus, effective leaders exhibit passive-avoidant (i.e., laissez-faire) leadership behaviors infrequently or in exceptional circumstances. Chaudry and Javed (2012) stated, based on their research, that such exceptional circumstances did exist when passive-avoidant leadership was appropriate. Passive-avoidant leadership was found to yield positive results in circumstances in which team members had an intrinsic motivation (Chaudry & Javed, 2012). Chaudry and Javed (2012) stated that passive-avoidant leadership could be appropriate where team members were highly experienced in their fields and well-motivated. Chaudry and Javed (2012) provided a specific example of scientists as highly experienced and well-motivated professionals.

Despite the potential benefits in some situations, Chaudry and Javed (2012) noted that passive-avoidant leadership was still negatively associated with “motivation toward extra effort” (p. 260). Not all researchers concur that passive-avoidant leadership can have benefits in some situations. Stafford (2010) argued that there were no circumstances in which laissez-faire leadership was a positive leadership quality. Instead, Stafford argued that those circumstances that appeared to suggest passive-avoidant leadership was being used were instances of management by exception (MBE). MBE is a form of transactional leadership.

Research has shown that passive-avoidant leadership has a gender dimension. Seminal research on gender and passive-avoidant leadership demonstrated that male leaders engage in passive-avoidant leadership more often than female leaders (Eagly, Johannesen-Schmidt, & Van Engen, 2003). Eagly et al.’s research has been supported by more recent findings that female leaders are significantly more interested in and concerned about a leader’s integrity than male leaders and they are more sensitive to the diction of passive-avoidant leaders (Green, Duncan, Salter, & Chavez, 2012; Salter, Green, Duncan, Berre, & Torti, 2010). In light of the current gender imbalance in IT leadership, these results suggest that current efforts by organizations to redress this balance are wise (Noland, Moran, & Kotschwar, 2016). Regardless of gender, scholars appear nearly unanimous in finding passive-avoidant, laissez-faire management approaches to equate to ineffective leadership and negative team and organizational outcomes. Table 3 illustrates the relationships of the three styles of leadership and their sub-dimensions with the least effective leadership style, laissez-faire (i.e., passive-avoidant) on the left.

Table 3. *The FRLT Spectrum*

Laissez-Faire	Transactional			Transformational			
Hands-Off Leadership	Management by Exception [MBE]		Contingent Reward	Individual Consideration	Intellectual Stimulation	Inspirational Motivation	Idealized Influence [II]
	Passive MBE	Active MBE	[CR]	[IC]	[IS]	[IM]	

Transactional leadership. Transactional leadership is a style of leadership that focuses on organization and supervision in pursuit of group performance (Odumeru & Ifeanyi, 2013). Scholars sometimes also refer to this style of leadership as managerial leadership (Odumeru & Ifeanyi, 2013). The three distinct factors that characterize variants of the transactional leadership style are (a) passive management by exception (MBE), (b) active MBE, and (c) contingent reward (see Table 3)

The transactional leadership style concentrates on the exchanges between leaders and subordinates in the organization (Bass, 1995; Burns, 1978). Burns (1978) initially proposed the transactional leadership theory basing it on the idea that an employee receives a reward for their acceptance of authority within the organization. Penn (2015) defined transactional leadership as a contract between a leader and followers. Such implicit contracts or agreements are based on performance commitments allowing each party to receive something of value (Tyssen et al., 2014). The transactional leadership approach rewards compliance and punishes nonperformance or noncompliance. Leaders are motivated to achieve the business's goals and objectives, and they are empowered to train, evaluate, and reward subordinates in pursuit of the organization's objectives.

Leaders who follow the transactional approach rely on establishing parameters, guidelines, rules, and standards for performance as well as on extrinsic-based systems of reward and punishment (Dartey-Baah, 2015). A manager implementing the transactional leadership style is a leader who monitors his or her followers' work to ensure minimal deviations in work practices from those established for the given task. Such leaders are responsive to changes in circumstance and focus on task completion, not on the people they lead (Dartey-Baah, 2015).

***Contingent rewards and MBE*.** Transactional leadership rests on two factors. These are MBE, and contingent reward understood as constructive or corrective transactions, respectively (Diaz-Saenz, 2011; Odumeru & Ifeanyi, 2013). Leaders using MBE strive to maintain the status quo, intervening when subordinates fail to perform to expectation. These leaders initiate corrective action when a task or project fails to meet performance goals (Odumeru & Ifeanyi, 2013). Contingent rewards associated with transactional leadership are rewards for accomplishing tasks in a timely fashion (Odumeru & Ifeanyi, 2013). Punishments are assigned when a task is late or not completed as required (Odumeru & Ifeanyi, 2013). Transactional leaders "define and communicate what is done and how it is done, and the rewards and recognition followers will receive if the assignments are performed satisfactorily" (Zhu, Sosik, Riggio, & Yang, 2012, p. 192). Thus, the leader establishes a system of extrinsic rewards as part of the implicit contract between leaders and followers (Dartey-Baah, 2015). Odumeru and

Ifeanyi (2013) noted that such reward systems result in “minimal compliance” from followers (p. 358).

Transactional leadership is a mostly passive style wherein leaders react to events requiring attention as opposed to acting proactively (Odumeru & Ifeanyi, 2013). Overall, transactional leadership divides into two approaches, the first is passive MBE, and the second is active MBE. The following section discusses these two approaches.

MBE Active and Passive. The passive transactional MBE leadership approach waits for problems to arise before applying remedies. Leaders applying this approach seek to maintain the status quo while implementing a wait, and see attitude, and only intervene when errors occur, or a project starts to miss milestones. Active MBE is a micromanagement approach with strict observance of procedures and guidelines to minimize and correct errors and deviations (Odumeru & Ifeanyi, 2013). The leader continuously reviews the tasks assigned to individual workers and adjusts leadership expectations for those tasks as progress is made to ensure subordinates work patterns and behavior follow the leader’s guidelines and rules (Zhu et al., 2012, p. 192).

Transformational leadership. Downton (1973) first introduced the notion of transformational leadership; however, scholarly interest in transformational leadership commenced with Burns (1978). According to Zhu et al. (2012), transformational leadership theory is one of the most commonly used leadership theories in organizational management. Transformational leadership is a style of leadership that is more active than the transactional leadership style and which places a focus on the norms and values of followers (Bedi, Alpaslan, & Green, 2015). Such leadership aims to encourage followers to move beyond their self-interest and move towards a common shared purpose (Bedi et al., 2015). Transformational leadership represents leadership behaviors on the right-hand side of the FRLT leadership spectrum (Avolio & Bass, 2004). Leadership on the right-hand side of the spectrum represents the most effective leadership behaviors identified by Avolio and Bass (2004).

Four factors underpin the transformational leadership style. These are: (a) individual consideration (IC) or caring, (b) intellectual stimulation (IS) or thinking, (c) inspirational motivation (IM) or charming, and (d) idealized influence (II) or influencing (Table 4) (Warrilow, 2012). Table 4 directly below summarizes the four components of transformational leadership.

Table 4. *Transformational Leadership Components and Their Elements*

TFL Components	Elements
Idealized Influence (II)	Being a role model that is highly regarded, valued, trusted, and deserving emulation
Inspiration Motivation (IM)	Encouraging enthusiasm in others through challenge and instilling a sense of significance while promoting cohesion, harmony, and confidence
Intellectual Stimulation (IS)	Kindling creativity and inventiveness by encouraging novel ideas, questioning, and thinking outside the box
Individualized Consideration (IC)	Paying particular attention to the individual needs of each follower

Source: Bedi et al. (2015). A meta-analytic review of ethical leadership outcomes and moderators, permission forthcoming.

Individual consideration (IC) or caring. IC adds a personal dimension to transformational leadership lacking in passive-avoidant and transactional leadership. The individualized dimension of IC provides a follower with support, mentoring, encouragement and coaching (Gholamzadeh & Khazaneh, 2012). Such strategies demonstrate positive results on individual followers. Aggarwal and Krishnan (2013) in an information industry study in India found that the self-efficacy of IT workers was increased by leaders practicing a transformational style of leadership. These increases in self-efficacy, in turn, were related to increases in the quality of work delivered as well as self-confidence (Aggarwal & Krishnan, 2013).

Intellectual stimulation (IS) or thinking. IS is the factor in transformational leadership that measures the degree to which a leader challenges the status quo (Bedi et al., 2015). A leader utilizing the transformational style does so by attempting to enhance followers creative thinking by appealing to followers' intellects and being receptive to creative and innovative solutions (Bedi et al., 2015; Loughlin, Arnold, & Bell, 2011). Such solutions are often referred to by scholars of leadership theory as solutions based on outside-of-the-box thinking (Phipps & Prieto, 2011). Loughlin et al. (2011) conducted research to investigate participative versus directive transformational leadership among Canadian leaders. In this study Loughlin et al. (2011) found that IS as a factor supporting transformational leadership is more likely be enacted by transformational leaders of either gender with participative as opposed to directive approaches to IS.

In the continuously changing field of IT, it is crucial to maintain current expertise in new and emerging technologies (Fitzgerald, 2012). As a result, ongoing education is of disproportionate importance in all disciplines related to IT. Transformational leadership that utilizes IS in encouraging learning has been linked to positively influencing learner's intrinsic motivation (Bolkan, Goodboy, & Griffin, 2011). Such learners are more likely to approach the materials to be learned strategically and learn the materials thoroughly (Bolkan et al., 2011). However, IC and its impact on creativity must be approached with caution; Eisenbeiß and Boerner (2013) found that while transformational leadership increased follower creativity, paradoxically, the dependence followers developed on such leaders, in turn, reduced creativity, this adverse indirect effect thus attenuated the overall positive influence on creativity of transformational leadership (Eisenbeiß & Boerner, 2013)

Inspirational motivation or charming. Inspirational motivation is the factor in transformational leadership that measures the degree to which a leader can create a vision that is at once attractive to followers and which encourages action on their part (Balyer, 2012; Palrecha, Spangler, & Yammarino, 2012; Sadeghi & Pihie, 2012). Inspirational motivation involves leaders who provide optimistic visions of future achievement while also providing meaning and challenge to the tasks they set their followers (Avolio & Bass, 2004; Sadeghi & Pihie, 2012). Furthermore, such leaders display enthusiasm while setting high expectations and exhibiting their commitment to the goals that they set (Balyer, 2012).

Idealized influence or influencing. The fourth and final factor underpinning transformational leadership is II (see Table 4). Leaders who exhibit II are leaders who become role models for their followers (Bedi et al., 2015). To become role models, they evince personal behaviors that induce followers to value and trust them, hold them in high regard and as a result find them worthy of emulation (Bedi et al., 2015; Bellé, 2013).

II comes in two forms; the first is the idealized influence attribute which provided leaders with trust and respect (Sadeghi & Pihie, 2012). The second is idealized influence behavior in which leaders exhibit excellent behavior and a willingness to sacrifice their own needs when necessary to support the objectives of the group (Sadeghi & Pihie, 2012).

Information Security Governance

Cornforth (2003) defines governance formally as “systems and processes that ensure the overall direction, effectiveness, supervision, and accountability of an organization” (p. 79). Von Solms and Von Solms (2009) noted that corporate governance is engaged in directing, planning or establishing responsibilities and concerned with controlling outcomes, ensuring implementation and enforcing compliance. Furthermore, Von Solms and Von Solms noted that risk management was one of the “major responsibilities of Corporate Governance” (p. 4);~~,”~~ they also noted that risk management is core to board level information technology governance (p. ~~4; p.~~9). According to Brotby (2006), information security governance is the responsibility of the board of directors and senior executives. It must be an integral and transparent part of enterprise governance and aligned with the IT governance framework. Von Solms and Von Solms (2009) stated that the board of directors and executive management constituted the strategic level of an organization and that senior and middle management represented the tactical level. Thus, the present study related the strategic, security governance and tactical, IT leadership levels of an organization’s governance and management to the management of information security risk.

Based on the ISO 38500 standard, IS governance is the means by which an organization directs and controls information security. The Information Security Guide (Educause, 2014) stated that the eleven characteristics of effective security governance that was critical for an effective enterprise ISRM program were:

1. It affects the entire institution.

2. There is an accountability culture where leaders are held responsible.

3. It is viewed as an institutional necessity (cost of doing business).

4. It is based on risk.

5. Roles, responsibilities, and segmentation of duties are defined.

6. Policies address it and enforce it.

7. Adequate allocation of resources

8. Staff are conscious and properly trained

9. A development life cycle is required.

10. It is planned, managed, measurable and measured.

11. It is reviewed and audited.

In many instances, IS governance not only must deal with the risks identified by an organization but also those identified by government acts and government regulators. Organizations involved in the US health industry, for example, must ensure that they comply with the security standards mandated by the health insurance portability and accountability act of 1996 (HIPAA). Demonstrating compliance is resource intensive and may cost up to 34% of an organization's IT resources according to the security compliance council (Fitzgerald, 2012).

- Health Information Technology for Economic and Clinical Health Act (HITECH) - 2009

- NERC Critical Infrastructure Protection Cyber Security Standards - 2006

- Payment Card Industry Data Security Standard (PCI) - 2006

- Payment Card Industry Data Security Standard (PCI) - 2006

- HIPAA, Final Security Rule - 2003
- Sarbanes-Oxley Act (SOX) - 2002
- Federal Information Security Management Act (FISMA) - 2002
- Gramm-Leach-Bliley Act (GLBA) - 1999
- Computer Security Act - 1987
- Privacy Act - 1974

IS governance relies on control frameworks and standards to ensure compliance with regulatory requirements and also to be current with relevant best-practice (Fitzgerald, 2012). Significant extant frameworks include: (a) the Control Objectives for Information and related technology (CobiT), (b) the Committee of Sponsoring Organizations of the Treadway Commission (COSO), (c) the IT infrastructure library (ITIL), (d) the Federal Financial Institutions Institutional Examination Council (FFIEC) Handbook, (e) the Federal Information Systems Controls Audit Manual (FISCAM), (f) National Institute of Standards and Technology (NIST) Risk Management Guide and (g) the HITRUST Common Security Framework (Fitzgerald, 2012). These, in turn, are supported by standards such as the ISO/IEC 27001/2:2005 series, ISO 38500, and the NIST recommended controls, 800-53 Revision 3.

Frameworks

COBIT. The COBIT is a control methodology for engaging in IS governance best practices within an organization developed by ISACA, formerly known as the Information Systems Audit and Control Association (Kerr & Murthy, 2013). This framework, positioned at a high level, it has been designed to align both with more detailed frameworks and various standards such as the ISO 27000. Thus, COBIT functions as an integrator of various elements of best-practice and links them to both the business and governance requirements of organizations (de Haes & van Grembergen, 2015).

The COBIT can contribute to regulatory compliance when correctly deployed and integrated with supporting frameworks and components (Luellig & Frazier, 2013). High-quality deployments have also been associated with more efficient information management, increased business agility and lowered overall costs (Luellig & Frazier, 2013).

COSO. COSO was formed in 1985 to support the U.S.-based National Commission on Fraudulent Financial Reporting (i.e., the Treadway Commission) a private sector initiative to delve into the causal factors that may support fraudulent financial reporting (COSO, 2018). COSO was founded, and jointly sponsored and funded by the five main accounting associations and institutes in the U.S. The issues reported on by the Treadway Commission report were taken as the starting point by COSO to develop a common set of definitions of internal controls for organizations as well as an integrated framework for implementing internal controls whose initial version was launched in 2011 (COSO, 2018). Currently, Enterprise Risk Management-Integrating with Strategy and Performance is the most recent iteration of COSO's framework. COSO's framework has become the standard internal controls framework most organizations in the U.S. use and COSO continues to update and expand its framework (Hayne & Free, 2014). Furthermore, COSO is one of the critical frameworks that the COBIT is specifically designed to work with (de Haes, Debreceny, & van Grembergen, 2013).

ITIL. Originally developed for and supported by the UK government and known as the Information Technology Infrastructure Library (Cannon, 2011). The acronym is no longer in use and ITIL is now is now sponsored by AXELOS, a public-private joint venture in the UK. ITIL underpins the ISO/IEC 20000 standard (Cannon, 2011) The ITIL is a collection of five volumes covering standard practices for IT management (Cannon, 2011). These five volumes cover (a) service strategy, (b) service design, (c) service transition, (d) service operation, and (e) continual service improvement. ITIL certification is provided in five tiered levels, exclusively to individuals who have demonstrated a specific level of knowledge, at each level, of the contents of ITIL framework (Axelos, 2018, website). Furthermore, ITIL is one of the frameworks harmonized with the COBIT meta-framework (Fitzgerald, 2012).

