

2019

## Information Systems Security Leadership: An Empirical Study of Behavioral Influences of Leaders on Employees' Security Compliance

Marcus Alan Winkfield  
Nova Southeastern University, winkf1ma@cmich.edu

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



Part of the [Computer Sciences Commons](#)

## Share Feedback About This Item

---

### NSUWorks Citation

Marcus Alan Winkfield. 2019. *Information Systems Security Leadership: An Empirical Study of Behavioral Influences of Leaders on Employees' Security Compliance*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Computing and Engineering. (1099)  
[https://nsuworks.nova.edu/gscis\\_etd/1099](https://nsuworks.nova.edu/gscis_etd/1099).

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

Information Systems Security Leadership: An Empirical Study of  
Behavioral Influences of Leaders on Employees' Security Compliance

by

Marcus Alan Winkfield

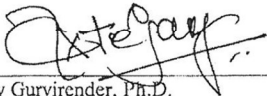
A dissertation submitted in partial fulfillment of the requirements  
for the degree of Doctor of Philosophy in Information Systems

College of Computing and Engineering  
Nova Southeastern University

2019

## Approval Signature Page

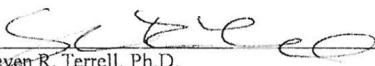
We hereby certify that this dissertation, submitted by Marcus Winkfield conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

  
\_\_\_\_\_  
Tejay Gurvirender, Ph.D.  
Chairperson of Dissertation Committee

12/10/19  
Date

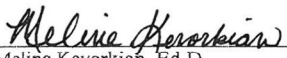
  
\_\_\_\_\_  
Souren Paul, Ph.D.  
Dissertation Committee Member

12/10/19  
Date

  
\_\_\_\_\_  
Steven R. Terrell, Ph.D.  
Dissertation Committee Member

12/10/19  
Date

Approved:

  
\_\_\_\_\_  
Melinc Kevorkian, Ed.D.  
Interim Dean, College of Computing and Engineering

12/10/19  
Date

College of Computing and Engineering  
Nova Southeastern University

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

**Information Systems Security Leadership: An Empirical Study of  
Behavioral Influences of Leaders on Employees' Security Compliance**

by  
Marcus A. Winkfield  
December 2019

This empirical study examined the behavioral influences of leaders on employees' security compliance. Organizations can use leadership concepts in the field of Information Systems (IS) security. Despite the adoption of technical and managerial approaches, organizations still face issues motivating employee IS security compliance. This dissertation argued that organizations need strong leadership to encourage employees. Using the expectancy theory, this paper created a theoretical model to help understand the influence of task and relationship-oriented leadership behaviors on nontechnical controls IS security compliance. The conceptual underpinnings translated into perceived security effort, perceived security performance, and expected security outcomes. The theoretical model was validated using Structural Equation Modeling (SEM) and Confirmatory Factor Analysis (CFA). The model-level results revealed a structural model that suggests task-oriented leadership is better suited for motivating IS security compliance. In addition, individual-level results provide additional support that task-oriented leadership was the only leadership behavior with a direct relationship with IS security compliance. These findings contribute to the body of knowledge that compliance behaviors are extrinsically motivated. Future research should aim to further examine the role of intrinsic motivators, and the indirect influence of relationship-oriented leadership behaviors on IS security policy compliance with more rigorous approaches.

## **Acknowledgements**

Firstly, I would like to express my sincere gratitude to my advisor Dr. Gurvirender Tejay for his continuous support of my Ph.D study and related research—for his directness, support, and immense knowledge was invaluable. I'll never forget the experience of his lectures and one-on-one teachings: his guidance not only helped me but also challenged me to grow intellectually. I could not have imagined having a better advisor and mentor.

Besides my advisor, I would also like to thank the rest of my dissertation committee: Dr. Souren Paul and Dr. Steven Terrell. My committee members were well crafted from the enlightening experiences I had during lectures and performing coursework in their classes. I saw their passion for research, and it inspired me to continue my journey as a researcher.

I give my sincere thanks to Dr. James Parrish and Dr. Ling Wang: without their additional support, it would not be possible to conduct this research. I would also like to thank Dr. Gerard Becker for his encouragement and consultation during my decision to pursue a Ph.D, and providing me a letter of recommendation into the program. Dr. Meena Clowes and Dr. Deirdre Rogers thanks for the support finalizing the dissertation report.

Last but not least, I would like to convey my deepest appreciation to my family and friends who supported me through this lengthy process of intellectual development. My mother is an attentive listener and great supporter. My siblings steer me in the right direction whenever I need help. My friends challenge and remind me there is always more to learn. I hope to inspire my son to follow in his dad's foot-steps and excel even higher in life.

While there are a lot of people who helped me get to where I am, I send my gratitude to all those not explicitly mentioned.

This is not the end of the road, but a start of a new beginning with the knowledge and skills to make a meaningful impact in the field of information systems.

## **Accepted Paper from this Research**

Winkfield, M. A., Parrish, J. L., & Tejay, G. (2017). Information Systems Security Leadership: An Empirical Study of Behavioral Influences. *Twenty-third Americas Conference on Information Systems, Boston*.

# Table of Contents

**Abstract** iii  
**Acknowledgements** iv  
**Table of Contents** v  
**List of Tables** viii  
**List of Figures** ix

## Chapters

**1) Introduction 1**  
1.1. Background 1  
1.2. Research Problem 3  
1.3. Importance of Research Problem 6  
1.4. Definition of Key Terms 8  
1.5. Structure of the Dissertation 9

**2) Literature Review 10**  
2.1. Introduction 10  
2.2. Risk Management, Security Controls, Policy Compliance 10  
2.2.1. Risk Management 10  
2.2.2. Security Controls 13  
2.2.3. Policy Compliance 17  
2.3. Security Leadership 20  
2.3.1. Leadership 21  
2.3.2. Chief Information Security Officers 23  
2.3.3. Organizational Support 26  
2.4. Summary 27

**3) Methodology 28**  
3.1. Introduction 28  
3.1.1. Epistemology 28  
3.2. Theoretical Framework 29  
3.2.1. Theoretical Basis 30  
3.2.2. Research Model 31  
3.2.3. Hypotheses 34  
3.3. Research Design 37  
3.3.1. Research Strategy 37  
3.3.2. Instrument Development 38  
3.3.3. Instrument Validation 44  
3.4. Data Collection 45

3.4.1. Phase I	47
3.4.2. Phase II	48
3.4.3. Phase III	49
3.5. Data Analysis	50
3.5.1. Statistical Technique	50
3.5.2. Statistical Software	52
3.5.3. Goodness of Fit	52
3.6. Empirical Validation	54
3.6.1. Reliability	55
3.6.2. Validity	56
3.7. Summary	57

#### **4) Results 59**

4.1. Introduction	59
4.2. Data Analysis	59
4.2.1. Expert Panel Results	59
4.2.2. Pilot Study Results	60
4.2.3. Pre-Analysis Data Screening	61
4.2.4. Main Study Results	62
4.3. Findings	73
4.4. Summary	75

#### **5) Conclusion 76**

5.1 Introduction	76
5.2 Discussion	76
5.3 Implications	77
5.4 Limitations	80
5.5 Recommendations	82
5.6 Summary	83

#### **Appendices 85**

##### **Appendix A. Approval Letter from Institutional Review Board 86**

##### **Appendix B. Results of Content Validity Ratio 87**

##### **Appendix C. Minimum Values for Content Validity Ratio 89**

##### **Appendix D. Survey Instrument for Pretest and Main Study 90**

##### **Appendix E. Results of Confirmatory Factor Analysis 100**

##### **Appendix F. Regression Analysis for Hypotheses Testing 102**

#### **References 106**

## List of Tables

### Tables

- Table 1. Operationalization of Theoretical Constructs 30
- Table 2. Perceived Effort in IS literature 33
- Table 3. The Measurement of Leadership Behaviors 40
- Table 4. The Measurement of Perceived Security Effort 41
- Table 5. The Measurement of Perceived Security Performance 42
- Table 6. The Measurement of Expected Security Outcomes 44
- Table 7. Sample Descriptive Statistics 63
- Table 8. Organizational Descriptive Statistics 64
- Table 9. Scale Descriptive Statistics and Cronbach's Alpha 66
- Table 10. Results of Structural Equation Modeling 68
- Table 11. Complete SEM Model 69
- Table 12. Non-mediation SEM of ESO 70
- Table 13. Alternative Path Model for Expected Security Outcome 71
- Table 14. Results of Regression Analysis 72



## List of Figures

### Figures

- Figure 1. IS Security Controls in Risk Management Framework 16
- Figure 2. IS Security Controls in International Organization for Standardization: 27001 16
- Figure 3. Information System Security Leadership: Research Model 32
- Figure 4. Pearson's Chi-square Test 54
- Figure 5. Cronbach Coefficient Alpha Formula 55
- Figure 6. Composite Reliability Formula 56
- Figure 7. Average Variance Expected Formula 56
- Figure 8. Results of Structural Equation Modeling 68
- Figure 9. Results of Alternative Structural Equation Model 69
- Figure 10. P-Plot of Regression Residuals 72
- Figure 11. Scatterplot of Regression Residuals 73

## Chapter 1

### Introduction

#### 1.1. Background

The behavioral influences of Information Systems (IS) security leaders are considered essential to motivate employee security compliance (Flores, Antonsen, & Ekstedt, 2014; Guhr, Lebek, & Breitner, 2019; Hu, Dinev, Hart, & Cooke, 2012; Knapp, Marshall, Rainer, & Ford, 2006; Lebek, Guhr, & Breitner, 2014; Merhi & Ahluwalia, 2015). Due to government regulations and industry standards, the critical business importance of Information Technology (IT) means the failure of information security governance programs result in serious personal and corporate liabilities (Von Solms & Von Solms, 2004, 2006, 2018). Researchers have found that employees play a major role in information security management (Stewart & Jürjens, 2017). The importance of employees in information security management is further reinforced by events in industry.

A *Forbes* online news article reported numerous data breaches that affected major corporations: Neiman Marcus, UPS, Dairy Queen, Goodwill, JP Morgan Chase, Staples, Sony, Kmart, and the list could continue (Hardekopf, 2015). According to Jim Garrett, Chief Information Security Officer (CISO) of the Fortune 500 company—3M: “Employees play a key role in protecting a company’s sensitive data because low-tech methods like snooping, social-engineering or phishing are common techniques used by hackers against employees to gain unauthorized access to corporate information” (Schiff,

2013, p. 2). A study reported that 19% of consumers said they would completely stop shopping at a retailer after a breach, and 33% said they would take a break from shopping there for an extended period (Green & Hanbury, 2019). Employee compliance with IS security policies is a pressing issue that security leaders must address for organizations to avoid regulatory compliance risks and security threats as well as fines, penalties, and loss of trust.

The fundamentals of IS security revolve around assets, threats, and vulnerabilities, while IS security controls are countermeasures that mitigate the risk to assets introduced by vulnerabilities (Von Solms & Van Niekerk, 2013). A *Harvard Business Review* article suggests the complexities of security implementations encourage employees to take shortcuts—and their noncompliance introduces vulnerabilities for attackers to exploit (Horenbeeck, 2017). Empirical research using the neutralization theory supports the previous claim: the study found employees use defense of necessity to rationalize security violations and meet work objectives (Cheng, Li, Zhai, & Smyth, 2014; Siponen & Vance, 2010). Despite emergent complexities of advanced IT influencing increased noncompliance of employees, security leaders need to find ways to motivate employee security compliance (Balozian, Leidner, & Warkentin, 2019). Employee IS security compliance is influenced by the culture set by organizational leaders through their implementation of controls such as computer monitoring and security awareness programs (D'Arcy & Greene, 2014).

Security leaders can utilize risk management approaches to balance technical and nontechnical controls at an acceptable level (Cram & D'Arcy, 2016). Although technical controls were once the primary concern in IS security, nontechnical controls have risen as

the dominant concern (Soomro, Shah, & Ahmed, 2016). Insider threat also continues to be a major concern for organizations requiring an increased focus on the human aspects of IS security (Safa, Von Solms, & Fitcher, 2016). Technical controls are only the first wave to IS security—once technical controls (i.e. malicious code protection, encryption, multifactor authentication, vulnerability scanning) are in place, there is a need for an emphasis on improving nontechnical controls (i.e. policies, training, rules of behavior, planning). Technical controls have limitations and are unable to thwart insiders with elevated privileges from violating security policies (Johnston, Warkentin, McBride, & Carter, 2016). Experts suggest complex forms of insider threat, such as fraud, require a mix of technical and nontechnical controls (Goode & Lacey, 2011; Soomro et al., 2016). The remainder of this chapter is organized in several sections. Section 1.2 explains the research problem. Section 1.3 demonstrates the importance of the research problem. Section 1.4 provides a definition of key terms. Section 1.5 offers the structure of the dissertation.

## **1.2. Research Problem**

The research problem was organizations need to further understand behavioral influences of IS security compliance. Employee noncompliance with IS security controls exist for two primary reasons: accidental versus intentional (Warkentin & Willison, 2009; Willison & Warkentin, 2013). Accidental violations involve negligence or lack of awareness, while intentional violations are for accomplishing work objectives or malicious personal gain. Insider threat issues are challenging due to the negative consequences an IS security breach can have on an organization's finances and reputation (Agrafiotis et al., 2015; Berezina, Cobanoglu, Miller, & Kwansa, 2012; Campbell,

Gordon, Loeb, & Zhou, 2003; Goel & Shawky, 2009). Unfortunately, this is the inherent IS security risk of providing employees with legitimate access to perform work functions. There are several options related to risk: avoidance, reduction, transfer, mitigation, and acceptance; however, other than avoidance which is not implementing the technology, there is no way to eliminate risk (Kutsch, Denyer, Hall, & Lee-Kelley, 2013).

Empirical IS security research has provided compelling evidence of the various factors related to employee IS security compliance, including: intrinsic motivators such as penalties and pressures as well as extrinsic motivators like perceived effectiveness (Herath & Rao, 2009), the perception of mandatoriness (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009), rational-based beliefs and awareness (Bulgurcu, Cavusoglu, & Benbasat, 2010), neutralizations (Siponen & Vance, 2010), fear (Johnston & Warkentin, 2010; Johnston, Warkentin, & Siponen, 2015; Son, 2011), poor routine of past and automatic behaviors which have formed a habit (Vance, Siponen, & Pahlila, 2012). Although these research conceptualizations have improved the IS community's understanding of the problem, organizations continue to struggle with creating an organizational culture where employees adhere to IS security controls. A literature review of information security management outlined that security compliance is an ongoing issue because technical implementations have limitations (Soomro et al., 2016).

Rapid technological change is changing how IS security leaders are doing business (Smith, 2014). Researchers suggest there is a demand for strong leadership in IS security (Choi, 2016; Collmann & Cooper, 2007; Da Veiga & Eloff, 2010; Dunkerley & Tejay, 2009; Flores & Ekstedt, 2016; Humaidi & Balakrishnan, 2015). The behaviors of leaders influence organizational performance (Moynihan, Pandey, & Wright, 2012; Wang, Tsui,

& Xin, 2011; Zainudin, Hamid, & Ur-Rahman, 2016). In addition, the behaviors of leaders can positively influence employee adherence with IS security controls, while the lack of leadership can have a negative effect (Flores & Ekstedt, 2016; Furnell & Thomson, 2009). Leadership is listed as a key skill for IS security managers (Haqaf & Koyuncu, 2018).

This research study argued the behaviors of leaders can encourage employees to adhere to IS security controls. The behavioral approach to leadership focuses on “what leaders do and how they act,” and there are two general types of behavior: those focused on accomplishing tasks as well as others focused on strengthening relationships (Northouse, 2016, p. 71). Leadership can be viewed as essential for any organization to implement successful IS security programs. Similarly, IS researches have used the theoretical lens of coerciveness and empowerment to conceptualize management approaches in IS security policy compliance (Balozian et al., 2019). Task-oriented Leadership (ToL) aligns with coercive approaches where authoritarian mechanism are in place to produce an outcome, while Relationship-oriented Leadership (RoL) aligns with empowerment where power is shared with employees. Organizational leaders must tailor their behavioral influences to encourage change and improve all employees’ IS security compliance that reduces risks to IS and the organization (Flores et al., 2014; Kolkowska & Dhillon, 2013).

For this study, employee security compliance with nontechnical controls is viewed as the expected security outcome. Humaidi and Balakrishnan (2015) states there is a lack of behavioral research on leadership’s influence on information security policies (p. 311). The research question that guided this study was: *what leadership behaviors influence the*

*expected security outcomes of IS security policy compliance?* More specifically, the focus was on the expected security outcomes of IS security compliance with nontechnical controls to help organizations understand how to mature past a high-reliance on technical controls. The attempt was to address this question by conceptually developing and empirically testing a theoretical model that was developed from the expectancy theory. Afterwards, survey data collected from a wide range of diverse from different organizations was analyzed with Structural Equation Modeling (SEM) to measure the predictability of the developed model.

### **1.3. Importance of Research Problem**

Technology alone is not enough to address modern IS security compliance issues—there are various human aspects to IS security that require behavioral changes of employees within the organization (Safa et al., 2016). Attackers can target the actions of employee's noncompliance behaviors, which means employees internal to the organization play a key role in improving IS security. The human aspects of IS security require organizations to further explore nontechnical aspects of their IS security program. The human aspects are often controlled using policies and procedure; however, this approach does not always translate into employee action. Unfortunately, normative beliefs—both social and personal—have a strong influence on if employees will comply with IS security policies (Yazdanmehr & Wang, 2016). Therefore, there is a strong need to understand how organizations can address this problem in order motivate compliance and improve IS security programs.

Organizations need to develop more intrinsic approaches to motivate employees to comply with IS security policies. Leadership behaviors play a major role in IS security

compliance with nontechnical controls. Leadership concepts are considered intrinsic, while management is considered extrinsic (Northouse, 2016). Therefore, it can be considered essential that organizations adjust their leadership behaviors influence the expected security outcomes of IS security policy compliance. Organizations have been focused on technical implementations without improving the nontechnical aspects. Understanding what leadership behaviors influence the expected security outcomes of IS security policy compliance will help organization better develop their IS security programs.

The purpose of this research study was to address a gap in literature by testing an empirically supported theoretical model for understanding behavioral influences of leaders that encourage employees' IS security compliance with nontechnical controls. Past research has not adequately explored the use of leadership behaviors as a potential solution to mitigate the insider threat issue (Guhr et al., 2019). Mitigating the risk of IS security noncompliance with leadership behaviors can potentially reduce the number of incidents and have a huge impact by saving organizations from numerous financial and legal obligations (Georg, 2017). IS researchers have claimed there is a major void in the theoretical and practical understanding of the role of leaders in IS security (Hu et al., 2012).

This research study addressed the problem from the employee's perspective. There are a few barriers and issues this research study was expected to encounter. Subordinates may be hesitant to answer truthfully to questions about their leaders. Employees may also feel reluctant to respond accurately to questions about their organizational IS security compliance. It is suggested that surveys that question sensitive topics, such as



cybercrimes, are potentially vulnerable to lies from respondents (Florêncio & Herley, 2013). Although these response issues cannot be eliminated, developing a quality instrument by applying rigorous data screening and data analyses is expected to reduce the concern. In addition, emphasizing that the survey results will remain anonymous will reduce these response issues. There is limited research on the role of leadership concepts and theories in academic IS journals (Choi, 2016). This stems from the fact that the primary focus of recent years has been to understand the role of management in IS security (Soomro et al., 2016).

#### **1.4. Definition of Key Terms**

**Information Systems (IS)** – “Systems that provide information used to control, manage, communicate, analyze, or collaborate” (Pearlson & Saunders, 2013, p. 214). “The information system field examines more than just the technological system, or just the social system, or even the two side by side; in addition, it investigates the phenomena that emerge when the two interact” (Boell & Cecez-Kecmanovic, 2015, p. 4961).

**IS Security** – “A well-informed sense of assurance that risks to information resources are in balance with technical, administrative, and behavioral controls” (Barton, Tejay, Lane, & Terrell, 2016, p. 9).

**IS Security Compliance** – Intentional and nonintentional adherence with policies and procedures aimed at controlling the information system environment (Vance et al., 2012).

**IS Security Controls** – Technical and nontechnical measures that are established, implemented, operated, monitored, reviewed, maintained, and improved to ensure the confidentiality, integrity, and availability of organizational information resources (Montesino, Fenz, & Baluja, 2012).

**IS Security Leaders** – Enablers of change to ensure difficult or risky projects have security built in from the beginning. IS Security Leaders generate information about threats, risks and potential consequences, enabling senior executives to decide how to balance cyber security risks against other risks (Johnson, Goetz, & Pfleeger, 2009, p. 6).

**Leadership** – “A process whereby individuals influence a group of individuals to achieve a common goal” (Northouse, 2016, p. 6).

## **1.5. Structure of the Dissertation**

This study was organized in a five-chapter model. **Chapter 1** highlighted the research topic with an introduction to research, problem, and its importance. **Chapter 2** provides a detailed literature review of key topic areas. **Chapter 3** explains the research methodology to include, including the theoretical basis, theoretical model, hypotheses, research design, instrument development, data collection, and analysis with empirical validation approach. **Chapter 4** provides results with a detailed data analysis and representation of findings. **Chapter 5** provides the conclusion with implications and recommendations. These chapters are considered the core ingredients popular in research (Bell, Bryman, & Harley, 2019).

## Chapter 2

### Literature Review

#### 2.1. Introduction

The goal of the literature review was to search and evaluate relevant material to develop a firm understanding of IS security leadership and associated topics. A literature review creates a firm foundation for advancing knowledge in academic projects (Webster & Watson, 2002). To further understand IS security leadership, this literature review investigated published works associated with the following sections. Section 2.2 examine the background of risk management, security controls, and policy compliance. Section 2.3 covers concepts related security and leadership. Lastly, the final section 2.4 summarizes the literature review.

#### 2.2. Risk Management, Security Controls, Policy Compliance

##### 2.2.1. Risk Management

Risk management skills to help conceptualize, assess, and manage risk was rated of top importance for IS security management roles (Haqaf & Koyuncu, 2018). The risk concept extends to several disciplines, such as: finance, safety, engineering, health, supply chain, security (Aven, 2016). For IS security to obtain a competitive advantage, there is a need to develop a framework for assessing systems with a risk-based approach (Shameli-Sendi et al., 2016; Vitale, 1986; Wang et al., 2018). Although there are several definitions to describe risk, the concept of risk can most generally be viewed as “exposure to consequences or negative outcomes” (Shameli-Sendi et al., 2016; Willcocks

& Margetts, 1994, p. 128). According to Straub and Welke (1998), managers cope with IS risk using their perceptions regarding the organizational environment, IS environment, and individual characteristics. Furthermore, Halliday, Badenhorst, and Von Solms (1996) argued conventional risk techniques—asset/threat/vulnerability models are not enough—there is a need for a more suitable approach for smaller organizations, as well as organizations requiring a quicker, more simplified and less resource-intensive approach.