FFIEC. Established in 1979 by the U.S. Congress under the Financial Institutions and Interest Rate Control Act (FIRA) of 1978, the FFIEC is a formal U.S. interagency body (FFIEC, 2018 The five senior federal U.S. banking regulators comprise FFIEC's membership. These are (a) the Federal Reserve Board of Governors, (b) the Federal Deposit Insurance Corporation, (c) the National Credit Union Administration, (d) the Office of the Comptroller of the Currency, and (e) since 2011, the Consumer Financial Protection Bureau (FFIEC, 2018). In 2014 FFIEC expressed official concern for the vulnerability of financial institutions to cyber-attacks (FFIEC, 2018). As a consequence, in 2015 the FFIEC released its first cybersecurity assessment tool which when implemented by a financial institution allows it to assess its cybersecurity readiness (FFIEC, 2018). This tool may be used by institutions for self-assessment and also by financial regulators examining an institution (FFIEC, 2018). The FFIEC cybersecurity readiness assessment tool provides a mapping to the NIST cybersecurity framework (FFIEC, 2018; Protiviti, 2016).

Federal Information System Controls Audit Manual (FISCAM). The FISCAM was first issued by the United States General Accountability Office (GAO) in 1999, and a revised version, GAO-09-232G, was issued in 2009. The FISCAM is a methodology to perform information control audits on U.S. Federal entities (GAO, 2009). This methodology meets current professional audit standards and specifically the generally accepted government auditing standards and is compliant with NIST publication 800-53 (GAO, 2009). Furthermore, the FISCAM maps all SP800-53 controls (GAO, 2009). The FISCAM is oriented primarily to fiscal and performance audits in a seven-step process.

Together these seven steps focus on five key areas. These five areas are: (a) security management, (b) access controls, (c) configuration management, (d) contingency planning, and (e) segregation of duties (GAO, 2009). FISCAM is another framework harmonized with the COBIT meta-framework (Fitzgerald, 2012). Finally, FISCAM complies with the Federal Information Security Modernization Act (FISMA) of 2014 (NIST, 2018).

NIST. The National Institute of Standards and Technology (NIST) is a non-regulatory agency of the US Commerce Department. As such, it is responsible for developing IS standards, guidelines, and minimum requirements for U.S. federal government information systems (NIST, 2018). The Federal Information Security Management Act (NIST, 2018) established the agency's responsibilities. The NIST currently publishes five special publications related to IT security and information security risk management. These five guides are Special publications: (a) 800-12, rev. 1, An Introduction to Information Security, which is an overview of computer security and control issues, (b) 800-14, provides high-level descriptions of what should be incorporated in a given security policy and common security principles, (c) 800-37, is a Guide for Applying the Risk Management Framework to Federal Systems, (d) 800-53, rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, and (e) 800-82, rev. 2, Guide to Industrial Control System (ICS) Security which outlines how to secure industrial control systems against cyber attacks (NIST, 2018). The NIST also has several additional documents in draft format, at the writing of the present study, an example of which is, SP 1800-1, Securing Electronic Health Records on Mobile Devices (NIST, 2018).

The first critical guide for federal government entities is the *Risk Management Guide for Information Technology Systems* (SP 800-37). Updated continuously since its first pub.4)lication in 2002, this cyber-security guide’s purpose is to provide risk assessment professionals with fundamental risk management program standards (NIST, 2018). Both for-profit and non-profit organizations often utilize this guide as a foundational document for setting up or updating risk management practices (Albakri, Shanmugam, Samy, Idris, & Ahmed, 2014).

The NIST also publishes a second guide, *Security and Privacy Controls for Federal Information Systems and Organizations* (Special Publication 800-53, rev. 4) published in 2013. This publication provides organizations with a comprehensive catalog of security and privacy controls including a process for selecting which controls apply to an organization (NIST, 2018). A draft of revision five was published in 2017 to solicit input from reviewers and security professionals both nationally and internationally (NIST, 2018). Revision five will focus on adding security controls that are more proactive and comprehensive, and that specifically address issues with such new technologies as ~~:~~ “cyber-physical systems, cloud and mobile systems, industrial/process control systems, and the Internet of Things (IoT) devices” (NIST, 2018).

In addition to the two guides the NIST publishes, the NIST provides federal agencies and all other interested parties with a Cyber Security Framework (NIST, 2018). This framework provides “a common language and systematic methodology for managing cybersecurity risk” and is designed to complement organizations’ existing cybersecurity programs and risk management practices (NIST, 2018). An update of this framework, version 1.1, has proven even more popular than the original version. This new version released in April of 2018 was downloaded over 129,000 times in the four months after its initial release. By comparison, the previous version was downloaded 262,000 times in four years (NIST, 2018).

Two issues have arisen with the NIST as a provider of security frameworks and the cybersecurity framework itself. The first issue is that the NIST is a U.S. governmental organization with a mandatory requirement to consult with such intelligence agencies as the U.S. National Security Agency. The consequence of this is that suspicions can arise that such an agency may build a cryptographic backdoor into the NIST security standards. Such suspicions were raised concerning the Dual_EC_DRBG random number generator in the NIST 800-90A standard. This concern after adverse public commentary resulted in revision 1 of that standard dropping the random number generator critics alleged was provided by the NSA (NIST, 2014).

The second issue explicitly associated with the NIST cybersecurity framework is that while an industry survey of 300 U.S. information security professionals found that 70% of professionals surveyed viewed the framework as security best-practice they also viewed full implementation of the framework as a very high-cost endeavor with 50% believing such cost to be a barrier to adoption (Dimension Research, 2016). Eighty-three percent of professionals surveyed as to their intentions for 2017 stated that they intended to adopt some, but not all, of the cybersecurity framework controls (Dimension Research, 2016). Industry speculation about the reasons for partial adoption related to both high cost and a lack of regulatory pressure for such partial adoption (Dimension Research, 2016).

HITRUST. The Health Information Trust Alliance (HITRUST, 2018) is a U.S. not-for-profit entity created, sponsored and directed by major U.S. healthcare organizations. Its mission is to participate in government advocacy as well as community building and cybersecurity education. HITRUST is of specific interest as it provides a cybersecurity framework to the healthcare industry. This framework, similarly to the COBIT harmonizes and cross-references globally recognized standards such as the EU Regulation 2016/679 and relevant U.S. regulations (HITRUST, 2018). It also integrates healthcare business requirements including ISO, NIST, PCI, HIPAA and State laws (HITRUST, 2018). To support their CSF, HITRUST also provides a web-based risk assessment tool (MyCSF) to assist in framework implementation.

Standards

Cybersecurity of national infrastructure became a concern of the U.S. government by the late 1990s resulting in the U.S. government contracting with Stanford University (2018) to create a consortium for research on information security and policy (CRISP). The research performed by this consortium lies at the root of most modern cybersecurity standards (Stanford University, 2018). High-level standards such as the ISO38500 underpin the security frameworks on which IS governance relies. Technical standards support execution of the directives emanating from IT governance to senior and middle levels of IT leadership. Thus, for senior IT leadership interacting with IS governance on information security governance standards such as ISO 38500, ISO 27001 and DoCRA are of particular relevance. Table 5 summarizes the most important and popularly used cyber-security related standards in current use.

ISO38500:2015. Governance of IT for the Organization (ISO 38500) specifically relates to the activities of the governing body of a generic entity and allows for specific sub-committees of that body to provide for more focused attention to the tasks required for good IT governance (Juiz & Tomey, 2015). The standard was designed to apply to organizations of all sizes public, private and not-for-profit (Smallwood, 2014). Specifically, it supplies guiding principles for the directors of organizations on the most effective, efficient and acceptable used of IT within their given organizations (Smallwood, 2014). As such the standard divides into three major sections: (a) scope, (b) framework, and (c) guidance (Juiz & Tomey, 2015).

ISO/IEC 27001. ISO/IEC 27001 is intended to apply to all categories of organizations, public, private, and not-for-profit. ISO 27001 is specifically designed to outline the requirements for best-practice in implementing information security management systems (ISO, 2018). Information security management systems provide a "systematic approach to managing sensitive company information so that it remains secure" (ISO, 2018). The standard introduces a cyclic model known as the "Plan-Do-Check-Act" (Calder & Watkins, 2015; Susanto, Almunawar, & Tuan, 2011). Susanto et al. (2011) note that the ISO reaches more than 80% of the world's nations and the standard itself is "like a global language in standards and benchmarking" (p. 29) for information security management systems.

DoCRA. Where ISO 38500 and 27001 are primarily supportive of IS governance, DoCRA is supportive of senior IT leadership and IS governance. DoCRA is designed to be industry, profession neutral and regulatory regime neutral. DoCRA provides IT leadership and IS governance a standard risk analysis method aligned with both regulatory and judicial expectations for the demonstration of due care taken by an organization's provision of reasonable and appropriate safeguards (DOCRA, 2018). Thus, application of a DoCRA duty of care risk analysis allows organizations to identify risks that can affect all parties that potentially may be affected by the identified risks. Thus, A DoCRA risk analysis, helps organizations determine whether they apply safeguards that appropriately protect others from harm while presenting a reasonable burden to themselves (Docra, 2018). Whereas ISO 27001 and 38500 primarily focus on an organization's risks to itself and its own goals, DoCRA focuses on the potential liabilities that an organization generates by its activities that are external to the organization.

Table 5. National & International Cyber-security Related Standards

Standard	Purpose
ISO 38500	Standard for corporate governance of IT
ISO/IEC 27001 & 27002	Information security management system standards. ISO27001 brings information security under specific management control. ISO 27002 is good security management practices
ISO/IEC 21827	Standard for measuring the maturity of ISO controls objectives
CISQ	Develops standards related to software structural quality and size for the Object Management Group
DoCRA	Authors maintain and distribute methods and standards for managing and analyzing risk
ISF Standard of Good Practice	Regularly updated and comprehensive list of best practices
ISO 15408	Sets a common criteria for hardware/software integration and secure testing
RFC 2196	Security policies and procedures for information systems connected to the internet
ANSI/ISA 62443 (formerly ISA-99)	Multi-industry standards for cybersecurity protection methods and techniques, specifically for industrial automation and control systems
IASME	UK-based information assurance standard for SMEs

Information Security Risk Management

Information security risk management (ISRM) is the process of managing IT technology-related risks. Identification of IT security risks is the first step in a process that includes assessing and then addressing risks to an organization's availability and maintenance of the integrity of organizational assets as well as the confidentiality of its data (Wheeler, 2011, p.8). Dearfield, Hoelzer, and Kause (2014) noted that ISRM involves communication of risks organizationally as well as their assessment and management.

ISRM operates in the context of what level of risk an organization's IS governance is willing to accept in the broader context of an organization's overall business goals. To facilitate this ISRM is both bounded and defined by the risk management frameworks that IS governance and senior IT leadership have put in place for an organization (Wheeler, 2011; ISACA, 2018).

Present practice concerning ISRM has come to rely on IS governance and IT leadership choosing parts or all of one or more security frameworks appropriate to their industry or economic sector as noted in previous sections. However, there is no one solution for managing IS risk that fits all organizations, particularly as the risks facing organizations continue to evolve quickly (Wheeler, 2011). As a result, some practitioners and scholars are noting that a check-list mentality or approach to ISRM itself can create managerial blind-spots and that the management of information security risk should focus on the business drivers that justify any given control or mitigation strategy (Fitzgerald, 2012; Wheeler, 2011). NIST SP800-37 launched in 2011 was the first NIST guideline to recognize this phenomenon as a security issue itself (Wheeler, 2011). Ultimately, the goal of IS governance and IT leadership in implementing ISRM programs is to maximize an organization's output while minimizing its risk profile internally and externally as reflected by the latest DoCRA standards (DoCRA, 2018; Wheeler, 2011).

Findings

The research findings clearly illustrate that current best practice rests heavily on complying with the prescriptions embodied in the various security frameworks that have been published and updated in the last fifteen years. These frameworks rest on equally new standards, and both standards and frameworks frequently reference each other. Excellent exemplars of this phenomenon are both the COBIT and HITRUST frameworks as previously noted.

The rise of a multiplicity of comprehensive security frameworks and related standards may be creating a new security issue in that it has started to create a framework compliance culture among IS professionals (Fitzgerald, 2012; Wheeler, 2011). This phenomenon was already starting to be noted as early as 2010 by the NIST and reflected in its revision to SP800-37 as well as by Wheeler (2011) who warned that relying on check-list type security procedures and existing best-practice was not a substitute for policies specific to the risks an organization faces in the real world.

Revision cycles for standards and frameworks appeared to be short, often no more than two or three years between revisions. For example, the NIST SP 800-53 security and privacy controls for information systems and organizations framework launched in February of 2005 were already in revision four by 2013 and the comments period for revision five closed September 12, 2017 (NIST, 2018). This rapid revision cycle suggested to the researcher that existing security frameworks and standards were in too many instances immature and merely attempting to stay current with fast-changing ISRM realities rather than pro-actively addressing future organizational risks. As specific evidence of this observation, the upcoming revision 5 of the NIST SP 800-53 frameworks states explicitly that the new revision will attempt to make systems both resilient and survivable, in other words, able to survive new forms of attack (NIST, 2018). Furthermore, according to the NIST that while the new revision needs to be systematic, it also notes that it must be proactive in its approach to creating information security safeguards (NIST, 2018).

The research findings showed a clear trend since the late 1990s and the pioneering work of CRISP at Stanford University. This trend was reflected by the rapid increase in the number of formal security standards and frameworks available since the late 1990s, their increased inter-relationships and the high-intent among IS security professionals to deploy and utilize security frameworks and standards. The NIST cybersecurity framework and the ISO27001/02 series stood out as leading exemplars of the most deployed frameworks and standards (NIST, 2018). The DoCRA due care standard is an indicator of how the awareness of the need to manage information security risk has led to an awareness of the impact of the consequences of information security breaches on stakeholders and third parties. This with particular emphasis on the legal consequences of security breaches that occur due to a lack of due care.

As previously noted the literature makes clear that implementing best practices in ISRM on a check-list or simple compliance basis is no longer enough (Wheeler, 2011). Furthermore, cherry-picking (often based on cost) the parts of security frameworks such as the NIST cybersecurity framework to comply with is increasingly questionable practice (Dimension Research, 2016). A result of the above issues is an increased awareness by scholars, regulators, and practitioners of the need for more proactive security practices to be built into security frameworks and standards.

Much of the need for continual revisions to security frameworks and standards is due to the rapid evolution of security threats to organizations (Wheeler, 2011). However, choices as to what security frameworks and related standards an organization ought to embrace and deploy is an issue of governance. Thus, it is senior IT leadership and IS governance at board level and the level of the executive management of organizations who must continually confront making new and critical decisions as to what frameworks and associated standards they will discard as obsolete or embrace as currently relevant or, necessary going forward.

In light of the above, the literature makes clear that strong leadership is paramount at the governance levels of organizations due to an ongoing need for governance to make critical choices in the management of IS risk (Mahy, Ouzzif, & Bouragba, 2016; Tu & Yuan, 2014). As threats continually evolve and more proactive approaches to ISRM are becoming a necessity, strong leadership must itself be proactive and not reactive (Mahy et al., 2016). Due to the multiplicity and heterogeneity of threats as well as the fact that many threats originate within organizations (Jouini, Rabai, & Aissa, 2014) leadership that inspires follower buy-in to leadership's security goals appears to be increasingly necessary going forward. However, a review of the current scholarly literature demonstrates a paucity of current research on the inter-relationships between information technology leadership, IS governance and ISRM and highlights the need for a better understanding of the effects of IT leadership styles and IS governance on IS risk management in U.S. organizations.

Critique of Previous Research Methods

Previous scholarship has established the importance of the dimension of governance to ISRM. The present study examines IT leadership and IS governance and their relationship with ISRM. The theoretical framework of analysis the present study utilized was the FRLT. As with all current theories of human leadership, the FRLT has both strengths and weaknesses. The following two sections discuss first the strengths and then the weaknesses of the FRLT as a theory of leadership.

Strengths of FRLT

The greatest strength of the FRLT is its explanatory power and the fact that the theory has been supported and validated in nearly all of its aspects (Avolio, 2011). Strong scholarly validation of the FRLT and its proven explanatory power, in turn, explain why the FRLT continues to have high rates of utilization by scholars of leadership. Due to the nearly continuous change that the IT field experiences and particularly those areas of IT related to ISRM, scholars and practitioners increasingly link effective IS risk management to the proactive application of risk management strategies (Wheeler, 2011). Hence, passive IT leadership or IS governance is not an option for organizations wishing to maintain sustainable ratios of IS risk accepted versus organizational output. Thus, the FRLT which accounts for a broad spectrum of leadership behaviors but explicates those transformational (i.e., proactive) leadership behaviors most likely to support organizations in times of sustained change is particularly appropriate in examining the relationship of IT leadership and IS governance to ISRM.