Despite difficulties, many organizations understand it is still in their best interest to manage risk related to the use of information technology (Dhillon & Backhouse, 1996; Shameli-Sendi et al., 2016). Risk management helps managers identify IS risk that are a threat to the success or existence of the organization in time to efficiently cope (Falkner & Hiebl, 2015). Risk management takes as an economic view to quantify the need for security controls (Bojanc & Blažič, 2008; Shameli-Sendi et al., 2016). Managers understand it is often impossible to eliminate risk—although, one-hundred percent security is impossible, organizations can use qualitative risk assessments to brainstorm and quantitative approaches afterwards to further address risk (Rainer, Snyder & Carr, 1991; Shameli-Sendi et al., 2016). Researchers have argued that rather than solely viewing risk analysis as a predictive tool, it should also be viewed as a communication channel between the designer and management – too much statistical rigor could damage the usefulness of the technique (Baskerville, 1991).

Despite the creation of various risk assessment models and frameworks, organizations are having a hard time realizing that an information security plan must be based on identified risk in order to be effective (Shameli-Sendi et al., 2016; Von Solms & Von Solms, 2004, p. 372). The complexity and interconnectedness of IS increased the need for

a more systematic approach to assess risks to critical infrastructures (Longstaff, Chittister, Pethia & Haime, 2000). The complexities encountered in traditional IS suggest a need for a risk assessment approach that has more management participation (Karabacak & Sogukpinar, 2004). The reoccurring theme involves management's dilemma between the advantages and disadvantages between qualitative and quantitative risk management (Munteanu, 2006; Shameli-Sendi et al., 2016).

Organizations have a difficult time selecting the best risk approach that suits their requirements—a framework for risk management terminology was developed to improve efforts of addressing risk (Bromiley, McShane, Nair, & Rustambekov, 2015; Eloff, Labuschagne & Badenhorst, 1993). IS risk assessments are accomplished with quantitative and qualitative approaches (Zang, 2014). Quantitative assessments examine the probability of threat and expected loss on the vulnerability, which are largely achieved with rigorous mathematical calculations (Bodin, Gordon & Loeb, 2008). Quantitative assessments are difficult—requiring a significant amount of time, money, and human resources (Shameli-Sendi, Aghababaei-Barzegar, & Cheriet, 2016). On the other hand, qualitative assessments rely on expert's estimate on expected losses (Feng & Li, 2011). Qualitative assessments lack measurable details, which makes it difficult to prioritize risk (Shameli-Sendi et al., 2016). Researchers have argued both approaches should be used (Alter & Sherer, 2004; Salmela, 2008) due to their strengths and weaknesses (Ryan, Mazzuchi, Ryan, De la Cruz & Cooke, 2012). More specifically, researchers have suggested quantitative—rigorous but resource intense—efforts should be applied to critical resources, while qualitative efforts should be the focus for non-critical resources (Shameli-Sendi et al., 2016). There is a need to understand how

managers can separate these critical and non-critical resources to improve risk assessment efforts (Shameli-Sendi et al., 2016). This study defines risk management: “the overall risk control process, including personnel, physical, and technical measures” (Blakley, McDermott, & Geer, p. 103). Based on the literature, the development of more sophisticated risk management approaches is likely the solution to addressing modern IS security concerns.

### *2.2.2. Security Controls*

This study defines security as “a well-informed sense of assurance that risks to information resources are in balance with technical, administrative, and behavioral controls” (Barton et al., 2016, p. 9). Information security concerns are a major issue for organizations (Hu, Hart, & Cooke, 2007; Safa et al., 2016; Willison, 2006). The need to advance information security measures with security controls has become more important as organizations become more dependent on IS (Cavusoglu, Cavusoglu, & Raghunathan, 2004; Lee, Geng, & Raghunathan, 2016). Additionally, the risks associated with IS are now further evaluated from various aspects due to the significant consequences of an information security breach. The reality is security breaches usually have monetary damages, as well as corporate liability and loss of credibility (Cavusoglu et al., 2004; Lee et al., 2016). These consequences have spurred a need to examine information security holistically, where all related aspects are considered with the ultimate aim of reducing information security risks (Baskerville, 1988; Posthumus & Von Solms, 2004; Soomro et al., 2016).

Technical resources play an important role in information security, but should not be the only resource applied to manage risks (Bulgurcu et al., 2010; Posthumus & Von

Solms, 2004). Although in the past information security was considered solely a technical issue, it is now also viewed as a non-technical issue (Herath et al., 2009) or socio-organizational issue (Dhillon & Backhouse, 2001). Organizations must now have effective policies and procedures to manage the behaviors of employees, who are often the biggest vulnerability due to their privileged access to perform their roles (Boss et al., 2009; Hu, West, & Smarandescu, 2015). Non-technical approaches increase information security measures by managing behavioral and organizational issues that increase risks (Bulgurcu et al., 2010).

Employees play a major role in protecting sensitive resources, so it is important to have up-to-date security policies that effectively communicate the importance of information security (Schiff, 2013). On the other hand, employees often place organizations in danger when violating security policies (Siponen, Pahnla, & Mahmood, 2010). According to Hu et al. (2015), “employee security policy violations can be defined as any act by an employee using computers against the established rules and policies of an organization regardless of the motives” (p. 7). Unfortunately, information security professionals label employees as the primary challenge for organizations (Schiff, 2013). Employees tend to use neutralization techniques to rationalize their negligent behavior (Vaast, 2007); employees may also have different perspectives of the importance of security policies due to their communities’ role in the organization (Siponen & Vance, 2010). The dilemma is that policies have limited effectiveness without employees being motivated to adhere to them (Boss et al., 2009). Due to the significant problem of employee non-compliance, there is a need to further understand ways to address IS security policy compliance (Herath & Rao, 2009).

Past research has aimed to understand information security issues from different disciplines (Anderson & Moore, 2009). These different disciplines—psychology, economics, criminology, sociology, etc.—aim to understand how to address various issues, such as information security policy non-compliance. Prior theoretical perspectives that have been used to understand IS security policy compliance have produced a conceptual understanding of related behavioral factors but have lacked practical applicability for industry leaders regarding motivating individuals to comply with information security policies. More specifically, these past studies aimed to understand what behaviors motivate individual compliance—but failed to explain what behaviors senior managers and information security managers should employ to motivate subordinates to comply. The current research study defines information security as all the goals relevant to the management of data through an organization’s information system, and security risks arise due to a failure in managing these goals (Koskosas & Asimopoulos, 2011). Security controls are technical and nontechnical measures that are established, implemented, operated, monitored, reviewed, maintained, and improved to ensure the confidentiality, integrity, and availability of organizational information resources (Montesino, Fenz, & Baluja, 2012). Effective systems security involves a continuous process of identifying and prioritizing risks, implementing safeguards or countermeasures, and constantly monitoring those controls to ensure risks are mitigated (Brock & Levy, 2013; Spears & Barki, 2010). Typically attempts to develop effective information system security measurements are often unsuccessful due to the inability to either identify all security expenditures within an organization or due to a lack of available expenditure data (Brock & Levy, 2013).



There are two popular frameworks security controls: National Institute of Standards and Technology (NIST) created the Risk Management Framework (RMF) and International Organization for Standardization (ISO) created 270001. While RMF is primarily used in the United States especially in the federal government (Figure 1), ISO 27001 is used worldwide (Figure 2). Although both frameworks take a different approach, they both have the same end goal of improving IS security.

**Figure 1.** IS Security Controls in Risk Management Framework

Class	Family	ID
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

**Figure 2.** IS Security Controls in International Organization for Standardization: 27001



The application of security controls provides a goal-oriented mission. Consistent with other IS researchers, this research study takes a goal-oriented view that perceives

information security as a collection of goals to accomplish to manage risks (Oladimeji, Supakkul, & Chung, 2006; Elahi & Yu, 2007; Koskosas & Asimopoulos, 2011).

Information security can be viewed as the aggregate of all the goals that are relevant to the management of data through an organization's information system, and security risks arise due to a failure in managing these goals (Koskosas & Asimopoulos, 2011). Goal setting, especially in areas regarding human factors and behaviors, has the potential to improve information security management because a goal can be used to consciously and unconsciously drive human activities (Koskosas & Asimopoulos, 2011). This view ties in well to the current behavioral research study, which aims to understand the role of leadership when communicating information security goals to encourage organizational support in the management of critical information resources. Goal setting is a pertinent part of the overall risk management process (Koskosas & Asimopoulos, 2011). A corporate information security policy is a starting point and reference point for organizations to develop sub-policies, procedures, and standards for business users to adhere (Von Solms & Von Solms, 2004). There are multiple goals to be achieved in information security; in the current research study, the goal to be achieved was IS security policy compliance. This research study aimed to examine how organizations can motivate information security policy compliance to reduce the risks associated with employees.

### *2.2.3. Policy Compliance*

The human factors of information security produced a need to understand how organizational leaders can motivate IS security policy compliance (Safa et al., 2016).

Consistent with other IS researchers, this research study takes a goal-oriented view that

perceives information security as a collection of goals to obtain to manage IS risks (Elahi & Yu, 2007; Koskosas & Asimopoulos, 2011; Oladimeji et al., 2006; Shropshire, Warkentin, & Sharma, 2015). Security compliance with policies is often divided into two categories: actual compliance and the intention to comply because an individual's intention is not always a reflection of actual behavior (Siponen et al., 2010). Actual compliance means "users comply, recommend others to comply, and assist others in complying;" but, the intention to comply refers to the "intent to comply, intent to recommend others to comply, and the intent to assist others to in complying" (Siponen et al., 2010, pg. 66). Security policies are extremely important for organizations; more importantly, employees must adhere to security policies to reduce the risk of security incidents. The goal is to promote actual and intentional compliance of individuals through the influence of leadership behaviors.

Security violations are a breach of compliance, which can be defined as "any act by an employee using computers that is against the established rules and policies of an organization for personal gain" (Hu, Xu, Dinev, & Ling, 2011, p. 54). Boss et al. (2009) aimed to understand how organizations could motivate security compliance, and found the act of specifying policies and evaluating behaviors are effective in motivating individuals because policies become viewed as mandatory. However, this is a major assumption, even when policies are specified as mandatory they may still not be followed. In addition, Boss et al. (2009) also found that rewards are not a significant factor in influencing compliance through the perception of mandatoriness. Siponen, Pahnla, and Mahmood (2010) also found rewards to be negatively associated with security compliance. These research findings suggest a need to look beyond the use of

rewards. Vance et al. (2012) argued security non-compliance issues are often caused by habit, which means individuals are caught in routine behavior that goes against security policies. Therefore, organizations need to have deterrence mechanisms in place to change the habitual behaviors of users.

Deterrence mechanisms are highly relied upon to encourage security compliance. Johnston and Warkentin (2010) highlighted the importance of incorporating fear-inducing communication to persuade end-users intentions to follow recommended individual security actions. Later, Johnston, Warkentin, & Siponen (2015) extended the conventional fear appeal model by adding personal relevance with sanctions. There should to be personal relevance with sanctions for deterrence mechanisms to be effective because employees with preconventional moral reasoning make decisions based on personal interest to avoid sanctions (Myry, Siponen, Pahlila, Vartiainen, & Vance, 2009). Additionally, users apply neutralization techniques and rationalize their workplace behavior violating security polices (Siponen & Vance, 2010). In short, deterrence-based approaches alone will often fail (Hu et al., 2011).

The weaknesses in deterrence mechanisms suggest a need for intrinsic forms of security compliance (Son, 2011), such as: socialization, influence, beliefs and cognition (Ifinedo, 2014) or personality factors (Shropshire et al., 2015). Herath and Rao (2009) emphasized the importance of extrinsic and intrinsic motivators to encourage security compliance; however, Son (2011) observed that although extrinsic factors are important, intrinsic factors have an increased chance of motivating security compliance. An intrinsic approach would likely be more successful because individuals are rationally influenced to comply with security policies based on normative beliefs, self-efficacy, and attitudes

(Bulgurcu et al., 2010). The perceived benefit often overshadows the perceived risk during the process of rationally calculating security compliance, which introduces a need to examine intrinsic factors such as self-control and moral beliefs (Hu et al., 2011). This approach requires strong awareness programs. Without user awareness, all other measures will likely fall short (Siponen & Kajava, 1998); it is important for user's education and training to develop intrinsic motivation to encourage security compliance (Siponen, 2000). More advanced awareness programs are necessary for computer savvy employees who may believe they can subvert controls (D'Arcy & Hovav, 2009). To sum it up, security compliance is a complex issue that requires numerous nontechnical considerations to be effective.

### **2.3. Security Leadership**

Research results found that leadership is especially important for businesses because they often lack the resources for costly implementations (Bhattacharya, 2011). This has given rise to the importance of strong leadership in IS security has become a popular topic. According to Dunkerley and Tejay (2009), "organizations will require strong leadership that understands how to define information security success within that organization's context, necessitating individuals who understand both information security needs of the organization (p. 5). Strong leadership is suggested to play a major role in achieving operational effectiveness (Flores & Ekstedt, 2016). In addition, strong leadership is also suggested to play a major role in developing the organizational culture (Choi, 2016; Collmann & Cooper, 2007). More importantly to this study, strong leadership can guide groups by motivating them to comply with information security policies (Da Veiga & Eloff, 2010; Humaidi & Balakrishnan, 2015). Therefore,

understanding what leadership behaviors motivate IS security compliance with nontechnical controls is important to improving IS security in organizations.

### *2.3.1. Leadership*

Leadership and management are not synonymous—the primary difference between management and leadership is: management is focused on “controlling”, and leadership is focused on the “creation of a common vision” (Weathersby, 1999, p. 5). Additionally, management motivates extrinsically, while leadership also motivates intrinsically by satisfying very basic human needs (Kotter, 1990). Strong management without leadership is unlikely to be successful—“the outcome can be stifling and bureaucratic” (Northouse, 2016, p. 13). After management approaches have been used to establish fundamental business goals and processes, leadership—especially in dynamic environments—is needed to establish direction, motivate, and align people to achieve a common goal (Kotter, 1990).

Leadership is also not the same as power; however, leadership involves the use of power (Northouse, 2016). Hollander and Offermann (1990) suggested there are only three forms of power in leadership: “implicit or explicit dominance, empowerment, and resistance to the power of others” (p. 179). Other experts have presented there are several forms of power: “legitimate, referent, coercive, information, reward, and expert” (Northouse, 2016, p. 10). There is also tension between leadership and power—leaders sometimes focus too much on power instead of leadership and sacrifice group goals for personal benefits (Maner & Mead, 2010). However, the consensus is that power is not the same as leadership—but power does play a role in influencing groups of people (Northouse 2016).

There is a fundamental divergence of opinion in leadership literature regarding whether individuals are born leaders or made leaders (Marques, 2010). In earlier research, it was believed that people were born with certain unique traits and skills not found in everyone—The Great Man Theory (Borgatta, Bales, & Couch, 1954). The trait approach determines leadership potential based on the characteristics of a person (i.e. intelligence, height, etc), and the skill approach refers to an individual’s competency to perform tasks (i.e. communication, problem solving, etc.) well (Northouse, 2016). Instead of being born a leader with unique traits or skills, other studies have been focusing on the behavioral aspects of leadership (Northouse, 2016). As stated earlier, the behavioral approach to leadership focuses on “what leaders do and how they act,” and there are two general types of behavior: those focused on accomplishing tasks, as well as others focused on building relationships (Northouse, 2016, p. 71). More specifically to this research study, leaders are those who display certain behaviors to influence followers. Leadership behaviors both task-oriented and relationship-oriented have a positive and significant association with organizational climate (Holloway, 2012).

Regarding the IS security context, the attitudes and behaviors of users play a key role in applying protective information technologies (Dinev, Goo, Hu, & Nam, 2009). Furthermore, the intrinsic and extrinsic factors of attitudes and behaviors encourage security compliance (Herath & Rao, 2009). Research found leadership behaviors have a direct effect on an individual’s attitudes and behaviors (Momeni, 2009). Siponen et al. (2010) supports this view that the behaviors of managers have a persuasive effect on employees to comply. Therefore, it can be assumed the leadership behaviors applied by

senior managers and security managers can modify the attitudes and behaviors of employees to motivate the IS security policy compliance of individuals.

### *2.3.2. Chief Information Security Officers*

Information security has shifted from a technical problem to a non-technical issue (Herath & Rao, 2009), socio-organizational issue (Dhillon & Backhouse, 2001), or institutional issue (Von Solms, 2001) that requires senior management to be more actively involved (Soomro et al., 2016). Delegated with the role of protecting critical company information resources (Fitzgerald, 2007), Chief Information Security Officers (CISOs) are faced with various challenges related to power, role identity, and employee involvement (Ashenden & Sasse, 2013). CISOs in many corporate environments lack organizational support, and are considered to have one of the most arduous roles for modern business professionals (Perloth, 2014). Furthermore, there is a lack of empirical research aiming to understand how CISOs can excel as information security leaders (Whitten, 2008). To build on existing studies (Ashenden & Sasse, 2013; Fitzgerald, 2007; Whitten, 2008), research is needed to understand how CISOs can excel as information security leaders.

Chief Information Security Officers (CISO), a relatively new title to be added to the C-suite, is responsible for a wide-array of information security responsibilities: “facilitating the implementation and ongoing compliance with the multiple domains of the common body of knowledge, such as risk management, operations security, physical security, business continuity, laws and ethics, network security, and so forth” (Fitzgerald, 2007, p. 262). In addition, CISOs may fall under different titles (Johnson & Goetz, 2007); for example, a CISO may be labeled as a “security manager, security director, or



information security officer” (Fitzgerald, 2007, 262). However, regardless of the title, CISOs are placed in charge of corporate IS security (Whitten, 2008).

CISOs need IT skills, but they require soft skills: communication and leadership (Whitten, 2008). These skills are needed for contracts, negotiations, mentors, and presentations. Based on experience on CISO job listings, Whitten (2008) found 61% included communication skills and 39% included leadership skills. Ashenden and Sasse (2013) recommended CISOs need to act as change agents and manage how language is communicated and received by employees to effectively deliver information security goals. Additionally, Koskosas and Asimopoulos (2011) suggested information security managers should enhance cooperation using effective communication with the aim of steering groups towards a common goal. Security involves more than the CISO—information security needs to be extended throughout the organization to get all employees to accept their leadership responsibly (Whitten, 2008). CISOs need use communication to act as change agents and remove blockages that prevent information security from becoming viewed as only a concern for specialists (Ashenden & Sasse, 2013).

According to Ashenden and Sasse (2013), there is a need for a more active leadership approach and effective communication of information security goals to change the organization. CISOs must effectively communicate business problems being resolved and inculcate information security throughout the company to obtain organizational support from employees (Johnson & Goetz, 2007). Leadership behaviors are pertinent to successful accomplishments in organizations (Holloway, 2012). Regarding the IS security context, the attitudes and behaviors of users play a key role in applying

protective information technologies (Dinev et al., 2009). Furthermore, the intrinsic and extrinsic factors of attitudes and behaviors influence information security (Herath & Rao, 2009). Research found leadership behaviors have a direct effect on an individual's attitudes and behaviors (Momeni, 2009). Therefore, information security goals can be achieved when CISOs use certain leadership behaviors to motivate employees' organizational support. What behavioral factors related to leadership produce motivation organizational support?

Numerous publications have acknowledged the need for senior information security professionals (CISOs) to have strong communication skills (Ashenden & Sasse, 2013; Bradbury, 2011; Johnson & Goetz, 2007; Koskosas & Asimopoulos, 2011; Whitten, 2008). Faced with a dynamic job role, CISOs must primarily have a firm understanding of how to communicate in languages both business and technical (Bradbury, 2011; Whitten, 2008). However, in the corporate suite (C-suite), technical expertise is not as important as adept leadership skills and business fundamentals (Groysberg, Kelly, & MacDonald, 2011). Insufficient communication causes employees to develop their own models and degrades their ability to understand the value of their support (Adams & Sasse, 1999). Instead of using a one-way approach of authoritatively announcing current information security actions, CISOs need to effectively communicate organizational business problems being resolved (Ashenden & Sasse, 2013; Johnson & Goetz, 2007). More specifically, "genuine two-way communication with employees, negotiation and involvement to overcome the often observed 'them' and 'us' relationship, and an acceptance that mistakes and errors will occur" (Ashenden & Sasse, 2013, p. 16).

To extend Johnson and Goetz's (2007) argument, CISOs can excel as security leaders by communicating to influence subordinates' perception of their work goals, as well as personal goals and paths to the attainment of goals. Moreover, this form of information security leadership will help employees actualize the relative worth of information security implementations to increase company-wide support. Overall, this is a more active approach for security leaders in the management of critical information resources. Not only will this provide a more practical method for understanding how CISOs can excel as security leaders, this will also contribute to a lack of information security research related to goals, leadership, and the role CISOs. Fundamentally, the role of motivating individuals can be viewed as a leadership issue—effective leaders create highly motivating work environments (Isaac, Zerbe, & Pitt, 2001). Therefore, it can be deduced the next step in influencing IS security policy compliance involves examining the role of leadership. Respectively, leadership concepts can be applied in the realm of information security to provide a better understanding of how organizations can motivate IS security policy compliance, both theoretically and practically.

### *2.3.3. Organizational Support*

Researchers have suggested information security should also be viewed as a goal by top management to motivate a change in behavior (Koskosas & Asimopoulos, 2011; Soomro et al., 2016). Unfortunately, practitioners rank organizational support—top management and user awareness—as the peak of organizational information security issues (Knapp et al., 2006). Organizations require support from management and users improve information security (Knapp et al., 2006). Top management support information security through information security governance, which consists of leadership,

organizational structures, and processes in the protection of corporate information assets (Johnston & Hale, 2009). Although it is often overlooked, middle management also plays an important day-by-day role and might represent the biggest barrier to transforming the organization (Johnson & Goetz, 2007). The involvement of middle management helps spread the responsibility and accountability for information security to lower levels (Johnson & Goetz, 2007). Middle management can help end-users understand how security applies to their daily operations and enforce training, awareness, and policy compliance (Johnson & Goetz, 2007). Senior management has an influence on information security, but there is a need for additional research to further understand the relationship (Cuganesan, Steele, & Hart, 2018). Organizational support plays a major role in corporate information security. The next section presents a summary of the literature review.

#### **2.4. Summary**

The goal of the literature review was to provide a firm understanding of IS security leadership and associated topics. To further understand IS security leadership, this literature review investigated published works associated with the following sections. This first section outlined the literature review. The second section examined the foundations of IS security. The third section investigated security controls, policy compliance, and risk management. The fourth section covered leadership. Lastly, the fifth section collectively discussed IS security leadership. An exhaustive review of the literature yielded that there is a gap in research applying leadership theories and concepts to understand the behaviors of leader's on employee IS security policy compliance. The next chapter explains the methodology used in the study.

## Chapter 3

### Methodology

#### 3.1. Introduction

The primary purpose of this chapter was to provide a methodology for understanding the behavioral influences of leaders on employees' security compliance. After the identification of a research-worthy problem along with a detailed literature review, a major challenge for researchers is matching the appropriate method with a research study (Ellis & Levy, 2009; Terrell, 2015). Researchers must outline the approach taken with clear justification. This section explains the methodology and provides the epistemology behind the chosen approach. Section 3.2 describes the theoretical framework to include the basis, model, and hypotheses. Section 3.3 covers the research design to include the strategy, instrument development, and validation. Section 3.4 explains the planned for data collection. Section 3.5 explains the approach data analysis. Section 3.6 outlines the empirical validation for reliability and validity. Lastly, Section 3.7 provides a summary of the methodology.