While all four dimensions, IC, IS, IM, and II, are critical components in the making of a transformational leader some dimensions are of particular importance in term of the type of leadership required to maintain IS security. The most critical dimension is IS or thinking. Furthermore, scholars state that outside-of-the-box is an essential component of IS (Phipps & Prieto, 2011) and as such is key to leading staff in proactive threat avoidance and minimization behaviors by encouraging staff to both anticipate and prevent new threats to an organization.

IM and II are also highly relevant in an environment of continuously evolving threats. IM allows the leader to provide meaning and challenge to the tasks IS security managers undertake. II encourages followers, in this case, IS security managers to emulate leaders who have become role models (Bedi et al., 2015).

Weaknesses of FRLT

According to Northouse (2018), one of the weaknesses of transformational leadership is a lack of clarity. This lack of clarity is due to the multiplicity of dimensions (IC, IS, IM, and II) and resultant goals a transformational leader appears to need to accomplish. Another difficulty with the transformational and transactional theory is that it appears to give little support for the functions of leadership related to strategic and work facilitation (i.e., those functions that Antonakis & House (2013) termed instrumental leadership). Antonakis (2012) performed empirical research that suggests that the transformational-transactional leadership model requires an extension to allow inclusion of instrumental leadership. Furthermore, Antonakis and House (2013) noted that no longitudinal studies were establishing that transformational leaders to transform individuals and organizations.

Another early but still relevant criticism leveled at transformational leadership in past has been that such leadership while effective has no moral dimension and such leaders can as easily lead followers to negative ends as positive ones (Stone, Russell, & Patterson, 2004; Yukl, 1989). Indeed, these criticisms drove theoretical offshoots of the transformational leadership theory such as authentic leadership and ethical leadership (Antonakis & House, 2013). Nonetheless, the fundamental criticism of the potential risks a non-authentic and non-ethical transformational leader poses remains intact and appears rooted in the human condition. Finally, within three years of co-proposing the FRLT, Bass (1997) noted that transformational leadership could in some circumstances lend itself to amoral self-promotion as it makes use of impression management.

Weaknesses/Strengths of FRLT Scholarship

A perceived weakness of all the FRLT scholarship over the past 25 years was the relentless focus on the leader and lack of explication of the properties of good followers or the act of following. Northouse (2018) noted this deficiency in the literature and recommended that more researchers examine followership. The researcher is of the belief that no theory of leadership can ever have full explanatory power until there is a solid understanding of how a given style of leadership interacts with followership. Finally, the researcher has noted the ongoing debates in the scholarly literature of leadership as to how to precisely define what the word transformational means in the context of the FRLT. In common with scholars such as Antonakis and House (2013), the researcher is of the belief that due to the ongoing usage by many scholars of the FRLT that reification of the term transformation is an increasingly urgent necessity to underpin further scholarship related to leadership, particularly leadership as understood by the FRLT.

Summary

The present study's review of the literature has verified the validity and explanatory power of the FRLT and its enduring popularity with scholars of leadership theory due to its explanatory power. The FRLT has a good fit with the specific IT and IS leadership needs of organizations as it addresses specifically behavioral traits such as encouraging the ability for followers to think outside of the box and to think regarding the organization's broader interests. This type of thinking is increasingly important due to the omnipresence and rapid evolution of IS security threats to organizations.

As a result of the rapid evolution of IS security threats security frameworks and standards have become increasingly prominent parts of the IS security puzzle since the millennium.

Furthermore, IS governance often reflected by organizations' appointing CIO's reporting to boards or appointing CIO's to the boards themselves has become a crucial part of overall IT strategies and a vital part of organizational governance. In turn, IS governance is a large part of IT leadership at the level of organizational boards in the current threat environment. This presence of IS governance at board level is essential as both threats and response to threats reflected in security frameworks and standards and their rapid evolution highlight the need for strong and proactive leadership on IS security risk management. Due to this rapid and recent evolution of both threats and responses, there is a gap in the literature as to precisely how IS governance and IT leadership relate to both each other and to ISRM as well as what leadership styles might be most suitable in the current environment. Whereas Chapter 2 provided the necessary context for the present study, Chapter 3 presents the methodology utilized by the current study in detail.

CHAPTER 3. METHODOLOGY

Purpose of the Study

The purpose of this quantitative, non-experimental descriptive study was to examine the effects of IT leadership and IS governance on IS risk management in US organizations. This chapter discusses research design, methodology, sample, data collection, analysis, instruments and measures, validity and reliability, and ethical considerations. The research design details the research methodology that was utilized as part of this study and addresses the research questions. The chapter begins with a presentation of the research questions and hypotheses.

Research Questions and Hypotheses

This research was designed to examine the relationships between IT leadership styles, IS governance, and IS risk management in U.S. organizations. The study was guided by an overarching research question that asked:

Overarching Research Question: To what extent are IT leadership style and IS governance related to IS risk management in U.S. organizations?

This question was answered by testing the following set of hypotheses:

H_0O: There is no statistically significant relationship between IT leadership styles, IS governance, and IS risk management in U.S. organizations.

H_aO: There is a statistically significant effect between IT leadership styles and IS governance on IS risk management in US organizations.

The overarching research question was also investigated by asking two specific subquestions. The subquestions and their corresponding hypotheses were as follows:

Subquestion 1: To what extent are IT leadership style and IS governance individually related to IS risk management in U.S. organizations?

$H_0$1: There are no independent, statistically significant relationships between IT leadership styles, IS governance and IS risk management in U.S. organizations.

H_a1: There are independent, statistically significant relationships between IT leadership styles, IS governance and IS risk management in U.S. organizations.

Subquestion 2: To what extent does IS governance mediate the relationship between IT leadership style and IS risk management in U.S. organizations?

$H_0$2: IS governance does not significantly mediate the relationship between IT leadership style and IS risk management in U.S. organizations.

H_a2: IS governance does significantly mediate the relationship between IT leadership style and IS risk management in U.S. organizations.

Research Design

The design of a study discusses the problem statement and includes other pertinent components of the study. Patton (2002) posited that sound design is essential and necessary to guide research. A research design serves as an initial framework based on previous research (Vaast & Walsham, 2013). An appropriate research design is fundamental to a researcher's ability to conduct a valid study.

This study used the quantitative, non-experimental design to examine the relationship between the independent and the dependent variables. Researchers use quantitative research to clarify a phenomenon by gathering measurable information that can be examined using numerical techniques (Creswell, 2014; Muijs, 2010). When variables in the research are not manipulated, modified, or controlled, the approach is characterized as non-experimental (Swanson, & Holton, 2005).

The present study sought to explore human conduct related to IT leadership style, IS governance and IS risk management. Specifically, the study tested the statistical significance of the associations between IT leadership styles (i.e., transactional, transformational, and passive-avoidant), IS governance and U.S. organizations' use of an IS risk management framework. IT leadership style functioned as an independent variable, IS governance served as a mediating variable, and level of use of the ISO/IEC 27001/27002 standard for risk management functioned as the dependent variable.

This study used a deductive framework for the variables and research questions based on theory. This study sought to determine the nature of the relationship between the independent and the mediating variables (Gbenle, 2013) and then tested the influence of those variables on the dependent variable. The design examined and provided results that contributed to the existing literature on relationships between IT leadership and IS governance and their impact on IS risk management.

Data were collected through the use of a survey instrument. The purpose of this descriptive study was to explain the relationships between the variables based on observations drawn from the participants' survey data. This approach is consistent with existing studies in the literature which note that the goal of descriptive statistics is to explain phenomena (Gall et al., 2007; Nassaji, 2015). The research study produced results that relate to the effects of IT leadership and IS governance on IS risk management practices. Data were collected at a single point in time from IT industry professionals working in U.S. organizations. Due to the use of the statistical approach, the variables required quantitative analysis to extrapolate findings from the sample to the broader population.

Target Population and Sample

The following sections introduce information on the population of interest in this study and the sampling strategy. First, the characteristics of the target population are described. Second, the sampling strategy, the sample characteristics, and the inclusion/exclusion criteria are discussed. Third and finally, the power analysis used to determine the minimum sample size is presented.

Population

The population included individuals working in senior management positions in establishments and agencies responsible for IT administration. This study included senior IT leaders with a range of titles including Chief Information Officer (CIO), Chief Information Security Officer (CISO), Director of IT, and IT Manager. This population is characterized by extensive knowledge of IT and IS issues, and these individuals are generally responsible for directing an organization’s approach to IS risk management.

The U.S. Bureau of Labor Statistics (BLS, 2018) noted that there are approximately 367,600 individuals in the US working as IS managers, directors, or CIOs. The BLS characterizes this population as individuals responsible for planning, coordinating, and directing IT and IS-related activities. Typically, these individuals have at least five years’ experience in IT or IS (BLS, 2018). The BLS (2018), anticipated that the number of these positions is expected to increase by 12% between 2016 and 2026. This growth rate is 5% faster than the expected growth rate in other occupations.

Sample

When conducting a study, one important consideration is the type of individuals that will be included in the sample and the required number to adequately explore the issues being examined (Sarantakos, 2013). To effectively draw a sample from the target population, the researcher must decide on the specific characteristics that are necessary to ensure the sample is representative. To do this, typically inclusion and exclusion criteria are used. The inclusion criteria for this study required that individuals fit the following parameters:

- Participants were required to work in U.S. organizations in the IT industry.
- Participants were required to hold senior management positions. This meant that participants held the title of CIO, CISO, Director of IT, or IT Manager.
- Participants were required to be between the ages of 21 and 65 years of age.

In addition to using the inclusion criteria, the researcher also utilized exclusion criteria to ensure that individuals that did not accurately represent the population were not included in the study. The following exclusion criteria were used to eliminate potential participants that were not representative of the study’s population:

- Participants working in organizations outside the US were excluded.
- Participants working in US industries other than the IT industry were excluded.
- Participants that did not hold senior management positions or have the titles of CIO, CISO, Director of IT, or IT Manager were excluded.
- Participants younger than 21 and older than 65 years of age were excluded.

These inclusion and exclusion criteria increased the likelihood that the sample was representative of the target population. The participants were selected from a sample frame provided by Survio Cint, an online market research organization that specializes in providing research participants for similar studies.

The sampling technique and sample size were selected as they played the leading role in the research. Specific demographic information on participants' age, job role, gender, technical expertise, and level of education was collected and analyzed to help characterize the sample. The sampling method employed in this study was random sampling technique. The recruitment and sampling strategies were selected based on methods used in previous research (Gbenle, 2013; Luftman, 2003). The sampling procedures are discussed later in this chapter.

Power Analysis

The researcher used G*Power 3.1.9.2, a statistical analysis software, to calculate the sample size in this study. The minimum sample size generated by the G* Power analysis was 160. This calculation was based on an effect size of .3 and an error probability of .01. The minimum required sample size of 160 was also based on a 95% confidence level based on the statistical examination using G*Power analysis.

Procedures

In this section of the chapter, the procedures used to conduct the study are explored. First, procedures used to select participants for the study are examined. Next, procedures used to protect participants are presented. The procedures used to collect data are discussed next, and the final subsection outlines the data analysis procedures used to test the study's hypotheses.

Participant Selection

Participant selection began with the process of calculating the appropriate sample size and identifying the population, sample frame, and sample characteristics of interest. The researcher chose to use Survio Cint to provide the sample frame, as this allowed the researcher to easily access a group of individuals that were willing to participate in research. The use of an online survey company also enabled the researcher to ensure that the participants were representative of the target population.

Survio Cint facilitated the sampling process, and a random sampling technique was used to limit the chance of bias in the data. The researcher provided Survio Cint with the study's inclusion and exclusion criteria, and Survio Cint used that information to filter their participant database and exclude any individuals that were not representative of the target population. Survio Cint then sent an email invitation to randomly selected individuals in this sample frame.

The email provided individuals with information on the study and directed them to the survey via a link to a webpage. The survey was hosted on Survey Monkey's website, and interested participants were able to visit the link and complete the survey. The sampling process yielded more than the minimum number of participants needed to conduct the study.

Protection of Participants

Several steps were taken to protect participants throughout the study. The researcher intentionally adopted methods that allowed participants to demonstrate autonomy, guaranteed anonymity, and reduced risk to participants. Survey Monkey and Survio Cint removed all personally identifiable information that can be used to trace or identify the participants or organization. These measures were taken to ensure that participants' privacy and anonymity were protected at all stages in the study. Names, email addresses, locations, and IP addresses were anonymized before any information was given to the researcher. To further protect participants, the researcher stored the survey data on a fully encrypted flash drive in the researcher's home office. Access to data was restricted to authorized personnel such as the dissertation committee members, the Capella University's Institutional Review Board (IRB), and the researcher. The finished questionnaires were downloaded and transferred to the researcher's computer in the home office after Survey Monkey and Survio Cint collected the data. Following the completion of the study, the researcher sent requests to Survey Monkey and Survio Cint administrators to delete all the relevant account information.

Data Collection

Data collection was accomplished using the Survey Monkey service to gather responses from participants. The objective was to collect a minimum of 160 completed surveys. Data collection began when Survio Cint sent invitation emails to potential participants directing them to a link on Survey Monkey's website. Survey Monkey hosted the survey and facilitated the data collection. Participants visited Survey Monkey's website, read and virtually signed the informed consent document, and then were directed to the survey instrument. Participants answered a total of 34 questions, and when they had finished the survey, they were directed to a page that thanked them for their contribution in completing the survey. Participants were allowed to end their participation at any point in the process. The survey remained open and available to Survio Cint members until the required number of completed surveys had been obtained.

Data Analysis

The information gathered was examined utilizing SPSS (Statistical Package for Social Researchers) version 24.0. The responses to the individual scales were tested and validated using Cronbach's alpha reliability coefficients to determine the internal and external reliability and validity (Och Dag & Storberg-Walker, 2014; Swanson & Holton, 2005). This study also utilized percentages, frequencies, correlation, and multiple linear regression to analyze the data. Ritchey (2008) noted that percentages and frequencies are generally used to describe categorical variables. This study used correlation to assess the bivariate relationships between IT leadership style and IS governance and IS risk management measured by the use of ISO/IEC 27001/27002 framework. A multiple regression analysis was then utilized to determine the strength of the correlation, effect size, and error probability. The regression analysis allowed for the integration of the forced entry method. This method required that the independent and mediating variables be entered into the model simultaneously for hypothesis testing. These data analysis procedures allowed the researcher to investigate the level of the relationship between IT leadership styles and IS governance and to predict their effects on IS risk management.

Instruments

Three instruments were combined to collect data on IT leadership style, IS governance, and IS risk management. The instruments were the MLQ-5x, the SAMM, and the ISO/IEC 27001/2. The following sections introduce the instrument and provide psychometric data regarding validity and reliability.

Multifactor Leadership Questionnaire (MLQ-5x)

The MLQ-5x was the first of the instruments utilized to collect data and was initially developed by Avolio and Bass (2004) to support their FRLT theory. The MLQ-5x was an instrument specifically designed to capture and measure a full range of leadership behaviors both in laboratory and field research. These leadership behaviors would be examined in the dimensions of performance and leadership style. The MLQ-5x created a spectrum of leadership styles with the least effective, the passive-avoidant leadership style on the left side of the scale, the transactional occupying values on either side of the middle of the scale, and transformational leadership, the most effective style occupying the right-most areas of the spectrum. The MLQ-5x is a well-established instrument, and previous studies support the continued use of the instrument (Avolio, 2011; Taylor, Psotka, & Legree, 2015).

The MLQ-5x and its predecessor variants are very frequently used in research studies related to leadership (Hargis et al., 2011; Taylor et al., 2015). The instrument has become the standard instrument for assessing transactional and transformational leadership styles (Avolio & Bass, 2004). The instrument is well supported (Avolio, 2011) and has been used in hundreds of

Table 6. MLQ Full Range Leadership Style Behaviors

Transformational Leadership	Transactional Leadership	Passive/Avoidant Leadership	Outcomes of Leadership
Idealized Attributes	Contingent Reward	Management by Exception (Passive)	Extra Effort
Idealized Behaviors	Management by Exception (Active)	Laissez-Faire	Effectiveness
Inspirational Motivation			Satisfaction
Intellectual Stimulation			
Individualized Consideration			

From Multifactor Leadership Questionnaire, 3rd Edition, Manuel and Sample Set, by Bruce J. Avolio and Bernard M. Bass, Copyright 2004, by Mind Garden, Inc. Reprinted with permission.

studies that measured leadership thus demonstrating its applicability for use in the present study. The instrument itself was purchased for use in the present study from Mind Garden (2016). The MLQ-5x includes 36 questions, nine of which were utilized in the present study to examine aspects of the three leadership styles. Table 6 presents the behaviors associated with the MLQ leadership styles.

Validity. Researchers have validated the MLQ-5x in multiple studies. The original MLQ, as created by Bass and Avolio (1997), provided robust evidence for validity. In the original validation, both discriminatory and confirmatory factor analysis was utilized, and factor validity was verified utilizing factor analysis. Antonakis, Avolio, and Sivasubramaniam (2003) further validated the model in a study with 1089 female and 2279 male participants. In this study utilizing the MLQ-5x, they used a nine-factor model and found that the model was stable within homogeneous contexts. Antonakis et al. (2003) noted that the same constructs were validly measured in both the male and female groups, an important desideratum for the present study in which over 40% of participants were female.

Reliability. The MLQ-5x has psychometric properties reflective of the utilization of a pre-specified structure analysis that supports overall goodness of fit. The reliability of the three leadership components of the FRLT (i.e., transformational, transactional, and passive-avoidant) is high. The alpha coefficients for the three components range from .74 to .94. Thus, the scale’s reliabilities are high and appear to measure each style’s components as well as exceeding standard cutoffs for internal consistency. The MLQ-5x utilizes an established confirmatory factor analysis based on structural equation modeling with values of .9 for both overall goodness of fit and the confirmatory fit index value (Bass & Avolio, 1997). The questionnaire’s root mean square error of approximation values closely approximate the suggested .05 level (Bass &

Avolio, 1997). The above values reflect why the MLQ and its variants are considered very reliable.

Strategic Alignment Maturity Model (SAMM)

Luftman's (2003) SAMM was chosen for the present study as unlike previous models that attempted to examine IT and strategic business alignment in organizations the SAMM not only includes descriptive elements, as previous models did, but also prescriptive elements (Luftman, Dorociak, Kempaiah, & Rigoni, 2008). A part of the SAMM scale was utilized to measures factors related to IS governance. The factors that were specifically examined utilizing the SAMM were: governance, the constructs of governance, partnership, scope and architecture, competency/values and skills maturity. Luftman (2003) was the originator of the SAMM and the researcher secured permission from Luftman to use a modified version of the model. The SAMM model is intended to capture the factors that drive coordination of an organization's IT activities with an organization's goals to ensure that activities within the organization are adjusted to meet business contingencies (Luftman, Lyytinen, & ben Zvi, 2015).

Validity. Luftman (2003) initially established the validity of the SAMM in a pilot test performed on 153 IT business executive at major global 2000 companies. Luftman et al. (2008) performed a structural equation modeling analysis to further validate the SAMM. Subsequent researchers have used the SAMM. Thus, the SAM was deemed valid for use in the present study.

Reliability. The SAMM has an acceptable good fit index in support of its psychometric properties. The fit values that support the good fit index are all either better than or meet their minimum threshold values. The SAMM was assessed utilizing Cronbach's alpha coefficient as well as average variance extracted and composite factor reliability. Each of these tests for coefficient and composite reliability exceeded the recommended value of 0.70. Case study research in 2000 and 2004 further confirmed reliability by demonstrating that the SAMM accurately reflects alignment in modern organizations (Avison, Jones, Powell, & Wilson, 2004; Cooper, Watson, Wixom, & Goodhue, 2000).

ISO/IEC 27001/2

Disterer (2013) noted that ISO 27001/2 is an instrument that measures the creation and execution of information security within organizations. Before data collection the researcher obtained permission from the ISO/IEC 27001/2 to use the survey instrument. The study received approval from the Capella University Institutional Review Board (IRB). The effectiveness of IS risk management is essential for the survival of organizations. Tu and Yuan (2014) noted that the ISO/IEC framework identifies critical success factors that help with the successful implementation of IS risk management in organizations. Disterer (2013) noted that there had been a gradual annual increase in the number of ISO 27000 certifications by businesses globally. The ISO 27001/27002 framework focuses on security implementation and supports the creation and operation of an effective IT security plan. ISO 27001/27002 as a governance framework supports IS risk management, and it is being adopted by establishments to build an overall IT governance framework.

The International Organization for Standardization uses the ISO/IEC 27001/2 to survey organizations each year to compare certification rates to ISO management standards use (ISO, 2018). According to McGhee (2008), an instrument's validity can be established through consistent use in previous research, as that use indicates the instrument was tested, measured, and deemed reliable for use in subsequent research. While the ISO has not openly shared the process for designing and validating the instrument, the Cronbach alpha coefficient for ISO 27001/27002 has been reported to be 0.929, which is considered to be excellent (see Field, 2013). Scholars have also noted that the instrument demonstrates exhibit inter-rater/observer reliability (McGhee, 2008; Nykänen, & Hakuli, 2013). As a result, the researcher deemed the instrument valid and reliable for this study.

Ethical Considerations

Ethical considerations are an essential component of scholarly research, and the present study was guided by principles outlined in *The Belmont Report* (U.S. Department of Health & Human Services, 1979) as well as guidelines provided by Capella University's Institutional Review Board (IRB). Ethical consideration in research arose principally due to the concern for the tradition of the integrity of scientific practices and societal need for ethics (Stilgoe, Lock, & Wilsdon, 2014). The development of ethical standards in research is a massive benefit to society. Ethical consideration is very crucial in the research design process, and many of the processes used in the present study were selected based on the traditions modeled in past studies.

The Belmont Report advised that it was necessary to follow the principles of respect, beneficence, and justice when conducting research that involves human subjects (McFadzean et al., 2011). Sarantakos (2013) offered the following list of actions researchers should take to ensure their work is conducted ethically:

- Maintain objectivity
- Uphold professional integrity
- Demonstrate responsibility, competence, and propriety
- Gather and analyze data accurately
- Employ relevant methodologies

- Interpret data appropriately and without intentional bias
- Report data honestly and precisely
- Avoid fabrication or falsification of data and/or results

During the present research, the researcher considered these ethical guidelines and acted accordingly to ensure the study was conducted ethically and to the highest standard of ethics.

Summary

This non-experimental, descriptive study was designed to examine the effects of IT leadership and IS governance on IS risk management in US organizations. This chapter illustrated the central methodology utilized in this study. Information was presented on the research design, the population and sample, the data collection and analysis procedures, the instruments used to collect the data, and ethical considerations that guided the research. Chapter 4 presents and discusses the results of the study's data analysis.

CHAPTER 4. RESULTS

Background

The purpose of this quantitative, non-experimental descriptive study was to examine the effects of IT leadership and IS governance on IS risk management in U.S. organizations. This chapter details the results of the study according to the research design and methodologies described in Chapter 3. Chapter 4 starts by providing background information on the study and analysis process. The next section presents the characteristics of the sample. A detailed presentation of data analysis in relation to the study's research questions follows. The chapter concludes with a summary.

This study was guided by an overarching research question and two subquestions:

Overarching Research Question: To what extent are IT leadership style and IS governance related to IS risk management in U.S. organizations?

Subquestion 1: To what extent are IT leadership style and IS governance individually related to IS risk management in U.S. organizations?

Subquestion 2: To what extent does IS governance mediate the relationship between IT leadership style and IS risk management in U.S. organizations?

The Statistical Package for Social Sciences (SPSS v. 24) was used to conduct both a descriptive and inferential statistical analysis. The descriptive statistics made use of exploratory data analysis (see Trochim, 2006; Trochim, Donnelly, & Arora, 2016) while the inferential statistical analysis utilized multiple linear regression, bivariate correlation, and linear regression analysis (see Field, 2013). The researcher tested four sets of hypotheses and described the association between the independent and the dependent variables. The intent of this quantitative non-experimental descriptive study was to evaluate the effects of leadership styles and IS governance on IS risk management effectiveness in U.S. organizations.

This study assessed three IT leadership styles (i.e., transactional, transformational, and passive-avoidant) to identify their collaborative strength when working with IS governance and risk management. IS governance practices include six IT/Business alignment maturity principles: (a) communications, (b) competency and value, (c) governance, (d) partnership, (e) scope & architecture and skills, and (f) IS risk management. These practices are important as they govern the management and protection of information assets, requiring the adoption of a more holistic methodology (Soomro, Shah, & Ahmed, 2016). Such a holistic approach results in better managerial practices and more effective IS management (Phillips, 2013).

Description of the Sample

The target population for this study consisted of senior IT leaders such as Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), Directors of IT, and IT managers. These individuals possess leadership skills and knowledge of IS risk management. To ensure that the sample was generalizable to the target population, only individuals working in these positions in U.S. organizations were invited to participate. The researcher excluded respondents below the age of 21 to ensure individuals had an appropriate level of experience. Additionally, participants were required to have a minimum of 10 years of experience working in the IT field. The researcher excluded individuals over 65 years of age and individuals that did not work for a U.S. organization.

Two online research companies, Survey Monkey and Survio Cint, facilitated the participant selection and data collection processes. Survey Monkey hosted the web-based survey used to collect the data, and Survio Cint provided the sample frame and orchestrated the participant selection. The sampling technique and sample size were selected to increase the validity and reliability of the research and limit the possibility of bias. The study utilized a random sampling technique. Specific demographic data such as age, job role, gender, technical expertise, and level of education were analyzed to provide a better understanding of the sample's characteristics.

The original dataset consisted of 263 cases. Among these cases, 13 participants did not provide valid data relevant to their leadership style. In the MLQ section of the survey, participants were allowed to avoid questions they could not answer. Avolio and Bass (2004), the creators of the MLQ, recommended this approach. In the statistical analysis of survey data, Allison (2002) argued for the casewise removal of missing data prior to analysis. As a result, the researcher eliminated the 13 cases with missing leadership style data from the dataset. This decision reduced the dataset to a final sample size of 250 cases.

Table 7 presents the descriptive information on the sample. As indicated in Table 7, just over half of the sample was between the ages of 31 and 40 years old (51.6%). The next largest age group included individuals between the ages of 21 to 30 years old (23.2%). Individuals between the ages of 41 to 50 years old constituted 15.6% of the sample. The number of people between 51 to 60 years was 17 (6.8%), and 1.6% (*n* = 4) were between the ages of 61 to 65.

Table 7 also displays the descriptive statistics related to the respondents' gender and ethnicity. Out of the 250 study participants, 142 were men (56.8%), while 105 participants (42.0%) were women. Table 7 indicates that a majority of the sample was White (75.6%). The remaining participants were divided between the Hispanic/Latino subgroup (9.2%), the subgroup of African Americans (6.8%), the Asian subgroup (4.8%), the American Indian subgroup (1.2%), and the participants that identified as Pacific Islander or Other (.4%).

Table 7. *Demographics of Selected Study Variables*

Demographic	Frequency	Percent
Age Distribution		
21- 30 years old	58	23.2%
31 to 40 years old	129	51.6%
41 to 50 years old	39	15.6%
51 to 60 years old	17	6.8%
61 to 70 years old	4	1.6%
Gender		
Male	142	56.8%
Female	105	42.0%
Race/Ethnicity		
White/ Caucasian	189	75.6%
American Indian	3	1.2%
Asian	12	4.8%
Hispanic/Latino	23	9.2%
African American	17	6.8%
Pacific Islander	1	0.4%
Other / please specify	1	0.4%
Total	250	100.0%

Hypothesis Testing

Following the evaluation of the sample demographics, the researcher calculated the descriptive statistics. This step involved calculating the mean and standard deviation for the answers to each scale. Table 8 presents this information. Of the three scales, IS governance had the highest mean score (3.86), followed by IT risk management (3.71) and IT leadership (3.64).

Table 8. *Means and Standard Deviations*

Variable	*M*	*SD*	Min.	Max.
IT Leadership scale	3.64	0.74	1	5
IS Governance scale	3.86	0.78	1	5
IT Risk Management scale	3.71	1.01	1	5

Note. *N* = 250

Next, the descriptive statistics were calculated to examine participants' responses to survey questions about the use of transformational leadership style. The transformational leadership style questions addressed five elements: (a) idealized influence attributed, (b) idealized influence behavioral, (c) inspirational motivation, (d) intellectual stimulation, and (e) individual consideration. Table 9 presents the five summated characteristic scale scores used to describe transformational leadership style. The scale items included data on idealized influence (attributed), *M* = 3.90, *SD* = 1.04; idealized influence (behavior), *M* = 4.16, *SD* = 1.01; inspirational motivation, *M* = 4.07, *SD* = 1.03, intellectual stimulation, *M* = 3.86, *SD* = 1.09; and individualized consideration. *M* = 4.02, *SD* = 1.04. Idealized influence (behavior) had the most reliable mean average among the study's participants.

Table 9. *Descriptive Statistics for Transformational Leadership Style*

Variable	*M*	*SD*	Min.	Max.	Median
Q4. Idealized Influence (Attributed)	3.90	1.04	1	5	4
Q5. Idealized Influence (Behavior)	4.16	1.01	1	5	4
Q6. Inspirational Motivation	4.07	1.03	1	5	4
Q7. Intellectual Stimulation	3.86	1.09	1	5	4
Q8. Idealized Consideration	4.02	1.04	1	5	4

Note. *N* = 250

A similar process was used with the scale scores for the transactional leadership style (see Table 10) and passive-avoidant leadership (see Table 11). The transactional leadership style was divided into two subparts that include (a) contingent reward and (b) active management by exception. Table 10 presents the descriptive characteristics associated with the two summated scale items for the transactional leadership style. The descriptive statistics for contingent reward were *M* = 3.98, *SD* = 1.04, and the descriptive statistics for active management by exception were *M* = 3.46, *SD* = 1.22.

The passive-avoidant leadership style also included two subparts: (a) passive management by exception and (b) laissez-faire. Table 11 contains the descriptive characteristics of the two summated scale items associated with passive-avoidant leadership style. The results of the descriptive statistics were *M* = 2.75, *SD* = 1.42 for passive management by exception and *M* = 3.71, *SD* = 1.06 for laissez-faire.

Table 10. *Descriptive Statistics for Transactional Leadership Style*

Variable	*M*	*SD*	Min.	Max.	Median
Q9. Contingent Reward	3.98	1.04	1	5	4
Q10. Management by Exception (Active)	3.46	1.22	1	5	4

Note. *N* = 250

Table 11. *Descriptive Statistics for Passive Avoidant Leadership Style*

Variable	*M*	*SD*	Min.	Max.	Median
Q11. Management by Exception	2.75	1.42	1	5	3
Q12. Laissez-Faire	3.71	1.06	1	5	2

Note. *N* = 250

Table 12 presents the descriptive statistics from the MLQ Rater Form to determine leadership style. The transformational leadership style had a high average mean of 4.01 rated on a scale of 1 to 5 and a standard deviation of 0.86. These values indicated that this was the most highly exhibited leadership style. The transactional leadership style yielded a mean score of 3.73

measured on a scale of 1 to 5. The scores indicated that many of the respondents utilized this leadership style because of its goal setting and rewards system. Few participants exhibited the passive-avoidant leadership style.

Table 12. *Descriptive Statistics for MLQ Rater Form Leaders Style*

Variable	*M*	*SD*	Min.	Max.	Median	α
Transformational Scale	4.01	0.86	1	5	4.20	0.887
Transactional Leadership	3.73	0.98	1	5	4.00	0.691
Passive-Avoidant Leadership	2.59	1.36	1	5	2.50	0.837

Note. *N* = 250

After examining the data on IT leadership style, the researcher analyzed the data on IS governance. There were a total of six scale items measuring IS governance. These items included (a) communications, (b) competency/value, (c) governance, (d) partnership, (e) scope and architecture, and (f) skills. The descriptive statistics for IS governance are presented in Table 13. The aspects of IS governance that were most highly rated by respondents were scope and architecture (*M* = 3.96, *SD* = .90) and governance (*M* = 3.91, *SD* = .89).

Table 13. *Descriptive Statistics for IS Governance Category*

Variable	M	SD	Min.	Max.	Median	α
Communications	3.71	0.92	1	5	3.75	0.876
Competency/ Value	3.88	0.91	1	5	4.00	0.823
Governance	3.91	0.89	1	5	4.00	0.821
Partnership	3.78	1.10	1	5	4.00	--
Scope & Architecture	3.96	0.90	1	5	4.00	0.815
Skills	2.59	1.36	1	5	2.50	0.837

Note. *N* = 250

Once the IS governance data had been analyzed, the researcher examined the survey responses addressing IS risk management. Tables 14 through 19 present the questions relating to risk management as measured by the use of ISO27001/27002 and other frameworks. Table 14 displays the participants' responses to the question of whether an organization implements ISO 27001/27002 objectives. As indicated in Table 14, over 85% of the sample work for organizations that implement IS risk management framework at least some time, with 65% of the sample indicating their company implements the objectives often or frequently.