##### *3.1.1. Epistemology*

There are primarily four philosophical worldview assumptions: postpositivism, constructivism, transformative, and pragmatism. This study's research design followed a postpositivist approach. The term postpositivist was derived after an attempt in the research community to rethink traditional notions of positivist research (Creswell, 2014). The postpositivist philosophical worldview holds key assumptions: "(1) knowledge is

conjectural; (2) research is the process of making claims and then refining or abandoning some of them for other claims more strongly warranted; (3) data evidence, and rational considerations shape knowledge; (4) researchers advance the relationship among variables and pose this in terms of questions or hypotheses; (5) being objective is an essential aspect of competent inquiry” (Creswell, 2014, p. 7).

In IS research, positivist/postpositivist research was considered the dominant paradigm with a well-respected approach for research validation (Orlikowski & Baroudi, 1991; Venkatesh, Brown, & Bala, 2013). Researchers with a postpositivism epistemology aim to expand knowledge through theory development and verification using observations and measurements (Creswell, 2014). Unlike constructivism, which places an emphasis on qualitative research, postpositivism primarily uses quantitative research approaches (Creswell, 2014). This research study aimed to develop and verify a better theoretical understanding of the relationship between the behavioral influences of leaders and employee’s IS security compliance with nontechnical controls from a postpositivist perspective. Therefore, quantitative research was an appropriate approach for this study.

### **3.2. Theoretical Framework**

According to Imenda (2014), a theoretical framework involves the use of theory to deductively guide the research study. Deductive research involves testing and validating an existing theory in the proposed study rather creating a brand new one. Theory in quantitative research provides supporting logic for interconnecting constructs that aligns with the research problem and research questions (Creswell, 2014). The process involves selecting a relevant theoretical basis that supports the research model and hypothesis. The next section presents the theoretical basis.

### 3.2.1. Theoretical Basis

This study adopted Vroom's (1964) *Expectancy Theory*, as the theoretical basis to understand the behavioral influences of leaders that motivate IS security compliance with nontechnical controls by examining expectancy, instrumentality, and valence. The expectancy theory argues individuals behave in a specific manner because they are motivated to choose a distinct behavior over other behaviors based on what they expect the outcome will be (Vroom, 1964). Expectancy, instrumentality, and valence are the primary categories (Table 1), which has been used in other IS research studies to understand human motivations (Burton, Chen, Grover, & Stewart, 1992; Hann, Hui, Lee, & Png, 2007; Liu, Liao, & Zeng, 2007; Snead & Harrell, 1994). The expectancy theory has several basic assumptions: "(1) a subjective measure of expectancy; (2) independence between expectancies and valences; (3) a multiplicative interaction between expectancies and valences; (4) instrumentality as a determinant of valence" (Reinhardt & Wahba, 1975, p. 522).

**Table 1.** Operationalization of Theoretical Constructs

<b>Theoretical Constructs</b>	<b>Variable</b>	<b>Description</b>
Expectancy	Perceived Effort (PE)	The belief that one's effort will result in the attainment of desired performance goals (Vroom, 1964).
Instrumentality	Perceived Performance (PP)	The belief that a person will receive a reward if the performance expectation is achieved (Vroom, 1964).
Valence	Expected Outcome (EO)	The extent to which a person values a given outcome or reward (Vroom, 1964).

The expectancy theory is considered a good fit for understanding individual behaviors and work performances (Vroom, 1995). This theory is also considered well-suited for understanding how individuals are motivated by their leaders (Isaac et al., 2001). This theory was used to develop the path-goal leadership approach (Northouse, 2016). However, these three constructs have not been used to understand behaviors of leaders that motivate IS security compliance with nontechnical controls. Since an employees' IS security compliance is part of their work performance, the expectancy theory was considered appropriate to understand the behavioral influences of leaders that motivate IS security compliance with nontechnical controls.

### *3.2.2. Research Model*

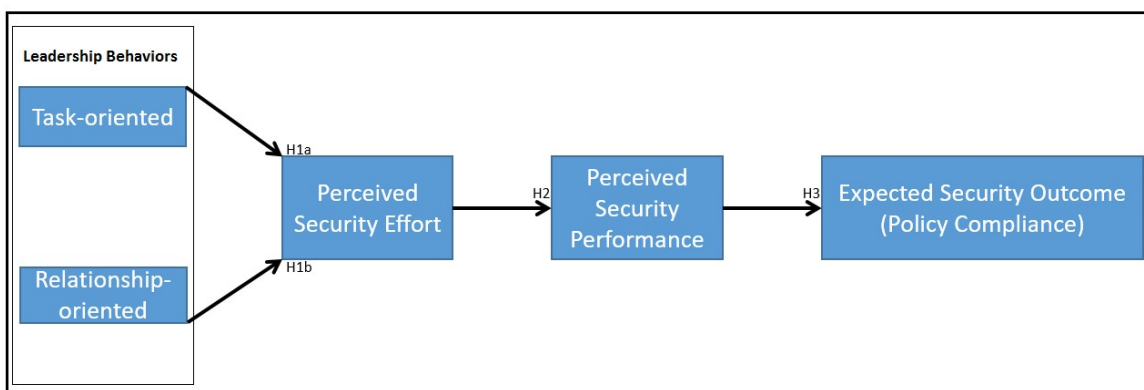
A research model is the diagram in Figure 3 that illustrates the research constructs (or variables) with their hypothesized relationships (Bell et al. 2019). Unlike a conceptual model, when the study uses a theory—it is also known as a theoretical model (Imenda, 2014). The expectancy theory was applied to information security context to develop the following constructs: perceived security effort, perceived security performance, and expected security outcome. By using an existing theory, researchers can provide clear justification about the relationship between variables that motivate IS security compliance with nontechnical controls.

Table 1 presented the constructs of the expectancy theory as developed by Vroom (1964). Basically, the expectancy theory can be used to explain how people choose between alternate types of behavior based on the three distinct perceptions:  $f(\text{expectancy} \times \text{instrumentality} \times \text{valence})$ . The expectancy theory has been used to understand the several forms of motivations in IS research: use of expert systems (Burton et al., 1992),



use of decision support systems (Snead & Harrell, 1994), blogging (Lui et al., 2007), and online information privacy concerns (Hann et al., 2007). This research study discussed expectancy theory in the context of understanding the behavioral influences of leaders, and their influence when employees are considering whether to comply with nontechnical IS security controls.

**Figure 3.** Information System Security Leadership: Research Model



The perceived efforts of leaders are displayed by the following functions: “information search and structure, information use in problem solving, managing personnel resources, and managing material resources” (Burke, Stagl, Klein, Goodwin, Salas, & Halpin, 2006, p. 289). To sum it up, there are two general types of leadership behaviors: those focused on “accomplishing tasks,” as well as others focused on “building relationships” (Northouse, 2016, p. 71). According to Blake and Mouton’s Leadership Grid, “the concern for people includes building organizational commitment and trust, promoting the personal worth of followers, providing good working conditions, maintaining a fair salary structure, and promoting good social relations” (Northouse, 2016, p. 75). While “the concern for tasks refers to policy decisions, new product development, process improvements, workload, and sales volume, to name a few” (Northouse, 2016, p. 75).

There are several references of ToL and RoL behaviors outlined in IS literature that suggest these behaviors are essential to goal attainment in IS security (Table 2). There are two forms of rewards: intrinsic and extrinsic (Herath & Rao, 2009; Siponen, 2000; Vance et al., 2012). These rewards culminate to produce a possibility of desirable outcomes, which can be viewed as a degree of value (Dhillon & Torkzadeh, 2006). Organizational leaders can use behavioral influences to encourage change and improve all employees' IS security compliance that reduces systems security risks to the organization (Flores et al., 2014; Kolkowska & Dhillon, 2013).

**Table 2.** Perceived Effort in IS literature

<b>Perceived Effort in IS Security</b>	<b>Leadership Behavior</b>	<b>Sources</b>
Commitment and Trust	Relationship-oriented	Barton et al., 2016; Colwill, 2009; Spurling, 1995
Management Support	Relationship-oriented	Hu et al., 2012; Knapp et al., 2006; Liang, Saraf, Hu, & Xue, 2007; Sharma & Yetton, 2003
User Participation	Relationship-oriented	Spears & Barki, 2010
Policy Decisions	Task-oriented	Bulgurcu et al., 2010; Höne & Eloff, 2002; Hu et al., 2011
Analysis and Design	Task-oriented	Kokolakis, Demopoulos, & Kiountouzis, 2000
Process Improvements	Task-oriented	Siponen, 2006

The expectancy theory is a process theory, which means it can explain the what and how related to motivation (Chiang & Jang, 2008). As stated earlier, the behavioral approach to leadership focuses on “what leaders do and how they act,” and there are two

general types of behavior: those focused on accomplishing tasks, as well as others focused on building relationships (Northouse 2016, p. 71). Leadership behaviors have been found to influence organizational security outcomes (Flores & Ekstedt, 2016). This is likely due to how followers view the perceived security efforts of leaders. In short, various IS security goals likely require differing leadership behaviors. Due to a lack of research, there is an unclear relationship between leadership behaviors and IS security compliance. The results of this study aimed to help understand the nature of this relationship.

### *3.2.3. Hypotheses*

In quantitative research, variables are often linked to a research question—hypotheses are used to make predictions about what the results will show (Creswell, 2014). When there is a suitable theory, the preferred approach is to use existing theories to support predictions. If no theory is suitable, the researcher should use existing literature and concepts to support predictions with a conceptual framework (Imenda, 2014). The expectancy theory demonstrates there is a predictive relationship between effort, performance, and outcomes (Vroom, 1995). Behavioral researchers in various disciplines have produced research that support this theory (Blau, 1993; Matsui, Okada & Mizuguchi, 1981). However, study aimed to view perceived efforts, perceived performances, and expected outcomes in the IS security context.

First, leadership behaviors are expected to have a relationship with how employee's perceive security efforts. This was not the first study to use perceived effort as a construct in IS literature. Researchers measuring the efforts of discrete emotions on the perceived helpfulness of online reviews where perceived cognitive effort was a mediator (Yin,

Bond, & Zhang, 2014). Security efforts can be described as implementations for protecting information and reducing vulnerability to attack (Whitman, 2003).

Organizations apply security controls in order to achieve security efforts—the perception of these efforts by employees was the area of focus for this research.

**H1a:** Task-oriented leadership behavior are positively associated with perceived security efforts.

**H1b:** Relationship-oriented leadership behavior are positively associated with perceived security efforts.

Second, the perception of how employees perceive security efforts will influence how employees perceive security performance. This was not the first study to use perceived performance as a construct in IS literature. Researchers measuring the effectiveness of computer-based information systems in the financial sector examined perceived performance as a key factor (Miller & Doyle, 1987). IS security performance can be described as measurable results (Singleton, McLean, & Altman, 1988). Once security efforts are implemented, the security performance are measurable results of the implementation—the perception of performance by employees is the area of focus for this research.

**H2:** Perceived security efforts are positively associated with perceived security performance.

Lastly, perceived security performance was expected to influence expected security outcomes. Security outcomes are the result of the application of security efforts (Hu et., 2012). Compliance intentions with security controls can be considered a security outcome. Based on expectancy theory, the higher perceived security efforts should produce higher perceived security performance, and higher perceived security performance should produce higher security outcomes. Organizations that develop

security environments where employees understand the need for security objectives are more likely to comply with security policies. This is largely since people are motivated to perform an action when the benefit is understood (Adams & Sasse, 1999).