Table 14. *Organizations that Implement ISO 27001/27002 Objectives*

Scale	*n*	Percent	Cumulative %
Not at all	20	8%	8%
Occasionally	15	6%	14%
Sometimes	52	20.8%	34.8%
Often	96	38.4%	73.2%
Frequently	67	26.8%	100%
Total	250		

The data indicated that the largest group of participants indicated their organization utilized ISO objectives in combination with other frameworks (see Table 15). Table 16 indicated that within the sample group, ISO frameworks were often aligned at least some of the time with an organization's use of COBIT. Table 17 reports the participants' assessments of whether or not the ISO framework is effective. The largest portion of the sample group indicated that they believed the ISO framework was effective in managing IS risk (see Table 18). Table 19 indicated that a large portion of the sample group believed that their organization had achieved effective IT Governance.

Table 15. *Organizations that Utilize ISO Objectives and Other Frameworks*

Scale	*n*	Percent	Cumulative %
Not at all	21	8.4%	8.4%
Occasionally	21	8.4%	16.8%
Sometimes	51	20.4%	37.2%
Often	81	32.4%	69.6%
Frequently	71	28.4%	98%
Missing	5	2%	100%
Total	250		

Table 16. *Organizations that have Aligned COBIT and ISO/27001/27002 Frameworks*

Scale	*n*	Percent	Cumulative %
Not at all	22	8.8%	8.8%
Occasionally	24	9.6%	18.4%
Sometimes	51	20.4%	38.8%
Often	82	32.8%	71.6%
Frequently	71	28.4%	100%
Total	250		

Table 17. *ISO 27001/27002 is Effective in Managing IS Risk*

Scale	*n*	Percent	Cumulative %
Not at all	20	8%	8%
Occasionally	22	8.8%	16.8%
Sometimes	58	23.2%	40%
Often	70	28%	68%
Frequently	80	32%	100%
Total	250		

Table 18. *ISO 27001/27002 has a Positive Relationship with Effective IS Risk*

Scale	*n*	Percent	Cumulative %
Not at all	14	5.6%	5.6%
Occasionally	23	9.2%	14.8%
Sometimes	45	18%	32.8%
Often	96	38.4%	71.2%
Frequently	72	28.8%	100%
Total	250		

Table 19. *Organizations that have Achieved Effective IT Governance*

Scale	*n*	Percent	Cumulative %
Not at all	11	4.4%	4.4%
Occasionally	21	8.4%	12.8%
Sometimes	49	19.6%	32.4%
Often3	83	33.2%	65.6%
Frequently	86	34.4%	100%
Total	250		

Assumption Testing

Following the completion of the descriptive statistics analysis, the researcher tested the methodological assumptions before analyzing regression models to answer the study's research questions. This step in the data analysis process involved testing the data for the assumptions related to the normality, linearity, and homoscedasticity of the data. The data were also examined visually for outliers. The result of the assumptions testing was the determination that the data conformed to the necessary assumptions. Thus, the data was appropriate for use with the statistical methods chosen to test the study's hypotheses. The histograms and scatterplots the researcher used to assess the data visually and test the methodological assumptions are presented in Appendix A.

Overarching Research Question

The Overarching Research Question asked: To what extent are IT leadership style and IS governance related to IS risk management in U.S. organizations? This question was answered by testing the following set of hypotheses:

H_0O: There is no statistically significant relationship between IT leadership styles, IS governance, and IS risk management in U.S. organizations.

H_aO: There is a statistically significant effect between IT leadership styles and IS governance on IS risk management in US organizations.

The researcher used a Pearson product-moment coefficient correlation to test the first set of hypotheses. The Pearson correlation is a measure of the linear dependence between two variables, and the test results in a score with a value between +1 and -1. The results of the data analysis indicated that there were statistically significant relationships between IT leadership styles, IS governance and IS risk management. As indicated in Table 20, IT Leadership was statistically significant at p <.01 and had a moderately strong relationship to IT Risk Management (r = 0.601). Similarly, IS governance also has a moderately strong relationship to IT Risk Management (r = 0.694, p = <.01). These results show correlations that were statistically significant at the bivariate level, and both IT leadership and IS governance are significantly related to IS risk management. Thus, the null hypothesis for the Overarching Research Question was rejected, and the alternative hypothesis was accepted.

Table 20. *Test Results for Correlation*

Statistic		SMEAN (IT Lead)	SMEAN (IS Gov)	SMEAN (IT Risk)
SMEAN (IT Lead)	Pearson Correlation	1	.698**	.601**
	Sig. (2-tailed)		.000	.000
SMEAN (IS Gov)	Pearson Correlation	.698**	1	.694**
	Sig. (2-talied)	.000		.000
SMEAN (IS Risk)	Pearson Correlation	.601**	.694**	1
	Sig. (2-talied)	.000	.000	

**. Correlation is significant at the 0.01 level (2-tailed).
b. Listwise N=250

Subquestion 1

Subquestion 1 asked: To what extent are IT leadership style and IS governance individually related to IS risk management in U.S. organizations? This research question was answered by testing the following two hypotheses:

$H_0$1: There are no independent, statistically significant relationships between IT leadership styles, IS governance and IS risk management in U.S. organizations.

H_a1: There are independent, statistically significant relationships between IT leadership styles, IS governance and IS risk management in U.S. organizations.

This set of hypotheses was also tested using a Pearson coefficient correlation test. The results of this test are presented in Table 21. Table 21 shows a strong, positive correlation between IT leadership style and IT risk management. This relationship was statistically significant (r = .601, n = 250, p = .000). Table 21 also shows a moderately strong relationship between IS governance and IT risk management (r = 0.694, p = <.01). These findings show that the individual correlations between the variables were statistically significant at the bivariate level. The results indicated that the null hypothesis for Subquestion 1 could be rejected. The individual relationships between IT leadership, IS governance and IS risk management were all statistically significant.

Table 21. *Pearson Coefficient Correlation Test*

Statistic		SMEAN (IT Lead)	SMEAN (IS Gov)	SMEAN (IT Risk)
SMEAN (IT Lead)	Pearson Correlation	1	.698**	.601**
	Sig. (2-tailed)		.000	.000
SMEAN (IS Gov)	Pearson Correlation	.698**	1	.694**
	Sig. (2-talied)	.000		.000
SMEAN (IS Risk)	Pearson Correlation	.601**	.694**	1
	Sig. (2-talied)	.000	.000	

**. Correlation is significant at the 0.01 level (2-tailed).

b. Listwise N=250

Subquestion 2

Subquestion 2 asked: To what extent does IS governance mediate the relationship between IT leadership style and IS risk management in U.S. organizations? This research question was answered by testing the following two hypotheses:

$H_0$2: IS governance does not significantly mediate the relationship between IT leadership style and IS risk management in U.S. organizations.

H_a2: IS governance does significantly mediate the relationship between IT leadership style and IS risk management in U.S. organizations.

The purpose of Subquestion 2 was to test the mediating influence of IS governance on the relationship between IT leadership and IS risk management. The presence of mediation indicates that the relationship between the independent and the dependent variable is weaker when there is interference by a third variable. Mediation can result in a smaller direct effect between a predictor and an outcome variable. Mediation can also result in a significant indirect effect on the outcome of the dependent variable. Table 22 presents the results of the statistical analysis to determine the influence of IS governance as a mediating variable.

Table 22. *Model Summary*

		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	t	Sig.
1	(Constant)	.824	.264		3.124	.000
	SMEAN (IT Lead)	.793	.071	.585	11.216	.764
2	(Constant)	-.078	.260		-.301	.000
	SMEAN (IT Lead)	.317	.086	.234	3.685	.000
	SMEAN (IS Gov)	.680	.084	.512	8.061	.002

a. Dependent Variable: SMEAN (IT Risk)

As indicated in Table 22, a strong, positive correlation existed between the variables. However, the Beta weight of IT leadership was .585 and IS governance was .512. The predictors were significant for both variables at (*p* =.000). The findings indicate that IS governance does not mediate the relationship between IT leadership and IS risk management in U.S. organizations. Thus, the null hypothesis was retained, and the alternate hypothesis was rejected. The results show that the correlations are statistically significant at the bivariate level. However, IS governance does not interfere with the relationship between IT leadership and IS governance in U.S. organizations.

In addition to using Pearson correlation analysis, the researcher also used a multiple regression analysis to examine the relationships between the variables of IT leadership, IS governance, and IS risk management in U.S. organizations. Table 23 presents the results of the multiple linear regression Model 1. Model 1 contained one critical independent variable. It was the case that IT leadership increased IT risk management (*B*= 0.793, *p*=.000). The omnibus *F*-test for Model 1 was statistically significant (*F* = 125.80, *p* = .000). The coefficient of determination, also known as the R^2 value, was .342 for Model 1. This value shows that 34% of the variation in IS risk management can be explained by the one independent variable.

Table 23. *Multiple Linear Regression of IT Risk Management Scale Model 1*

Variable	*B*	*SE (B)*	*p*
Constant	0.824	0.264	0.002
IT leadership scale	0.793	0.071	0.000
N	250		
F	125.80	0.000	
R^2	0.342		

Note. * < p .05; ** < p .01; *** < p .001, two-tailed tests.

Table 24 presents the results of a second regression model. In Model 2, two critical independent variables were used. In Model 2, IS governance increased IT risk management (*B*= 0.680, *p*=.000). The R^2 value was .482 for Model 2. This value shows that 48% of the variation in IS risk management can be explained by the two independent variables.

Table 24. *Multiple Linear Regression of IS Risk Management Scale Model 2*

Variable	*B*	*SE (B)*	*p*
Constant	-0.780	0.260	0.764
IS governance scale	0.680	0.084	0.000
N	250		
F	112.02	0.000	
R^2	0.482		

Note. * < p .05; ** < p .01; *** < p .001, two-tailed tests.

Table 25 presents the results of a third and final regression model. Model 3 presents the two key independent variables with the controls added. While none of the controls are statistically significantly related to IT risk management, both of the key independent variables remain statistically significantly (IT leadership was *B*= 0.334, *p*=.000 and IS governance was *B*= 0.661, *p*=.000). The R^2 value is .50 for Model 3. This value showed that 50% of the variation in IS risk management could be explained by the control variables in the equation.

Table 25. *Multiple Linear Regression of IS Risk Management Scale Model 3*

Variable	*B*	*SE (B)*	*p*
Constant	-1.179	0.292	0.540
IT leadership scale	0.334	0.087	0.000
IS governance scale	0.661	0.086	0.000
Demographic controls			
21 to 30 years old	0.165	0.185	0.372
31 to 40 years old	0.176	0.173	0.310
41 to 50 years old	0.062	0.197	0.752
Female	-0.174	0.095	0.068
Hispanic	0.196	0.162	0.229
Black	0.272	0.184	0.140
Other	0.272	0.184	0.431
N	250		
F	25.934	0.000	
R^2	0.50		

Note. * *p* < .05; ** *p* < .01; *** *p* < .001, two-tailed tests.

Summary

This study examined the effects of IT leadership styles and IS governance on IS risk management in US organizations. Chapter 4 was devoted to answering the study's three research questions. The data analysis indicated the existence of significant linear relationships between IT leadership styles and IS risk management and between IS governance and IS risk management. The chapter provided descriptive statistics, data analysis and detailed description of the results of the statistical tests. The chapter provided a summary of the results that indicate that there is a significant correlation between IT leadership and IS governance on the effectiveness of IS risk management in US organizations. The chapter gave a background on the study and a discussion of the data analysis methods, and a report of the findings from the data analysis. The chapter concludes with a summary of the results that indicate that there is a significant correlation between IT leadership and IS governance and the effectiveness of IS risk management in U.S. organizations. The next chapter provides a review of the study's findings and a discussion of the results in the context of the scholarly literature.

CHAPTER 5. DISCUSSION, IMPLICATIONS, RECOMMENDATIONS

This chapter has two primary objectives; the first is to assess how well the present study was able to address the problems that precipitated this study and second, provide recommendations for future research. The chapter divides into six major sections. These sections are (a) a summary of results, (b) a discussion of the results, (c) conclusions based on the results, (d) limitations, (e) implications for practice, (f) recommendations for further research, and (g) the conclusion.

Summary of the Results

U.S. organizations of all sizes, public and private are now finding that managing the risk of information security breaches is a matter of ongoing concern at board-level. As Knorst et al. (2011) noted, current research has demonstrated that organizations face continuously evolving risks, and as a result, IT leadership and governance practices related to organizational risk management must also continually evolve. As a result, the present study posed the research question asking: to what extent are IT leadership style and IS governance related to IS risk management in U.S. organizations?

The present study was significant as IT leadership, IS governance and IS risk management constitute crucial topics for modern organizations (McFadzean et al., 2011; Williams et al., 2013). Moreover, scholars have noted that organizations are challenged by the lack of knowledge related to the role that IT leadership plays in improving IS risk management in organizations (Landis et al., 2014). Additionally, scholars such as Nichols (2016) have noted that there are differences in the types of IT leadership traits that are useful in the analysis of leadership qualities and the resultant impact on ISRM.

The literature review examined scholarship and practitioner literature related to IT leadership styles, IS governance and ISRM. In turn, this required an examination of practitioner literature surrounding recent security framework revisions and national and international IS security standards. For recently introduced security standards and recent revisions of security frameworks, in many cases, the only literature as yet extant was practitioner literature and literature provided by security framework providers such as the NIST. The literature review of necessity examined key seminal works such as Thite's (2000) empirical study of effective IT leadership and Avolio and Bass's (2004) work introducing the FRLT and Eagly et al.'s (2003) study on FRLT leadership styles and gender.

A number of relevant scholarly studies have appeared since the 2013 commencement of the present dissertation. For example, Tyssen et al. (2014), supported by the further scholarship of Penn (2015) introduced the notion of exchanges of value, defined by Penn (2015) as implicit contracts between leaders and followers. Hayne and Free (2014) studied the COSO internal standards framework and highlighted the vulnerability of U.S. and global financial institutions to attack. Albakri et al. (2014) provided a study on risk assessment frameworks for the cloud computing environments in the context of the NIST SP800-37 risk management guide. Dartey-Baah (2015) provided new insights into what transactional leadership can deliver to an organization, and about the transformational leadership component of the FRLT, Bedi et al. (2015) provided a meta-analytic review of ethical leadership outcomes and moderators. Bedi, Alpaslan, & Green (2015) addressed issues with transformational leadership initially identified by Bass (1997) and also addressed by Antonakis and House (2013).

The security frameworks and standards space continued to evolve while the dissertation was being written. For example, the NIST introduced their cyber-framework in 2014, with a revision published in April of 2018 (NIST, 2018). The NIST cyber-security framework was studied by Protiviti (2016) in the context of the FFIEC. COBIT was the subject of a study by de Haes and van Grembergen (2015) as well as by Luellig and Frazier (2013). The NIST continued to move quickly on new revisions during the period the dissertation was written with draft five of the critical Security and Privacy controls guideline coming out in 2013 and the draft five of the same guideline being completed later with a much-increased emphasis on both comprehensiveness and proactivity.

Just as the dissertation was being completed Northouse (2018) stated that an issue with transformational leadership was a lack of clarity due to the multiplicity of the dimension supporting it. Northouse (2018) also introduced the notion of followership and the idea that no theory of leadership can be complete without a solid understanding of how a given style of leadership interacts with followers. The researcher notes that the notion of followership may provide grounds for an important extension of the scholarship on leadership going forward. Finally, in 2018, in a sign of the accelerating pace of security framework development, the NIST published several new draft guides for public comment addressing specific IT security topics.

The present study posed the question: to what extent are IT leadership style and IS governance related to IS risk management in U.S. organizations? The findings indicated a strong relationship between IT leadership styles and IS governance on ISRM. The present study also found that there are independent, statistically significant relationships between IT leadership styles, IS governance and ISRM in U.S. organizations. Additionally, the present study found that IS governance when examined individually did not significantly mediate the relationship between leadership style and ISRM.