For this study, there was one expected security outcome composed of two types of IS security controls: administrative and behavioral. Administrative security controls refer to policies and procedures aimed at securing the IS environment (Talib, El Barachi, Khelif & Ormandjieva, 2012). Administrative security controls are how management outlines the responsibility and control of systems in their organization. For instance, an administrative security control is an acceptable use policy, which aims to reduce the risk associate with the misuse of systems in the organization. Behavioral security controls refer to deterrents or penalties and pressures to ensure policies and procedures influence the intentions of users (Hazari, Hargrave, & Clenney, 2008). Behavioral security controls attempt to reinforce the usefulness of policies and procedures. Administrative and behavioral security controls are effective when there is employee policy compliance.

**H3:** Perceived security performance are positively associated with the expected security outcome of employee policy compliance.

Although leadership behaviors are believed to influence IS security compliance (Furnell & Thomson, 2009), risk management approaches often lack leadership behaviors to encourage employee compliance. Despite clearly defined technical and managerial security controls, there are often few controls that directly outline guidelines for behavioral expectations of leaders. Without strong leadership in IS security programs, organizations will likely find it difficult to motivate employees to comply with nontechnical security controls. This study took a slightly different approach from existing security compliance research by using the expectancy theory to understand the influence

of leadership behaviors from the perspective of employees. Results from this study were expected help identify the usefulness of the expectancy theory for understanding leadership behaviors in IS security. The research study was expected to contribute a theoretical model in the field of IS security, as well as promote organizations to integrate leadership concepts into their IS security programs.

### **3.3. Research Design**

According to Creswell (2014), there are three types of research methods: qualitative, quantitative, and mixed—and within these methods there are several research designs. The focus of research design was to outline the strategy for conducting the study to include data collection, analysis, and interpretation. Since the current research study was a quantitative study, there are two alternate options: experimental and non-experimental. Experimental studies aim to test for a cause-and-effect relationship, which involves the manipulation of independent variables to determine if the treatment influenced the outcome. Non-experimental studies assess the relationship between variables or constructs without manipulation. Non-experimental approaches predominately use surveys for data collection. This can be done using a cross-sectional or longitudinal study. The difference is that longitudinal data are collected from the same subject repeatedly over time, while cross-sectional data are collected in a single point in time. This research study used follow quantitative study research method with a non-experimental research design, utilizing a cross-sectional survey.

#### *3.3.1 Research Strategy*

The study used an electronic survey. The population included IT or closely related fields with business employees who work with IT professionals. This targeted population

is expected to have a general understanding of basic security concepts as well as interact with security leaders. Cross-sectional approach was most appropriate since the aim was to document and test differences with a sample at one point in time (Pinsonneault & Kraemer, 1993). Surveys are used in both qualitative and quantitative research to gather data from subjects for exploration and explanation (Salkind, 2012). Oftentimes, survey research is used in quantitative research which involves written structured questions to gather standardized information about characteristics, actions, or opinions of the subjects being studied to generalize the sample to the population (Pinsonneault & Kraemer, 1993).

Survey research was a key method borrowed from established disciplines outside the IS discipline. The major challenge for IS researchers includes ensuring the appropriateness of survey research for the study (Pinsonneault & Kraemer, 1993). There are numerous reasons to conduct survey research: “(1) easy to administer, score, and code; (2) understand relationship among variables and constructs; (3) generalizable; (4) reusable and objective; (5) predictive tool; (6) test theoretical model; (7) confirm and quantify findings” (Newsted, Huff, & Munro, 1998, p. 553).

### *3.3.2. Instrument Development*

According to Creswell (2014), a researcher must decide if an instrument must be newly designed for this research, modified from existing research, or used intact from published research. Newly designed instruments require extra steps for validation. Modified instruments need the author’s permission and may still require some form of validation. Intact instruments are difficult to find, and in most cases a single instrument may be a collection of validated items from separate studies. For this study, the instrument was designed specifically for this research. Although other instruments were

referenced for ideas, some of the constructs needed to be translated into the IS security context. As a result, the current research has some modified items from existing studies—but overall this is classified as a newly developed instrument.

The instrument opened with a qualifying question and requesting demographic data from participants. The very first question is a qualifying question, which means if answered “no”—participants were not allowed to proceed. The first question asked participants if they work in an IT or closely related field of business employees who work with IT professionals. This was important because a lot of the questions are geared towards employee’s familiarity with general IT concepts, and work with IS security leaders. The second questions asked if participants age range; if participants were under the age of 21, they were disqualified due to a presumed lack of professional experience. The remaining demographic questions aim to obtain descriptive information about respondents to identify where each participant fits in the randomized sample in the general population.

The behavioral approach to leadership focuses on “what leaders do and how they act,” and there are two general types of behavior: those focused on accomplishing tasks as well as others focused on strengthening relationships (Northouse, 2016, p. 71). Leadership can be viewed as essential for any organization to implement successful IS security programs. Similarly, IS researches have used the theoretical lens of coerciveness and empowerment to conceptualize management approaches in IS security policy compliance (Balozian et al., 2019). ToL aligns with coercive approaches where authoritarian mechanism are in place to produce an outcome, while RoL aligns with empowerment where power is shared with employees. Northouse (2016) provided an



instrument for measuring ToL and RoL behavior, these items were not modified (Table 3). The overall goal was to gather data from employees about leadership behaviors displayed from security leaders in their organization. This data will be used to evaluate leadership behaviors (Table 3).

**Table 3.** The Measurement of Leadership Behaviors

Construct		Items	Adapted	Modified	Reference
<b>Task-oriented Leadership</b>	<b>ToL1</b>	Sets standards of performance for group members.	Yes	No	(Northouse, 2016, p. 88
	<b>ToL2</b>	Defines roles and responsibilities for each group member.	Yes	No	Northouse, 2016, p. 88
	<b>ToL3</b>	Clarifies his or her own role within the group.	Yes	No	Northouse, 2016, p. 88
	<b>ToL4</b>	Provides a plan for how the work is to be done.	Yes	No	Northouse, 2016, p. 88
	<b>ToL5</b>	Makes his or her perspective clear to others.	Yes	No	Northouse, 2016, p. 88
	<b>ToL6</b>	Tells group members what they are expected to do.	Yes	No	Northouse, 2016, p. 88
<b>Relationship-oriented Leadership</b>	<b>RoL1</b>	Helps group members get along with each other.	Yes	No	Northouse, 2016, p. 88
	<b>RoL2</b>	Responds favorably to suggestions made by others.	Yes	No	Northouse, 2016, p. 88
	<b>RoL3</b>	Helps others in group feel comfortable.	Yes	No	Northouse, 2016, p. 88
	<b>RoL4</b>	Discloses thoughts and feelings to group members.	Yes	No	Northouse, 2016, p. 88
	<b>RoL5</b>	Shows concern for the well-being of others.	Yes	No	Northouse, 2016, p. 88
	<b>RoL6</b>	Communicates actively with group members.	Yes	No	Northouse, 2016, p. 88

The concept of perceived effort is belief that one's effort will result in the attainment of desired performance goals (Vroom, 1964). In extant literature, perceived effort has been measured by asking participants to indicate how effortful they perceived a task (Lyxell, Borg, & Olsson, 2009). This approach to understanding and measuring perceived effort will be applied in the IS security context. Perceived security effort involves the view of how employees view initiatives in their organization. Security efforts can be described as implementations for protecting information and reducing vulnerability to attack (Whitman, 2003). IS literature has outlined several categories related to improving security program, the following are: strong commitment and trust, top management support, user participation, policy decisions, analysis and design, and process improvements (Table 2). These categories will be used to measure perceived security effort (Table 4).

**Table 4.** The Measurement of Perceived Security Effort

Construct		Items	Adapted	Modified	Reference
Perceived Security Efforts	PSE1	I believe my organization's security leaders encourages strong commitment and trust.	No	No	New
	PSE2	I think my organization's security leaders encourages top management support.	No	No	New
	PSE3	I believe my organization's security leaders encourages user participation.	No	No	New
	PSE4	I think my organization's security leaders focuses on policy decisions.	No	No	New

	<b>PSE5</b>	I believe my organization's security leaders focuses on analysis and design	No	No	New
	<b>PSE6</b>	I think my organization's security leaders focuses on process improvements.	No	No	New

The concept of perceived performance is the belief that a person will receive a reward if the performance expectation is achieved (Vroom, 1964). Perceived performance (or performance beliefs) are how individuals approximate expected performance (Cronin & Taylor, 1992). IS security performance can be described as measurable results (Singleton et al.,1988). For this study, perceived security performance involves how well individuals perceive security programs as functioning. As a result, this study used various categories to security programs to measure the perceived performance (Table 5).

**Table 5.** The Measurement of Perceived Security Performance

<b>Construct</b>	<b>Items</b>	<b>Adapted</b>	<b>Modified</b>	<b>Reference</b>	
<b>Perceived Security Performance</b>	<b>PSP1</b>	I think my organization's security program produce noticeable results.	No	No	New
	<b>PSP2</b>	I believe my organization's security program prevent security incidents.	No	No	New
	<b>PSP3</b>	I think my organization's security program have strong security performance.	No	No	New
	<b>PSP4</b>	I believe my organization's security program prevent security threats.	No	No	New
	<b>PSP5</b>	I think my organization's security program has strong implementation.	No	No	New

	<b>PSP6</b>	I believe my organization's security program is operating effectively.	No	No	New
--	-------------	--	----	----	-----

Information security is closely related to the concept of risk management (Blakley et al., 2001). Information security involves the application of security controls to mitigate security threats, while risk management involves applying security controls in such a way that is feasible for the organization. Therefore, IS security risk management is a subdomain, which involves the application of controls to manage risk. Since this study aimed to understand security control compliance with non-technical controls, RMF (Figure 1) and ISO 270001 (Figure 2) non-technical security controls and concepts from other research were used to develop a survey instrument. These are the two information security frameworks that organizations use to practice risk management. NIST Special Publication (SP) 800-37 also known as RMF was selected because it is widely used by diverse organizations. Although RMF is primarily used for IS security risk management in the United States federal government, NIST publications are also used to develop private sector security programs. ISO 27001 is an international information security framework used to develop security programs worldwide. RMF and ISO 270001 were chosen for this study because they provide a list of security controls that can be translated into items to measure the construct of expected security outcomes. Table 6 presented security controls used to create measurable outcomes that are a good fit for surveying employees.

**Table 6.** The Measurement of Expected Security Outcomes

Construct		Items	Adapted	Modified	Reference
Expected Security Outcomes	<b>ESO1</b>	Employees within your organization follow access control policies.	No	No	New
	<b>ESO2</b>	Employees within your organization follow physical and environmental security policies.	No	No	New
	<b>ESO3</b>	Employees within your organization follow incident response security policies.	No	No	New
	<b>ESO4</b>	Employees within your organization follow security policies that limit individual access.	No	No	New
	<b>ESO5</b>	Employees within your organization obtain physical access to resources when required.	No	No	New
	<b>ESO6</b>	Employees within your organization report incidents where polices are violated.	No	No	New

### 3.3.3. Instrument Validation

Leadership behaviors were measured using twelve items (six for each sub-construct) from an existing instrument (Northouse, 2016). Perceived security effort and perceived security performance was measured using six newly created items. Perceived security outcomes are measured using six security controls from RMF and ISO 270001: access control, physical and environmental, and incident response. The selected security controls are consistent with overlap in both RMF and ISO 270001. Although some items were derived from existing literature, the majority were newly developed. Since the overall instrument was classified as a newly developed, there is a need for instrument validation.

The survey instrument must be validated to ensure questions asked to participants address the research questions (Straub, 1989).