Discussion of the Results

The present study's results supported the study's overarching research question which asked to what extent are IT leader leadership style and IS governance related to risk management in U.S. organizations? As the researcher expected it proved that leadership style and IS governance were strongly statistically linked to ISRM in U.S. organizations. Based on the previously extant scholarly literature on IT leadership the relationship between lT leadership style and ISRM was not a surprising finding as ISRM is a sub-component of the overall set of responsibilities for which IT leadership is responsible. While IS governance has become a board-level activity and a significant component of IT leadership at board-level this is a new phenomenon characteristic of the last two decades (Von Solms & Von Solms, 2009). Furthermore, IS governance is an activity that provides overall guidance via the choice and establishment of security frameworks and security policies but does not direct IT line management (Fitzgerald, 2012). Thus, the finding that IS governance as directly understood by IT professionals can be statistically linked to organizational outcomes related to ISRM suggests that the choice of IS policies and what security frameworks are chosen at board-level by IS governance make an impact on organizational outcomes in the opinion of IS security professionals.

The present study's findings also found support for the notion that there are individual relationships between IT leadership style, IS governance and ISRM. These relationships suggest that IS security professionals make a distinction between IT leadership broadly understood and

IS governance as a specific source of leadership policy. In turn, this suggests that IS security professionals not only appreciate that good IT leadership is necessary to superior ISRM outcomes but that IS governance is a necessary component of IT leadership if superior outcomes are to be supported.

The present study's final and unexpected result was that IS governance did not significantly mediate the relationship between IT leadership style and ISRM. While this was unexpected, the result was in alignment with both the extant literature which notes that IS governance is a function or division of IT leadership at board-level and the present study's findings that IS governance had a direct relationship with ISRM. The researcher speculates that study participants did not perceive IS governance as mediating between leadership style and ISRM as IS governance was an activity that took place at board-level and set policy. Furthermore, policy setting was an activity separate from and preceding the actions of IT leadership and the leadership style chosen to be followed by senior or executive management of the organization in question. Moreover, IS governance was an activity that would be required to support any form of IT leadership in a modern organization.

The findings of the present study supported the research questions. The exception was sub-question two in which the null hypothesis was supported in regards to IS governance not mediating the relationship between IT leadership style and ISRM in U.S. organizations. Overall, the findings of the present study supported the importance of both leadership style and IS governance both collectively and individually to superior ISRM outcomes.

Conclusions Based on the Results

The present study had results that both confirmed most of its hypotheses and also what those results might have been expected to be based both on the scholarly literature and the literature surrounding and supporting the development of both security frameworks and security standards both national and international. The present study highlighted that practicing IS security professionals perceived the links between IS governance and ISRM. This perception made sense in the context of IS security frameworks, and standards are making a real-world difference. The present study also found both support for the effect of leadership style on ISRM which supported the notion inherent in later revisions of the NIST SP800-53 and scholarly writing that more proactive approaches to managing IS security risk were becoming important (Fitzgerald, 2012; Naseer, Shanks, Ahmad, & Maynard, 2016).

Comparison of the Findings with the Theoretical Framework and Previous Literature

Previous scholarly literature had found that IT leadership was essential to organizations and that transactional and transformational leadership, interacting with technical leadership was an effective set of leadership styles for IT leadership (Ghasabeh, Soosay, & Reaiche, 2015; Thite, 2000). Furthermore, that transformational leadership possessed as one of its dimensions the ability of the leader to generate out-of-the-box thinking patterns (Creary, Caza, & Roberts, 2015). The literature surrounding the development of standards and security frameworks was coming to emphasize proactive approaches to managing security risk by 2011 (Fitzgerald, 2012; NIST, 2018) and building analytic tools to assist in supporting IS security leadership proactivity in the years following (Naseer et al., 2016).

The present study found strong support for both the importance of IT leadership style and IS governance both jointly and individually when related to ISRM in U.S. organizations. These relationships supported the findings the researcher expected based on the literature. In turn, this supported the broader scholarly consensus that to optimize IS security outcomes based on an organization’s governance policies and resources deployed to support them, would require effective leadership to decrease systemic organizational security risks (Alqahtani, 2015; Apollonia, & Ihagh, 2016; Arslan, & Staub, 2013; Richard et al., 2009).

Interpretation of the Findings

The present study found strong implicit support in the fact that organizations and their associated IS security professionals devote substantial resources and place high confidence in standards-based security frameworks (Dimension Research, 2016). This implicit empirical support was related to the fact that these frameworks are built specifically for application by IS governance at board-level. Furthermore, there was strong support in the scholarly literature for the importance of effective IT leadership (Alqahtani, 2015; Apollonia, & Ihagh, 2016; Arslan, & Staub, 2013; Richard et al., 2009).). Thus, it was not startling that the results of the present study were in alignment with both IS governance and the FRLT.

The theoretical scholarly literature on leadership strongly linked effective leadership whether in the field of IT or more generally, with the style of leadership. The FRLT as the single most popular explanatory theory of leadership in the last two decades was particularly appropriate for application as it specifically provided a spectrum of leadership types, identified from least to most effective (Avolio & Bass, 2004). In light of the extremely rapid change in the field of IT and the sub-field of ISRM, it was at minimum plausible that the most effective leadership styles would be most applicable to IT leadership and IS governance. Thus, both previous scholarly research, the practitioner literature and the present study's findings suggested that the FRLT theoretical framework was an appropriate analytical choice. Indeed, it proved serendipitous as during the years in which the dissertation was being written the increasing emphasis on proactive IS security policies made the FRLT's transformational leadership style and increasingly strong choice as a style related to superior ISRM outcomes.

A 2016 survey of U.S. IS security professionals noted that full application of frameworks such as the NIST SP800-543 while optimal can be very resource intensive (Dimension Research, 2016). Indeed, the professionals surveyed noted that many organizations only implemented parts of the frameworks they deployed due to cost considerations (Dimension Research, 2016). However, in light of the resources devoted to ISRM in current U.S. organizations the present study's linkage of IS governance to ISRM outcomes is particularly important. It is important not only regarding effective risk management but also regarding the high level of resources devoted to ISRM which suggest that ineffective or suboptimal IS governance could lead not only to increased risk but also a waste of substantial organizational resources.

Limitations

This study determined that statistically significant correlations exist between IT leadership style, IS governance and IS risk management in U.S. organizations. However, the study did have some limitations. The first limitation was that the data analysis relied on the use of a correlational approach to analysis. This limitation meant that while it was possible to determine that the variables were significantly related, the data analysis process was not able to determine whether a causal relationship existed between the variables. Thus, the research could only forecast the magnitude and the direction of the associations between the variables, not whether the independent variables directly influenced the dependent variables.

A second methodological limitation was linked to the use of a cross-sectional instrument to collect data. The researcher only collected data at a single point in time, and the instrument was not designed to ask participants about change over time. Thus, the research findings cannot be extended to determine how changes in IT leadership style or changes in IS governance may impact changes in IS risk management. While a longitudinal study may address this issue, it was not within the limited scope of the research to measure changes in IS risk management over time.

The study was limited by the sample chosen to represent the population of interest. The study only included U.S. IT professionals in specific categories such as Chief Information Officer (CIO), Chief Information Security Officer (CISO), Director of IT, and IT manager. As a result of this limitation, the study's findings are not generalizable to other users or organizational decision makers. Nor were the study's findings generalizable to IT professionals in other countries.

There were five additional non-methodological limitations. The first of these was that the study was limited based on the researcher's decision to only focus on IT leadership style and IS governance. Many other associated factors impact the effectiveness of IS risk management such as organizational funding, geographical locations of organizations, best practice frameworks, types of businesses, laws, and cultural perspectives of IS governance (Novotny, Bernroider, & Koch, 2012). The study's findings cannot be extended to allow scholars to draw conclusions about the significance or non-significance of these other facts.

The second non-methodological limitation was that the scope of the study included only the U.S. The U.S. has a distinctive, primarily English-speaking culture. Other countries representing other cultures and language groups may have differences that are significant in the dimensions of leadership style and approaches to ISRM. As a result, the explanatory power of the present study's results may be limited or nullified in other countries or regions.

The third non-methodological limitation was the gender-distribution of the present study's sample. In 2016, the U.S. Bureau of Labor Statistics noted that only 27.2% of IT professionals were female. However, in the present study, 42% of respondents were female. As a result, based on BLS statistics it would appear that females are over-represented compared to the overall population of IT professionals in the U.S.

The fourth non-methodological limitation was the fact that while the FRLT is a full-spectrum leadership theory, well validated and well supported other leadership styles exist in the scholarly literature. Examples of such leadership styles include technical leadership (Avolio, 2011) and strategic leadership (Van, Coleman, & Simpson, 2014). As previously noted in chapter two there are also variants or extensions of the FRLT that include ethical leadership and authentic leadership (Antonakis & House, 2013). Scholars such as Alsamydai, Alensour, and Abdelrazzaq (2016) have suggested that different leadership styles may provide different results.

The fifth and final non-methodological limitation that is directly applicable to the present study is the fact that the data used was self-reported. Self-reported data allowed for the potential introduction of human bias into the data-set. Such biases can include the potential for exaggeration and selective memory as well as the potential for the volitional introduction of misinformation (Brutus, Aguinis, & Wassmer, 2013; Aguinis & Bradley, 2014).

Implications for Practice

Management of IS risk has become an ongoing concern for organizations at the level of policy and constant concern for IS professionals on a daily basis. Furthermore, it has become clear over the last two decades that ISRM cannot be disentangled or dis-intermediated from IT leadership practices and IT line management practice. ISRM including the IS governance that supports it has become a crucial and integral part of IT in U.S. organizations (Da Veiga & Martins, 2015).

The present study found that there were independent relationships between each of IT leadership styles and IS governance to ISRM. These relationships suggest that, in practice, IS security professionals in organizations that have implemented security frameworks perceive each of these relationships independently as relevant to maintaining effective ISRM. Despite the distinction practitioners make, scholars note that IS governance is a board-level policy function of organizations and falls within the domain of senior IT leadership (Bobbert & Mulder, 2015). However, in practice, the present study's findings suggest that IT leadership and its associated leadership styles are not perceived as a substitute for IS governance nor vice versa in the minds of IS professionals in line management. Thus, an implication for practice for organizations who have not yet fully implemented IS governance, (and its associated security frameworks) is that when implementing IS governance at board-level it is necessary to ensure that such governance is seen within the organization as guiding IS policy separately from other activities related to IT leadership.

There was explicit support in both the practitioner and scholarly literature (Fitzgerald, 2012; NIST, 2018) for movement to more proactive IS security risk management policies. The present study also found a strong statistical linkage between IT leadership style and ISRM. ISRM is now a vital dimension of IT which suggests that IT leadership that both accepts and encourages pro-active approaches to IS security is becoming of increasing importance to the ability of organizations to meet their goals. However, if proactive and out-of-the-box leadership is increasingly in demand and the transformational leadership style is characterized by these personal properties related to leadership then an implication for human resources departments is that the selection criteria for IT leadership have to include the ability to be a transformational leader and not merely to be an individual who exhibits technically superior knowledge.

ISRM is a very resource intensive activity and absorbs up to a third of overall IT budgets (Dimension Research, 2016). As such, misallocation of resources in establishing, managing and enforcing IS risk management can be costly to an organization both in regards to resources wasted and the assumption of risk by an organization beyond that intended by senior governance. ISRM’s resource intensity combined with the statistically strong linkages the present study found between IT leadership style, IS governance and ISRM, suggests that errors made in choosing an organization's IT leaders are increasingly costly in the current environment and going forward whether measured by the metrics of unnecessary risk assumed or resources misallocated. Thus, this also supports the implication for practice that the type of IT leadership style that can motivate and unify teams of IT and IS security managers is of increasing importance to organizations in an era of high-cost preventative measures to increasingly diverse and quickly evolving threats to IS.

Recommendations for Further Research

The present study raised many questions. Many scholarly questions still need to be addressed in the field of leadership in general as well as IT leadership in particular. Beyond leadership, IS security is a field and associated discipline experiencing a state of rapid evolution as witnessed by key NIST (2018) standards having a life of approximately two years before being superseded.

On the FRLT spectrum, transformational leadership exhibits the most characteristics of effective leadership (Bass & Avolio, 1994). The need has now arisen for proactive management of IS security due to (a) the rapid evolution of threats and (b) the need to deal with unknown threats. This need implies that every possible individual in an organization involved with IT as well as formally with IS security must be on the lookout for unusual anomalies and never before seen threats to an organization’s systems. Thus, the transformational leadership style which lends itself to effective team building, as well as support for pro-active approaches to problems, appears ideal for IT leadership to adopt going forward. However, this raises many areas for further research. The first area fruitful of future research would be to examine what constitutes transformational leadership in the context of IT leadership, and its subdomain IS governance. Transformational leadership has four components (II, IM, IS, and IC); a very pertinent research topic might be to attempt to discover if any of these components, for example, intellectual stimulation (IS), were of disproportionate importance in the realm of IT leadership? Another topic for future research might inquire as to how does transformational leadership relate to technical leadership and whether there is an optimal balance between the two?

In addition to future research on how the transformational leadership style might be incorporated into IT leadership, studies on the number of IT leaders in today’s organizations who exhibit a transformational style might be indicated. Another related study proposal would be to inquire as to whether the number of IT leaders who lead with a transformational style is increasing, decreasing or staying the same? Two more studies that would be fruitful of new insights into transformational leadership as a style of IT leadership would be studies that examined how well transformational leaders have performed both in relation to their organizations' goals and to IT leaders exhibiting other styles of leadership in the current business environment.

IS governance is now a board-level activity but still often considered part of IT leadership. In the present study both IS governance, and IT leadership style had a relationship with ISRM collectively as well as independently. Future research might examine the ongoing relationship of IS governance to IT leadership. Should IS governance, acting both to set policy and as auditors of an organization’s applied risk management policies, continue to be part of IT leadership or be entirely independent of IT leadership?

IS governance relies on security frameworks that in turn rest on various international and national IS security standards. These frameworks and standards are still evolving rapidly and in tandem with a continuously changing threat environment. A final recommendation for future research might be to examine whether the leaders of standards and security framework organizations also be chosen for their ability to apply transformational leadership styles?

Conclusion

The present study posed the question: to what extent are IT leadership style and IS governance related to IS risk management in U.S. organizations? The findings indicated a strong relationship between IT leadership styles and IS governance on ISRM. The present study also found that there are independent, statistically significant relationships between IT leadership styles, IS governance and ISRM in U.S. organizations. Additionally, the present study found that IS governance when examined individually did not significantly mediate the relationship between leadership style and ISRM.

The present study took place during a time of rapid and possibly transformative change in the field of ISRM. During the years the present study was proposed, researched and its accompanying dissertation was written, ISRM moved to best-practice being security framework based with new frameworks (for example the COSO cyber-security framework) emerging over the period of writing in tandem with new national and international standards applicable to IS security. By 2018, nearly all larger organizations in the U.S. relied on security frameworks to underpin IS security policies and practices (Dimension Research, 2016). However, there is still disagreement on which frameworks are best for which organizations and on whether partial implementation of security standards such as the NIST 800-53 series is acceptable or if only full deployment is adequate (Dimension Research, 2016).

The extant scholarly and practitioner literature surrounding both security standards and framework development made clear that IS security professionals in the U.S. are now fully invested in the idea that IS governance is a vital part of IT leadership. The present study supported this and found that IT leadership style makes a difference to ISRM outcomes as does IS governance both directly and jointly with IT leadership style.

The practitioner literature, as well as literature surrounding both standards and security frameworks, made clear that as threats have both proliferated and become more complex and innovative that passive security standards and practices are no longer enough. In conjunction with the present study's findings, this study strongly suggested that transformative styles of leadership hold the key to more proactive and, hence, better, security practices on the part of organizations. That stated, questions remain as to how to define what makes a security policy proactive? What makes an IT leadership style proactive, and how might the two optimally intersect?

REFERENCES

Adesemowo, A. K., Von Solms, R., & Botha, R. A. (2016). Safeguarding information as an asset: Do we need a redefinition in the knowledge economy and beyond? *South African Journal of Information Management, 18*(1), 1–12. doi:10.4102/sajim.v18i1.706

Agarwal, R. N. (2017). *Cases in leadership*. India: Sage.

Aggarwal, J., & Krishnan, V. R. (2013). Impact of transformational leadership on follower's self-efficacy: Moderating role of follower's impression management. *Management and Labour Studies, 38*(4), 297–313. doi:10.1177/0258042X13513129

Aguinis, H., & Bradley, K. J. (2014). Best practice recommendations for designing and implementing experimental vignette methodology studies. *Organizational Research Method*s, *17*, 351-371. doi:10.1177%2F1094428114547952

Albakri, S. H., Shanmugam, B., Samy, G. N., Idris, N. B., & Ahmed, A. (2014). Security risk assessment framework for cloud computing environments. *Security and Communication Networks, 7*(11), 2114–2124. doi:10.1002/sec.923

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security, 42*, 56–65. doi:10.1016/j.cose.2014.01.005

Allison, P. D. (2002). Missing data: Quantitative applications in the social sciences. *British Journal of Mathematical & Statistical Psychology, 55*, 193–196. doi:10.4135/9781412985079

Alqahtani, A. (2015). Towards a framework for the potential cyber-terrorist threat to critical national infrastructure: A quantitative study. *Information & Computer Security*, *23*(5), 532–569. doi:10.1108/ICS-09-2014-0060

Alsamydai, M. J., Alensour, J., & Abdelrazzaq, Y. (2016). The specific factors for strategic leadership style and its impact on competition strategy selected. *International Review of Management and Business Research*, *5*, 42–49. Retrieved from https://www.questia.com/library/journal/1P3-4288482731/the-specific-factors-for-strategic-leadership-style

Antonakis, J. (2012). Transformational and charismatic leadership. In D. V. Day & J. Antonakis (Eds.), *The nature of leadership* (2nd ed., pp. 256–288). Thousand Oaks, CA: Sage.

Antonakis, J., Avolio, B. J., & Sivasubramaniam, N. (2003). Context and leadership: An examination of the nine-factor full-range leadership theory using the Multifactor Leadership Questionnaire. *The Leadership Quarterly, 14*(3), 261–295. doi:10.1016/S1048-9843(03)00030-4

Antonakis, J., & Day, D. V. (Eds.). (2017). *The nature of leadership* (2nd ed.). Los Angeles, CA: Sage.

Antonakis, J., & House, R. J. (2013). The full-range leadership theory: The way forward. In B. J. Avolio & F. J. Yammarino (Eds.), *Monographs in leadership and management, Transformational and charismatic leadership: The road ahead 10th-anniversary edition* (Vol. 5, pp. 3–33). Bradford, England: Emerald. doi:10.1108/S1479-357120130000005006

Apollonia, A., & Ihagh, I. F. (2016). Effect of relational leadership on organizational effectiveness in the Nigerian public sector: A study of power holding company of Nigeria. *Imperial Journal of Interdisciplinary Research, 2*, 1326-1332. Retrieved from https://www.onlinejournal.in/ijir/

Armstrong, C. P., & Sambamurthy, V. (1999). Information technology assimilation in firms: The influence of senior leadership and it infrastructures. *Information Systems Research, 10*(4), 304–327. doi:10.1287/isre.10.4.304

Arslan, A., & Staub, S. (2013). Theory X and theory Y type leadership behavior and its impact on organizational performance: Small business owners in the Şishane Lighting and Chandelier District. *Procedia: Social and Behavioral Sciences, 75*, 102–111. doi:10.1016/j.sbspro.2013.04.012

Avison, D., Jones, J., Powell, P., & Wilson, D. (2004). Using and validating the strategic alignment model. *The Journal of Strategic Information Systems, 13*(3), 223–246. doi:10.1016/j.jsis.2004.08.002

Avolio, B. J. (1999). *Full leadership development: Building the vital forces in organizations*. Thousand Oaks, CA: Sage.

Avolio, B. J. (2011). *Full range leadership development*. Thousand Oaks, CA: Sage. doi:10.4135/9781483349107

Avolio, B. J., & Bass, B. M. (2004). *MLQ multifactor leadership questionnaire: Manual and sample set* (3rd ed.). Redwood City, CA: Mind Garden.

Axelos. (2018). *ITIL certifications*. Retrieved from https://www.axelos.com/certifications/itil-certifications

Badshah, S. (2012). Historical study of leadership theories. *Journal of Strategic Human Resource Management, 1*(1), 49–59. Retrieved from http://www.publishingindia.com/jshrm

Balyer, A. (2012). Transformational leadership behaviors of school principals: A qualitative research based on teachers' perceptions. *International Online Journal of Educational Sciences,4*, 581–591. Retrieved from http://www.iojes.net/Anasayfa.Aspx

Barrick, M. R., Thurgood, G. R., Smith, T. A., & Courtright, S. H. (2015). Collective organizational engagement: Linking motivational antecedents, strategic implementation, and firm performance. *Academy of Management Journal, 58*(1), 111–135. doi:10.5465/amj.2013.0227

Bass, B. M. (1995). Comment: Transformational leadership: Looking at other possible antecedents and consequences. *Journal of Management Inquiry, 4*(3), 293–297. doi:10.1177/105649269543010

Bass, B. M. (1997). The ethics of transformational leadership. *KLSP: Transformational Leadership, Working Papers*. Retrieved from http://www.academy.umd.edu/publications/klspdocs/bbass_pl.htm

Bass, B. M., & Avolio, B. J. (1994). Transformational leadership and organizational culture. *International Journal of Public Administration, 17*(3-4), 541–554. doi:10.1080/01900699408524907

Bass, B. M., & Avolio, B. J. (1997). *Full range leadership development: Manual for the Multifactor Leadership Questionnaire* (pp. 43–44). Palo Alto, CA: Mind Garden.

Bedi, A., Alpaslan, C. M., & Green, S. (2015). A meta-analytic review of ethical leadership outcomes and moderators. *Journal of Business Ethics, 139*(3), 517–536.doi:10.1007/s10551-015-2625-1

Bellé, N. (2013). Leading to make a difference: A field experiment on the performance effects of transformational leadership, perceived social impact, and public service motivation. *Journal of Public Administration: Research and Theory, 24*(1), 109–136. doi:10.1093/jopart/mut033

Bobbert, Y., & Mulder, H. (2015, December). Governance practices and critical success factors suitable for business information security. In *2015 International Conference on Computational Intelligence and Communication Networks* (pp. 1097-1104). Washington, DC: IEEE Computer Societydoi:10.1109/CICN.2015.216

Bojanc, R., & Jerman-Blazic, B. (2013). A quantitative model for information-security risk management. *Engineering Management Journal, 25*(2), 25–37. doi:10.1080/10429247.2013.11431972

Bolkan, S., Goodboy, A. K., & Griffin, D. J. (2011). Teacher leadership and intellectual stimulation: Improving students' approaches to studying through intrinsic motivation. *Communication Research Reports, 28*(4), 337–346. doi:10.1080/08824096.2011.615958

Brotby, W. K. (2006). *Information security governance: guidance for boards of directors and executive management*. Information Systems Audit and Control Association.

Brutus, S., Aguinis, H., & Wassmer, U. (2013). Self-reported limitations and future directions in scholarly reports: Analysis and recommendations. *Journal of Management*, *39*, 48-75. doi:10.1177%2F0149206312455245

Burns, J. M. (1978). *Leadership*. New York, NY: Harper & Row.
Calder, A., & Watkins, S. (2015). *IT governance: An international guide to data security and ISO 27001/ISO27002* (6th ed.). London, England: Kogan Page.

Cannon, D. (2011). *ITIL service strategy*. Norwich, England: The Stationary Office.

Caudle, D. (2013, January). Improving cyber warfare decision-making by incorporating leadership styles and situational context into poliheuristic decision theory. In D. Hart (Ed.), *Proceedings of the 8th*

International Conference on Information Warfare and Security: ICIW 2013 (pp. 240-248). Reading, England: Academic Conferences and Publishing International.

Chaudry, A. Q., & Javed, H. (2012). Impact of transactional and laissez-faire leadership style on motivation. *International Journal of Business and Social Science, 3*, 258–264. Retrieved from http://www.ijbssnet.com/journals/Vol_3_No_7_April_2012/28.pdf

Chen, Y. A. N., Ramamurthy, K. R. A. M., & Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11–19. doi:10.1080/08874417.2015.11645767

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2018). About us. Retrieved from https://www.coso.org/Pages/aboutus.aspx

Cooper, B. L., Watson, H. J., Wixom, B. H., & Goodhue, D. L. (2000). Data warehousing supports corporate strategy at the first American corporation. *Management Information Systems Quarterly*, *24*(4), 547–567. doi:10.2307/3250947

Creary, S. J., Caza, B. B., & Roberts, L. M. (2015). Out of the box? How managing a subordinate’s multiple identities affects the quality of a manager-subordinate relationship. *Academy of Management Review*, *40*(4), 538–562. doi:10.5465/amr.2013.0101

Creswell, J. W. (2014). *A concise introduction to mixed methods research*. Thousand Oaks, CA: Sage.

Dartey-Baah, K. (2015). Resilient leadership: A transformational-transactional leadership mix. *Journal of Global Responsibility*, *6*(1), 99–112. doi:10.1108/JGR-07-2014-0026

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security,49*, 162–176. doi:10.1016/j.cose.2014.12.006

Dearfield, K. L., Hoelzer, K., & Kause, J. R. (2014). Review of various approaches for assessing public health risks in regulatory decision making: Choosing the right approach for the problem. *Journal of Food Protection, 77*(8), 1428–1440. doi:10.4315/0362-028X.JFP-14-046

de Haes, S., Debreceny, R., & van Grembergen, W. (2013). Understanding the core concepts in COBIT 5. *Isaca Journal*, *5*, 1-8. Retrieved from https://www.isaca.org/Journal/Pages/default.aspx

de Haes, S., & van Grembergen, W. V. (2015). *COBIT as a framework for enterprise governance of IT. Enterprise governance of information technology: Achieving alignment and value, featuring COBIT* (pp. 103–128). Cham, Switzerland: Springer International.

DeSimone, J. A., Harms, P. D., & DeSimone, A. J. (2014). Best practice recommendations for data screening. *Journal of Organizational Behavior, 36*(2), 171–181. doi:10.1002/job.1962

Diaz-Saenz, H. R. (2011). Transformational leadership. In A. Bryman, D. Collinson, K. Grint, B. Jackson, & M. Uhl-Bien (Eds.), *The SAGE handbook of leadership* (pp. 299–310). Thousand Oaks, CA: Sage.

Dimension Research. (2016, March 2016). *Trends in security framework adoption: A survey of IT and security professionals*. Retrieved from https://static.tenable.com/marketing/tenable-csf-report.pdf

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security, 4*(02), 92–100. doi:10.4236/jis.2013.42011

DoCRA Council (DoCRA). (2018). *About DoCra*. Retrieved from https://docra.org

Downton, J. V. (1973). *Rebel leadership: Commitment and charisma in the revolutionary process*. Florence, MA: Free Press.

Eagly, A. H., Johannesen-Schmidt, M. C., & van Engen, M. L. (2003). Transformational, transactional, and laissez-faire leadership styles: A meta-analysis comparing women and men. *Psychological Bulletin, 129*(4), 569–591. doi:10.1037/0033-2909.129.4.569

Educause. (2014, May 1). *Information security guide: Effective practices and solutions for higher education*. Retrieved from https://library.educause.edu/resources/2014/5/information-security-guide-effective-practices-and-solutions-for-higher-education

Eisenbeiß, S. A., & Boerner, S. (2013). A double-edged sword: Transformational leadership and individual creativity. *British Journal of Management, 24*(1), 54–68. doi:10.1111/j.1467-8551.2011.00786.x

Epstein, A. J. (2014). Thinking strategically about cyber risk. *NACD Directorship, 2014*(1-2), 32-35. Retrieved from https://www.nacdonline.org/Magazine/index.cfm

Fadun, O. S. (2013). Risk management and risk management failure: Lessons for business enterprises. *International Journal of Academic Research in Business and Social Sciences, 3*, 225-239. Retrieved from http://hrmars.com/index.php/pages/detail/IJARBSS Federal Financial Institutions Examination Council (FFIEC). (2014). Speeches. Retrieved from https://www.occ.gov/news-issuances/speeches/2014/pub-speech-2014-69a.pdf

Federal Financial Institutions Examination Council (FFIEC). (2018). *Welcome to the Federal Financial Institutions Examination Council's FFIEC web site*. Retrieved from https://www.ffiec.gov/about.htm

Field, A. (2013). *Discovering statistics using IBM SPSS statistics*. Atlanta, GA: Sage.

Fitzgerald, T. (2012). *Information security governance simplified*. Boca Raton, FL: CRC Press.

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security, 43*, 90–110. doi:10.1016/j.cose.2014.03.004

Gajendran, T., & Brewer, G. (2012). Cultural consciousness and the effective implementation of information and communication technology. *Construction Innovation, 12*(2), 179–197. doi:10.1108/14714171211215930

Galdies, P. (2014). The insider threat to data assets. *Journal of Direct, Data and Digital Marketing Practice, 15*(3), 197–200. doi:10.1057/dddmp.2014.2

Gall, M. D., Gall, J. P., & Borg, W. R. (2007). Collecting research data with questionnaires and interviews. In *Educational research: An introduction* (pp. 227–261). New York, NY: Pearson.

Gbenle, I. T. (2013). *An examination of the relationship between information technology governance (ITG) and leadership in organizations* (Doctoral dissertation). Capella University, Minneapolis, MN.

Ghasabeh, M. S., Soosay, C., & Reaiche, C. (2015). The emerging role of transformational leadership. *The Journal of Developing Areas*, *49*(6), 459-467. doi:10.1353/jda.2015.0090

Gholamzadeh, D., & Khazaneh, A. T. (2012). Surveying the relationships between leadership styles, organizational health, and workplace bullying. *Journal of Global Strategic Management,12*(6), 5–22. doi:10.20460/JGSM.2012615770

Green, M. T., Duncan, P., Salter, C., & Chavez, E. (2012). The educated worker: An empirical investigation of expectations of leadership. *Journal of Leadership, Accountability and Ethics,9*(6), 94–112. Retrieved from http://www.na-businesspress.com/jlaeopen.html

Hargis, M. B., Watt, J. D., & Piotrowski, C. (2011). Developing leaders: Examining the role of transactional and transformational leadership across business contexts. *Organization Development Journal*, *29*(3), 51. Retrieved from https://www.isodc.org/page-1730212

Hayne, C., & Free, C. (2014). Hybridized professional groups and institutional work: COSO and the rise of enterprise risk management. *Accounting, Organizations and Society, 39*(5), 309–330. doi:10.1016/j.aos.2014.05.002

Hiekkanen, K. (2015). The impact of IT governance practices on strategic alignment. *International Journal of IT/Business Alignment and Governance*, *6*(2), 1–13. doi:10.4018/IJITBAG.2015070101

Hinkin, T. R., & Schriesheim, C. A. (2008). A theoretical and empirical examination of the transactional and non-leadership dimensions of the Multifactor Leadership Questionnaire (MLQ). *The Leadership Quarterly, 19*(5), 501–513. doi:10.1016/j.leaqua.2008.07.001

HITRUST. (2018). *HITRUST alliance*. Retrieved from https://hitrustalliance.net/

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615–660. doi:10.1111/j.1540-5915.2012.00361.x

Hussain, M., & Hassan, H. (2016). Leader’s self-efficacy and effectiveness of leadership styles. *Abasyn University Journal of Social Sciences, 9*(1), 86-102. Retrieved from http://www.aupc.info/

Information Systems Audit and Control Association Inc. (ISACA). (2018). *About*. Retrieved from http://www.isaca.org/about-isaca/Pages/default.aspx

International Organization for Standardization (ISO). (2018). *Popular standards*. Retrieved from https://www.iso.org/popular-standards.html

Jadric, M., Cukusic, M., & Garaca, Z. (2016). Exploring the responsibilities and practices behind information security governance. In *International OFEL Conference on Governance, Management and Entrepreneurship* (p. 328-342). Dubrovnik, Hrvatska: CIRU – Governance Research and Development Centre.