It is important to ensure the instrument has reliability and validity before the results of the study can be trusted (Salkind, 2012). An interval scale was selected for this study, which allows researchers to perform arithmetic operations to understand survey results. A common interval scale in social science research is the five-point Likert scale. Although Likert scales typically range anywhere from four to eleven, this study used a seven-point Likert interval scale. An interval scale with a higher value can produce better approximation of results (Wu & Leung, 2017). IS research have used the 7-point Likert scale (Ifinedo, 2014; Romanow, Rai, & Keil, 2018). As a result, mostly quantitative approaches were used to evaluate instrument and analyze results. Further details describing instrument validation are in the upcoming data collection and data analysis sections.

### **3.4. Data Collection**

The term data refers to “the purposive collection of perceived facts” (Ellis & Levy, 2012, p. 407). The sampling approach to collect data for this study requires several steps: (1) define the population; (2) determine the sample frame; (3) determine the sampling design; (4) determine the appropriate sample size; (5) execute the sampling process (Sekaran & Bougie, 2013).

The target population identified the general category for individuals needed for the study in terms of elements, geographic boundaries, and time (Sekaran & Bougie, 2013, p. 245). This study contracted, a data collection service called Qualtrics, to gather data from a sample of employees. The sampling frame is a depiction of all elements in the

population that can be used for sampling (Sekaran & Bougie, 2013). More specifically, the sampling frame for this study is employees who work in an IT or related field—which means they work closely with IT professionals and are familiar IT policies and procedures. In addition, questions were built into the instrument to ensure participants fit the sampling frame. The sampling design can either be probability or nonprobability sampling (Sekaran & Bougie, 2013). This study used probability based simple random sampling. A random sample of participants are selected from a pool of qualified employees. Random sampling helps improve generalizability; however, there has long been concern expressed that generalizability is often not a concern in IS research (Lee & Baskerville, 2003).

The aim was to isolate respondents that have some level of understanding of IT concepts to adequately answer questions. Although researchers often use non-probability sampling for convenience, survey research with probability sampling is better suited and not uncommon in IS research. The sampling size defined the number of participants necessary for the study (Sekaran & Bougie, 2013). The sampling size varied based on the phase of the study, which means each phase will require a different number of participants. The sampling process identified the final plans for data collection (Sekaran & Bougie, 2013). This data was collected at the individual unit of analysis using electronic surveys. In a cross-sectional approach, surveys were administered to each participant once. After obtaining Institutional Review Board (IRB) approval from Nova Southeastern University (Appendix A), there was a three-phased approach to data collection: expert panel, pilot study, and main study to validate the observed variables or items.

### 3.4.1. Phase I

The first phase of the data collection used an expert panel to validate the instrument before the pilot study. This approach is recommended in IS research because positivist science often lack “clear consensus on the methods and means for determining content validity” (Straub, Boudreau, & Gefen, 2004, p. 387). In an expert panel, a team of professionals are selected to validate observed variables or items used before data collection to assess whether the items were a true representation of the construct being measured (Skinner, 2015). Verhagen, Van Den Hooff, & Meents (2015) referenced the use of eleven participants in a panel experienced in scale development to evaluate an instrument in IS research. The current research instrument was sent using Survey Monkey to six to ten people with a Ph.D. to obtain meaningful feedback on how to improve the research instrument.

The study used a quantitative approach to content validity. Lawshe (1975)’s Calculated Average (CVR) calculation was used for consensus analysis and the minimum ratios are in Appendix C. Participants were asked to evaluate on a scale from one to three (1 = not essential; 2 = useful but not essential; 3 = essential) if survey questions (or items) measure the construct. The first equation is to calculate the CVR, which is  $(CVR = (Ne - N/2)/(N/2))$ . The first equation assesses the ratio of the total of the experts who perceive an item as essential to the overall number of experts. The  $Ne$  is the number of experts with essential responses, and the  $N$  is the total number of experts. The qualifying consensus and suggestions were followed:

Any item, performance on which is perceived to be “essential” by more than half of the panelists, has some degree of content validity. The more panelists (beyond 50%) who perceive the item as “essential,” the greater the extent or degree of its content validity...when fewer than half say “essential,” the CVR is negative. When half say “essential” and half do not, the CVR is zero (Lawshe 1975, p. 567).



Furthermore, the study applied a substantive validity analysis to validate observed constructs as well as the acceptability of construct definitions (Anderson & Gerbing, 1991, p. 734; Hinkin, 1998, p. 108). Along with rating the quality of the survey items for content validity, the expert panel participants were asked to evaluate how well each item aligns with construct definitions. In addition, comment boxes were added to allow respondents to add additional feedback.

#### *3.4.2. Phase II*

The second phase of the data collection was from the pilot study to evaluate the instrument before the main data collection. The pilot study was used to evaluate and fine tune the instrument at a smaller scale, and address areas of concern before proceeding to a larger scale study (Straub, 1989). IS literature recommend a pilot study or pretest following the expert panel (Anderson & Gerbing, 1991; Hinkin, 1998; Milne & Bahl, 2010). A pilot study can further establish the “content validity of scores on an instrument and to improve questions, format, and scales” (Creswell, 2014, p. 161).

IS security compliance research use pilot tests to evaluate and improve the survey instrument. Safa et al. (2016) used 52 participants to pilot test an instrument for an information security compliance model in organizations. The results revealed that participants understand and interpreted questions. Flores and Ekstedt (2016) used 47 participants to test resistance to social engineering. The results revealed a need for minor changes, but overall most participants understood the questions. Straub et al. (2004) recommends more IS journals should use pilot tests as a form of validation.

Based on existing IS literature, this study used 55 participants for the pilot study. The survey in Appendix D was administered electronically to voluntary participants using

Qualtrics. This service was used as a data collection service to collect a randomized sample in a reasonable timeframe. Participants in the pretest were given a week to respond to the survey. Based on feedback, changes and updates were made after pilot study to improve the instrument.

### *3.4.3. Phase III*

The main study collected actual data to test the research model and validate research hypotheses. The study utilized the survey instrument that was refined in the expert panel and pilot study for data collection. Qualtrics was used for their data collection service to collection a randomized sample in a reasonable timeframe. Participants were comprised of working professionals with an IT or closely related background.

There was a need to ensure the sample size is sufficiently large (Terrell, 2012). According to Weston and Gore (2006), “there is no consensus [in sample size], except to suggest that missing or nonnormally distributed data require larger samples than do complete, normally distributed data” (p. 734). The sample size in explanatory research must be “sufficient to test categories in the theoretical framework with statistical power” (Pinsonneault & Kraemer, 1993, p. 12). The statistical power is the ability of a statistical test to detect the statistical significance relationships between variables or constructs (Sekaran & Bougie, 2013). According to Sekaran and Bougie (2013), “there are six factors influencing sample size: (1) research objective; (2) confidence interval; (3) confidence level; (4) variability in the population; (5) cost and time constraints; (6) size of population” (p. 246). The main study collected actual data to test the research model and validate research hypotheses. In addition, Pinsonneault and Kraemer (1993) found the average sample size for an individual unit of analysis was 388 participants (p. 21).

This study aimed to collect over 400 participants is above average in comparison to similar IS research studies.

### **3.5. Data Analysis**

Data analysis in quantitative research is performed using: “a mathematical procedure for organizing, summarizing, and interpreting data” (Gravetter & Wallnau, 2009, p. 3). There are two general categories for data analysis: descriptive statistics and inferential statistics. While descriptive statistics are used to organize and summarize data, inferential statistics are used to help make decisions (or inferences) about the data (Terrell, 2012). Descriptive statistics have four primary measuring techniques: “central tendency, variability, relative position, and relationship” (Mertler & Vannatta, 2013, p. 7). Descriptive statistics will likely have sampling error, which means even when data are gathered from similar samples under the same population there will likely be different results (Terrell, 2012). Inferential statistics aim to address sampling error by normally distributing results around the population mean (Mertler & Vannatta, 2013). This study has a research model with hypotheses testing, which requires the use of inferential statistics to reasonably test predictions and address sampling error caused by nonprobability sampling. However, descriptive statistics were also used to obtain a clear understanding of sample that represents the overall population, which is a common approach in the social sciences to include IS literature.

#### *3.5.1. Statistical Technique*

This research study used Structural Equation Modeling (SEM) for data analysis. SEM is a “collection of statistical techniques that allow a set of relationships between one or more independent variables (IVs), either continuous or discrete, and one or more

dependent variables (DVs), either continuous or discrete to be examined” (Ullman & Bentler, 2003, p. 661). SEM, or latent variable modeling, technique was chosen rather than regression to test the theory. The conceptualization of leadership behaviors is a multidimensional second order construct, for which SEM methods are better suited. Unlike first-generation techniques, SEM is a second-generation technique reduces measurement errors and allows researchers to incorporate unobservable variables measured indirectly by indicator variables in path models (Mertler & Vannatta, 2013). This study used Confirmatory Factor Analysis (CFA), which is an advanced form of statistical analysis that is often used to test a theory about latent processes that occur among variables: this means it measures of constructs (or factors) are consistent with the underlying theory or concepts (Mertler & Vannatta, 2013).

According to Hair, Hult, Ringle, and Sarstedt (2017), path models should be created based on theory—which are a collection of systematically related hypotheses created from the scientific method that can be used for predications and explanations. SEM has two models created from theory: measurement and structural (Hair et al., 2017). While “the measurement specifies how latent variables (or constructs) are measured, the structural model shows how the latent variables are related to each other” (Hair et al., 2017, p. 13).

Partial Least Squares (PLS) was the selected type of SEM, which allows researchers to simultaneously measure the data and the theory (Hair et al., 2017). PLS was a good fit for this study because the originating theory is well-established and strong from a non-IS discipline; as a result, the model aimed to evaluate the predictiveness of the model in the IS security context. SEM has been used in existing IS security studies published in top IS

Journals to understand problems with employee compliance using existing theories and concept (Siponen & Vance, 2010; Vance et al., 2012).

### *3.5.2. Statistical Software*

There are three common software packages used in social science research. SmartPLS is a software package that uses Ordinal Least Square estimation techniques that are primarily used for theoretical exploration (Ong & Puteh, 2017). Statistical Package for Social Sciences (SPSS) is a widely used software package used for interactive, or batched, statistical analysis. Analysis of Moment Structures (AMOS) is an add-on that provide an enhanced version of SPSS, which a complete drawing environment for SEM data analysis (Blunch, 2012). While SmartPLS can examine smaller sample sizes in variance-based to explore theories, SPSS AMOS better suited for covariance-based research to confirm or reject theories (Ong & Puteh, 2017, p. 21). Since this research study is testing an existing theory in an IS security leadership model, SPSS AMOS was the statistical software package selected for data analysis.

### *3.5.3. Goodness of Fit*

SEM has two components: the measurement model and the structural model (Hair et al., 2017). The structural model is used to assess unobserved (or latent) constructs. The structural model represents the constructs, and the relationships between the constructs (Hair et al., 2017, p. 11). The measurement model consists of constructs that display the relationship between constructs and the indicator variables (Hair et al., 2017, p 12).

Therefore, this study used SEM because it allowed it to test the observed item linkage the construct and assess the covariance of the constructs depicted in Figure 3.

SEM contains CFA as one form of statistical analysis, which is a good fit for theory or hypothesis driven research (Hair et al., 2017). This study also used CFA, which is an advanced form of statistical analysis that is often used to test a theory about latent processes that occur among variables: this means it measures of constructs (factors) are consistent with the underlying theory or concepts (Mertler & Vannatta, 2013). This study used CFA to test the hypothesis and assess the model's fit to see if the hypothesized relationships developed from the Expectancy Theory hold true upon rigorous examination (Sekaran & Bougie, 2013).