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science, 32*, 489–496. doi:10.1016/j.procs.2014.05.452

Juiz, C., & Tomey, M. (2015). To govern IT, or not to govern IT? *Communications of the ACM,58*(2), 58–64. doi:10.1145/2656385

Kerr, D. S., & Murthy, U. S. (2013). The importance of the CobiT framework IT processes for effective internal control over financial reporting in organizations: An international survey. *Information & Management, 50*(7), 590–597. doi:10.1016/j.im.2013.07.012

Knorst, A. M., Vanti, A. A., Andrade, R. A. E., & Johann, S. L. (2011). Aligning information security with the image of the organization and prioritization based on fuzzy logic for the industrial automation sector. *Journal of Information Systems and Technology Management,8*(3), 555–580. doi:10.4301/S1807-17752011000300003

Landis, E. A., Hill, D., & Harvey, M. R. (2014). A synthesis of leadership theories and styles. *Journal of Management Policy and Practice, 15*, 97–100. Retrieved from http://www.na-businesspress.com/jmppopen.html

Langley, A., Smallman, C., Tsoukas, H., & Van de Ven, A. H. (2013). Process studies of change in organization and management: Unveiling temporality, activity, and flow. *Academy of Management Journal, 56*(1), 1–13. doi:10.5465/amj.2013.4001

Latham, J. R. (2014). Leadership for quality and innovation: Challenges, theories, and a framework for future research. *The Quality Management Journal, 21*(1), 11–15. doi:10.1080/10686967.2014.11918372

Loughlin, C., Arnold, K., & Bell, J. B. (2011). Lost opportunity: Is transformational leadership accurately recognized and rewarded in all managers? *Equality, Diversity and Inclusion, 31*(1), 43–64. doi:10.1108/02610151211199218

Luellig, L., & Frazier, J. (2013). A COBIT approach to regulatory compliance and defensible disposal. *IASCA Journal, 5*, 31-34. Retrieved from https://iasca.com/

Luftman, J. (2003). Assessing IT-business alignment. *Information Systems Management, 20*(4), 9–15. doi:10.1201/1078/43647.20.4.20030901/77287.2

Luftman, J., Dorociak, J., Kempaiah, R., & Rigoni, E. H. (2008). Strategic alignment maturity: A structural equation model validation. Americas Conference on Information Systems AMCIS 2008 Proceedings

Luftman, J., Lyytinen, K., & Zvi, T. (2015). Enhancing the measurement of information technology (IT) business alignment and its influence on company performance. *Journal of Information Technology, 32*(1), 26–46. doi:10.1057/jit.2015.23

Luftman, J. N., Ben-Zvi, T., Dwivedi, R., & Rigoni, E. H. (2012). IT governance: An alignment maturity perspective. In W. van Grembergen (Ed.), *Business Strategy and Applications in Enterprise IT Governance* (pp. 87–101). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-1779-7.ch006

Mahy, Y., Ouzzif, M., & Bouragba, K. (2016). Toward a shared view of IT governance. *International Journal of Innovation, Management and Technology, 7,* 125–131. doi:10.18178/ijimt.2016.7.4.658

McCleskey, J. A. (2014). Situational, transformational, and transactional leadership and leadership development. *Journal of Business Studies Quarterly*, *5*(4), 117 -130. Retrieved from https://jbsq.org

McFadzean, E., Ezingeard, J. N., & Birchall, D. (2011). Information assurance and corporate strategy: A Delphi study of choices, challenges, and developments for the future. *Information Systems Management, 28*(2), 102–129. doi:10.1080/10580530.2011.562127

McGhee, W. E. (2008). *Information technology governance: An exploratory study of the impact of organizational information technology security planning* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses. (304830176).

Mellado, D., Sánchez, L. E., Fernández-Medina, E., & Piattini, M. (2013). *IT security governance innovations: Theory and research*. Hershey, PA: IGI Global. doi:10.4018/978-1-4666-2083-4

Meuser, J. D., Gardner, W. L., Dinh, J. E., Hu, J., Liden, R. C., & Lord, R. G. (2016). A network analysis of leadership theory: The infancy of integration. *Journal of Management,42*(5), 1374–1403. doi:10.1177/0149206316647099

Mind Garden. (2016). *Multifactor Leadership Questionnaire*. Retrieved from http://www.mindgarden.com/products/mlq.htm

Muijs, D. (2010). *Doing quantitative research in education with SPSS*. Atlanta, GA: Sage.

Naseer, H., Shanks, G., Ahmad, A., & Maynard, S. (2016). Enhancing information security risk management with security analytics: A dynamic capabilities perspective. *ACIS2016*. Retrieved from https://ro.uow.edu.au/acis2016/papers/1/52/

Nassaji, H. (2015). Qualitative and descriptive research: Data type versus data analysis. *Language Teaching Research, 19*(2), 129–132. doi:10.1177/1362168815572747

National Institute of Standards and Technology (NIST). (2018). *Computer security resource center*. Retrieved from https://csrc.nist.gov/

National Institute of Standards and Technology (NIST). (2014, April 21). *NIST removed cryptography algorithm from random number generator recommendations*. Retrieved from https://www.nist.gov/news-events/news/2014/04/nist-removes-cryptography-algorithm-random-number-generator-recommendations

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management, 52*(1), 123–134. doi:10.1016/j.im.2014.10.009

Nichols, A. L. (2016). What do people desire in their leaders? The effect of leadership experience on desired leadership traits. *Leadership and Organization Development Journal,37*(5), 658–671. doi:10.1108/LODJ-09-2014-0182

Noland, M., Moran, T., & Kotschwar, B. R. (2016). Is gender diversity profitable? Evidence from a global survey. *Peterson Institute for International Economics* Working Paper No. 16-3. doi:10.2139/ssrn.2729348

Northouse, P. G. (2018). *Leadership: Theory and practice*. Thousand Oaks, CA: Sage.

Novotny, A., Bernroider, E. W. N., & Koch, S. (2012). Dimensions and operationalizations of IT governance: A literature review and meta-case study. *CONF-IRM 2012 Proceedings, Association for Information Systems*. Retrieved from https://aisel.aisnet.org/confirm2012/23/

Nykänen, R., & Hakuli, M. (2013). Information security management system standards: A gap analysis of the risk management in ISO 27001 and KATARI. In J. Blooma, M. Nkhoma, & N. Leung (Eds.), *Proceedings of the 12th European Conference on Information Warfare and Security* (pp. 344-350). Reading, England: Academic Conferences and Publishing International.

Och Dag, K. N., & Storberg-Walker, J. (2014). *Understanding authentic leadership theory from a HRD perspective: Steps toward developing authentic leadership development programs*. Retrieved from https://www.ufhrd.co.uk/wordpress/wp-content/uploads/2014/11/Kristina-Natt-och-Dag.pdf

Odumeru, J. A., & Ifeanyi, G. O. (2013). Transformational vs. transactional leadership theories: Evidence in literature. *International Review of Management and Business Research, 2*, 355–361. Retrieved from http://www.irmbrjournal.com/

Palrecha, R., Spangler, W. D., & Yammarino, F. J. (2012). A comparative study of three leadership approaches in India. *The Leadership Quarterly, 23*(1), 146–163. doi:10.1016/j.leaqua.2011.11.012

Patton, M. Q. (2002). Designing qualitative studies. In *Qualitative Research and Evaluation Methods* (3rd ed., pp. 230–246). Thousand Oaks, CA: Sage.

Penn, A. (2015). *Leadership theory simplified*. Retrieved from https://www.uaex.edu/publications/PDF/FSPSD200.pdf

Phillips, B. (2013). Information technology management practice: Impacts upon effectiveness. *Journal of Organizational and End User Computing, 25*(4), 50–74. doi:10.4018/joeuc.2013100103

Phipps, S. T., & Prieto, L. C. (2011). The influence of personality factors on transformational leadership: Exploring the moderating role of political skill. *International Journal of Leadership Studies, 6*, 430–447. Retrieved from https://www.regent.edu/acad/global/publications/ijls/new/home.htm

Protiviti. (2016). *Understanding the FFIEC cybersecurity assessment tool: An internal audit perspective*. Retrieved from https://www.protiviti.com/sites/default/files/united_states/ffiec-cybersecurity-assessment-tool-ia-perspective-whitepaper-protiviti.pdf

Reyes, F. P. (2015). *Enterprise systems, information security management systems and their impact on enterprise risk: A 3-essay dissertation* (Doctoral dissertation). Retrieved from Digital Commons @ UTEP. (AAI3708557)

Richard, P. J., Devinney, T. M., Yip, G. S., & Johnson, G. (2009). Measuring organizational performance: Towards methodological best practice. *Journal of Management, 35*(3), 718–804. doi:10.1177/0149206308330560

Rid, T., & Buchanan, B. (2015). Attributing cyber-attacks. *The Journal of Strategic Studies,38*(1-2), 4–37. doi:10.1080/01402390.2014.977382

Ristov, S., & Gusev, M. (2013). *Security evaluation of open source clouds. In 2013 IEEE EUROCON* (pp. 73–80). Washington, DC: IEEE Computer Society; doi:10.1109/EUROCON.2013.6624968

Ritchey, F. (2008). *The statistical imagination: Elementary statistics for the social sciences*(2nd ed.). Boston, MA: McGraw-Hill.

Robbins, S. P., Judge, T. A., & Sanghi, S. (2007). *Organizational Behavior* (12th ed.). India: Pearson.

Russell, E. (2011). *Leadership theories and style: a traditional approach*. Unpublished manuscript submitted for the General Douglas MacArthur Military Leadership Writing Competition.

Sadeghi, A., & Pihie, Z. A. L. (2012). Transformational leadership and its predictive effects on leadership effectiveness. *International Journal of Business and Social Science, 3*(7), 186–197. Retrieved from http://www.ijbssnet.com/

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70–82. doi:10.1016/j.cose.2015.10.006

Salter, C., Green, M., Duncan, P., Berre, A., & Torti, C. (2010). Virtual communication, transformational leadership, and implicit leadership. *The Journal of Leadership Studies*, *4*(2), 6–17. doi:10.1002/jls.20164

Salter, C., Harris, M., & McCormack, J. (2014). *Bass & Avolio's full range leadership model and moral development*. Retrieved from https://www.g-casa.com/conferences/milan/paper/McCormack.pdf

Sarantakos, S. (2013). *Social research* (4th ed.). New York, NY: Palgrave Macmillan. doi:10.1007/978-1-137-29247-6

Shao, Z., Feng, Y., & Liu, L. (2012). The mediating effect of organizational culture and knowledge sharing on transformational leadership and enterprise resource planning systems success: An empirical study in China. *Computers in Human Behavior*, *28*(6), 2400–2413. doi:10.1016/j.chb.2012.07.011

Smallwood, R. F. (2014). *Information governance: Concepts, strategies, and best practices*. Hoboken, NJ: John Wiley & Sons.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs a more holistic approach: A literature review. *International Journal of Information Management*,*36*(2), 215–225. doi:10.1016/j.ijinfomgt.2015.11.009

Stafford, M. (2010). *The full-range leadership model: A brief primer*. Retrieved from https://www.holmcenter.com/

Stanford University. (2018). *Consortium for research on information security and policy*. Retrieved from https://fsi.stanford.edu/research/consortium_for_research_on_information_security_and_policy

Stair, R. M., & Reynolds, G. W. (2010). *Principles of information systems, course technology*(9th ed.). New York, NY: Mc-Graw-Hill.

Stilgoe, J., Lock, S. J., & Wilsdon, J. (2014). Why should we promote public engagement with science? *Public Understanding of Science (Bristol, England)*, *23*(1), 4–15. doi:10.1177/0963662513518154

Stone, A. G., Russell, R. F., & Patterson, K. (2004). Transformational versus servant leadership: A difference in leader focus. *Leadership and Organization Development Journal*, *25*(4), 349–361. doi:10.1108/01437730410538671

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences*, *11*(5), 23–29. Retrieved from http://ijens.org/ijecs.html

Swanson, R. A., & Holton, E. F., III. (2005). *Research in organizations: Foundations and methods in the inquiry*. San Francisco, CA: Berrett-Koehler.

Taylor, T. Z., Psotka, J., & Legree, P. (2015). Relationships among applications of tacit knowledge and transformational/transactional leader styles: An exploratory comparison of the MLQ and TKML. *Leadership and Organization Development Journal, 36*(2), 120–136. doi:10.1108/LODJ-01-2013-0008

Thite, M. (2000). Leadership styles in information technology projects. *International Journal of Project Management, 18*(4), 235–241. doi:10.1016/S0263-7863(99)00021-6

Trochim, W. M. (2006). *Descriptive statistics*. Retrieved from https://socialresearchmethods.net/kb/statdesc.php

Trochim, W. M., Donnelly, J. P., & Arora, K. (2016). *Research methods: The essential knowledge base*. Boston, MA: Cengage Learning.

Tu, Z., & Yuan, Y. (2014, August). *Critical success factors analysis on effective information security management: A literature review*. Paper presented at the Twentieth Americas Conference on Information Systems, Savannah, Georgia.

Turel, O., & Bart, C. (2014). Board-level IT governance and organizational performance. *European Journal of Information Systems, 23*(2), 223-239. doi:10.1057/ejis.2012.61

Tyssen, A. K., Wald, A., & Spieth, P. (2014). The challenge of transactional and transformational leadership in projects. *International Journal of Project Management, 32*(3), 365–375. doi:10.1016/j.ijproman.2013.05.010

United States Bureau of Labor Statistics (BLS). (2018). *Home*. Retrieved from https://www.bls.gov/home.htm?view_full

United States Government Accountability Office (GAO). (2009). *Federal information system controls audit manual (FISCAM)* [GAO-09-232G]. Retrieved from https://www.gao.gov/new.items/d09232g.pdf

US Department of Health and Human Services. (1979). The Belmont report.

Vaast, E., & Walsham, G. (2013). Grounded theorizing for electronically mediated social contexts. *European Journal of Information Systems, 22*(1), 9–25. doi:10.1057/ejis.2011.26

Van, B. A., Coleman, A. N., & Simpson, J. A. (2014). Development of the Vannsimpco Leadership Survey: A delination of hybrid leadership styles, *SBS Journal of Applied Business Research, 3*, 28-38. Retrieved from https://jabr.sbs.edu/vol3/02_Vann-Coleman-Simpson.pdf

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

Von Solms, S. H., & Von Solms, R. (2009). *Information security governance*. New York, NY: Springer. doi:10.1007/978-0-387-79984-1

Warrilow, S. (2012). Transformational leadership theory – The 4 key components in leading change & managing change. Retrieved from http://ezinearticles.com/?Transformational-Leadership-Theory---The-4-Key-Components-in-Leading-Change-and-Managing-Change&id=2755277

Wheeler, E. (2011). *Security risk management: Building an information security risk management program from the ground up*. Waltham, MA: Elsevier.

White, H. (2013). *The China choice: Why we should share power*. Oxford, England: Oxford University Press.

Williams, S. P., Hardy, C. A., & Holgate, J. A. (2013). Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective. *Electronic Markets*, *23*(4), 341-354.doi:10.1007/s12525-013-0137-3

Wu, S. P. J., Straub, D. W., & Liang, T. P. (2015). How information technology governance mechanisms and strategic alignment influence organizational performance: Insights from a matched survey of business and IT managers. *Management Information Systems Quarterly*,*39*(2), 497–518. doi:10.25300/MISQ/2015/39.2.10

Yukl, G., & Mahsud, R. (2010). Why flexible and adaptive leadership is essential. *Consulting Psychology Journal, 62*(2), 81–93. doi:10.1037/a0019835

Yukl, G. A. (1989). *Leadership in organizations* (2nd ed.). Englewood Cliffs, NJ: Prentice Hall.

Zhu, W., Sosik, J. J., Riggio, R. E., & Yang, B. (2012). Relationships between transformational and active transactional leadership and followers' organizational identification: The role of psychological empowerment. *Journal of Behavioral and Applied Management, 13,* 186–212. Retrieved from https://jbam.scholasticahq.com/

STATEMENT OF ORIGINAL WORK

Academic Honesty Policy

Capella University's Academic Honesty Policy (3.01.01) holds learners accountable for the integrity of work they submit, which includes but is not limited to discussion postings, assignments, comprehensive exams, and the dissertation or capstone project.

Established in the Policy are the expectations for original work, rationale for the policy, definition of terms that pertain to academic honesty and original work, and disciplinary consequences of academic dishonesty. Also stated in the Policy is the expectation that learners will follow APA rules for citing another person's ideas or works.

The following standards for original work and definition of *plagiarism* are discussed in the Policy:

> Learners are expected to be the sole authors of their work and to acknowledge the authorship of others' work through proper citation and reference. Use of another person's ideas, including another learner's, without proper reference or citation, constitutes plagiarism and academic dishonesty and is prohibited conduct. (p. 1)
>
> Plagiarism is one example of academic dishonesty. Plagiarism is presenting someone else's ideas or work as your own. Plagiarism also includes copying verbatim or rephrasing ideas without properly acknowledging the source by author, date, and publication medium. (p. 2)

Capella University's Research Misconduct Policy (3.03.06) holds learners accountable for research integrity. What constitutes research misconduct is discussed in the Policy:

> Research misconduct includes but is not limited to falsification, fabrication, plagiarism, misappropriation, or other practices that seriously deviate from those that are commonly

> accepted within the academic community for proposing, conducting, or reviewing research, or in reporting research results. (p. 1)

Learners failing to abide by these policies are subject to consequences, including but not limited to dismissal or revocation of the degree.

STATEMENT OF ORIGINAL WORK AND SIGNATURE

I have read, understood, and abided by Capella University’s Academic Honesty Policy (3.01.01) and Research Misconduct Policy (3.03.06), including Policy Statements, Rationale, and Definitions.

I attest that this dissertation or capstone project is my own work. Where I have used the ideas or words of others, I have paraphrased, summarized, or used direct quotes following the guidelines set forth in the APA *Publication Manual*.

Learner name
and date Henry Okonofua September 15, 2018