There are several Goodness-of-Fit (GoF) measures that can be used to assess each single-factor model for their validity. This study follows the following: Chi-square with degrees of freedom, the Goodness of Fit Index (GFI), Comparative Fit Index (CFI), Adjusted Goodness of Fit index (AGFI), and Root Mean Square Error of Approximation (RMSEA) model fit indices (Hair et al., 2017). This approach to evaluate model fitness was used in Safa et al. (2016)'s IS research study to understand information security conscious care behavior formation in organizations.

**Goodness-of-fit index (GFI).** The GFI is used for validating the PLS model globally to describe how well it fits a set of observations. (Hair et al., 2017, p. 193). This approach was used to validate the current PLS model (Figure 3). The minimum accepted value for GFI is  $\geq .90$  (Hooper et al., 2008, p. 54).

**Pearson's Chi-square.** This test is often used as a measure for goodness of fit: this measure is the sum of differences between observed and expected outcome frequencies (that is, counts of observations), each squared and divided by the expectation (Figure 4).

**Figure 4.** Pearson's Chi-square Test

$$\chi^2 = \sum_{i=1}^n \frac{(O_i - E_i)^2}{E_i}$$

**Adjusted Goodness of Fit Index (AGFI).** The AGFI corrects the GFI based upon degrees, which is affected by the number of indicators of each latent variable (Hooper et al., p. 54). AGFI tends to increase based on sample size. The minimum accepted value for AFI is  $\geq .90$  (Hooper et al., 2008, p. 54).

**Comparative Fit Index (CFI).** A revised form of Non-normed Fit Index (NFI). This approach is not as sensitive to sample size and allows researchers to compare the fit of an independent, or null, model (Hooper et al., 2008, p. 54). The minimum accepted value for CFI is  $\geq .95$  (Hooper et al., 2008, p. 55).

**Root Mean Square Error of Approximation (RMSEA).** The RMSEA is an index that calculates the difference between the observed covariance matrix per degree of freedom and the hypothesized covariance matrix which denotes the model (Chen, 2007). RMSEA is one of the most widely reported measures of model fitness when using structural equation modeling. The formula:  $RMSEA = \sqrt{\max( [(\chi^2/df) - 1]/(N - 1) , 0)}$ . The minimum accepted value for RMSEA is  $<.08$  (Arpaci & Baloğlu, 2016, p. 69; Hooper et al., 2008, p. 54).

### 3.6 Empirical Validation

Reliability and validity tests were conducted for empirical validation. This study used Cronbach's coefficient alpha and CFA for empirical validation. Reliability tests how consistently a measuring instrument measures whatever concept it is intended to measure

(Sekaran & Bougie, 2013, p. 225). Validity tests how well an instrument that is developed measures the concept it is intended to measure (Sekaran & Bougie, 2013, p. 225). Empirical validation involves the use of statistical techniques to test for reliability and validity. Cronbach's coefficient alpha was used to test for reliability, and CFA was used to test for content validity, convergent validity, and discriminant validity (Sekaran & Bougie, 2013).

### 3.6.1 Reliability

Reliability assesses the confidence that the measuring instrument will yield the same results when subjected to the same measurement (Straub et al., 2004, p. 426). Cronbach coefficient alpha ( $\alpha$ ) is a reliability test that examines the “consistency of respondent's answers to all the items in a measure” (Sekaran & Bougie, 2013, p. 229). Cronbach's alpha is used when researchers want to test the internal consistency of a survey instrument made up of Likert-type scales and items. Cronbach's alpha is computed by correlating the score for each scale item with the overall score for each observation, and then comparing that to the variance for all individual item scores (Figure 5). Cronbach's alpha is thus an output of the number of items in a test, the average covariance between pairs of items, and the variance of the overall score. The resulting reliability statistics for PLS should produce a score where research look for a “minimum score of over .7” for high internal consistency (Straub et al., 2004, p. 411).

#### **Figure 5.** Cronbach Coefficient Alpha Formula

$$\alpha = \frac{K}{K-1} \left( 1 - \frac{\sum_{i=1}^K \sigma_{Y_i}^2}{\sigma_X^2} \right)$$

Furthermore, using CFA, the reliability of a construct (or latent variable) is deemed valid if the Composite Reliability (CR) is more than the Average Variance Extracted



(AVE). The CR and AVE are calculated using the formula in Figure 6 and Figure 7. The AVE aims to measure the "percent of variance obtained by a construct by revealing the ratio of the sum of the variance obtained by the construct and measurement variance" (Straub et al., 2004, p. 424). The CR is calculated by dividing the squared sum of the factor loading for each construct, by the squared sum of the factor loading for each construct and the sum of the error variance for each construct (Paswan, 2009; Hair et al., 2017).

**Figure 6.** Composite Reliability Formula

$$\rho_C = \frac{\left(\sum_{i=1}^k \lambda_i\right)^2}{\left(\sum_{i=1}^k \lambda_i\right)^2 + \sum_{i=1}^k \sigma_{e_i}^2}$$

**Figure 7.** Average Variance Expected Formula

$$\text{AVE} = \frac{\sum_{i=1}^k \lambda_i^2}{\sum_{i=1}^k \lambda_i^2 + \sum_{i=1}^k \text{Var}(e_i)}$$

### 3.6.2 Validity

Validity assesses the mathematical relationships between variables and make inferences about whether this statistical formulation correctly expresses the true covariation (Straub et al., 2004). Although there are several tests for validity, this study aims to address content validity and construct validity. Content validity is considered highly recommended, and construct validity is considered mandatory (Straub et al., 2004).

Content validity aims to measure the adequacy and representation of items to their related concept (Sekaran & Bougie, 2013). For instance, does the measure adequately measure the concept? Content validity is highly recommended in IS research, especially in the absence of strong theory and prior empirical practice specifying the range and

nature of the measures (Straub et al., 2004, p. 413). An expert panel or judges was the selected technique to obtain content validity of formative constructs before collecting data or estimating path models (Straub et al., 2004).

On the other hand, construct validity is a combination of convergent validity and discriminate validity aimed at evaluating the operationalization (or measurement between constructs) to see how well the results obtained fit the theoretical model (Straub et al., 2004, p. 388; Sekaran & Bougie, 2013, p. 227). Convergent validity is established when the scores obtained with two different instruments measuring the same concept are highly correlated (Sekaran & Bougie, 2013, p. 227). For instance, do two instruments measuring the concept correlate highly? The outer loading of indicators and the AVE must be considered. Outer loading should be greater than 0.70, and the AVE should be greater than 0.50 (Hair et al., 2017). Discriminant validity is established when, based on theory, two variables are predicted to be uncorrelated, and the scores obtained by measuring them are indeed empirically found to be so (Sekaran & Bougie, 2013, p. 227). For instance, does the measure have a low correlation with a variable that is supposed to be unrelated to this variable? Discriminate validity states the construct is valid if there is no inter-construct correlation. A construct's AVE would need to be more than its associated squared inter-construct (SIC) correlations (Pawson, 2009; Hair et al., 2017).

### **3.7. Summary**

This chapter addressed the methodology used to understand the behavioral influences of leaders on the expected outcome of policy compliance. The introduction section explained the selected methodology along with the epistemology. The theoretical

framework section explained the chosen theory, research model, and hypotheses. The research design section described the research strategy, instrument development and validation, and data collection. The data analysis section explained the statistical techniques and empirical validation. The major takeaway was that this study proposed the use of the expectancy theory to formulate a research model and hypothesis testing in a quantitative approach. The next chapter explains the results of the study.

## Chapter 4

### Results

#### 4.1. Introduction

The primary purpose of this chapter was to provide a detailed data analysis and representation of findings. Statistical techniques borrowed from the social sciences are applied to address a problem in IS security management. The use of social science techniques is a common approach to address business-related issues (Sekaran & Bougie, 2013). Data was obtained from participants to statistically analyze if the hypothesized relationships outlined in the previous chapter are supported. Section 4.2 describes the statistical results of the data analysis. Section 4.3 uses the results of the data analysis to provide a representation of findings. Lastly, Section 4.4 provides an overall summary of the results.

#### 4.2. Data Analysis

##### *4.2.1. Expert Panel Results*

An expert panel of eight experienced researchers were sought to judge the initial research instrument. The current research instrument was sent to a total of eight participants who hold a Ph.D. level degree, but only seven fully completed all the responses. Data collected was analyzed with a substantive validity analysis and content validity ratio. Existing IS literature has used an expert panel to evaluate survey items

aimed at measuring the influence of top management support on an organization's security culture and level of security policy enforcement (Knapp, 2006).

Lawshe (1975) outlined the use of an expert panel in a quantitative approach to content validity and substantive validity the research instrument. For each instrument item, the CVR was calculated and results are in Appendix B. All CVR values were measured against the minimum ratio score in Appendix C. For missing values, calculations were adjusted based in the total responses for that item—which means the weighted average for each response was adjusted based on the number of completions for that item. Most construct items held an average rating of 50 or higher, which means those construct items would carry over to the pilot study. However, there were low ratings for various demographic items—but these items were left in the survey to obtain a better understanding of who was sampled. There was one missing item, and an item with a low average and CVR. The missing item was added without retesting, and no change was made to the poorly rated item because these items were obtained from existing literature. In addition, written feedback helped identify various grammatical errors, minor updates, and improve the overall quality of the instrument. The expert panel helped improve the confidence that instrument items measure the constructs in the research model.

#### *4.2.2. Pilot Study Results*

According to Straub (1989) a pilot study (or pretest) can use a draft of the research instrument to perform a qualitative analysis to identify the need for revisions. For instance, a pilot study was used to improve a survey instrument in the assessment of gender differences in information quality in virtual communities (Liu, Li, Zhang, & Huang, 2017). The current pilot study aimed to evaluate the survey instrument to identify

errors early on before the full-range data collection. Data was exported from Qualtrics' user interface into a CSV file and reviewed in a spreadsheet. The pilot study was completed by all 55 participants. All respondents qualified to participate and were able to complete the survey under the estimated time of 10-15 minutes. There were no technical issues identified, and all inputs are considered within a valid range. There were no written comments added at the end of the study. The qualitative review of the pilot study's results suggested the instrument was ready for the remaining data collection.

#### *4.2.3. Pre-Analysis Data Screening*

After all data was collected, a number of best practices were applied to screen for clean data and ensure the accuracy of the data collected from surveys (DeSimone, Harms, & DeSimone, 2015). The main study collected the remaining data to test the research model and validate research hypotheses. There were 439 results collected during this phase of the data collection. Since the main study did not require any instrument modifications from the pilot study, and results were combined to produce a grand total of 494 responses. A few best practices from DeSimone et al. (2015) were used for data screening. Data was reviewed for visible errors, extreme outliers, and respondents who missed a significant number of answers. There were 19 responses from participants removed because there were more than two missing answers. For responses missing two or less, the average value (or mean substitution) was applied as dummy data to satisfy SEM computational requirement (Allison, 2003). There were eight responses from participants removed because they were under the age of 21. Participants under the age of 21 are assumed to lack the overall experience to reliably answer questions. An additional four were removed because they did not work in an IT or closely related field. All data

adjusted based on data screening has been reported. The final number of participants for analysis after data screening was N=455.

#### *4.2.4. Main Study Results*

##### *Descriptive Statistics*

Descriptive statistics are used to provide a summary of a collected data set (Mertler & Vannatta, 2013, p. 7). Demographic information was collected to provide descriptive statistics about the sample of participants and their organization. Sekaran and Bougie (2013) advise researchers to gather demographic information from participants even if the research study does not require it in order to describe the sample's characteristics in the written report. The sample descriptive statistics in Table 7 revealed demographic information about respondents who participated.

The most common time working in an IT or closely related field was 8-9 years (169, 37.1%) followed by 4-5 years (101, 22.2%). The least common was less than 1 year (32, 7.0%). There were 208 (45.7%) males and 246 (54.1%) females. Most participants held a bachelor's degree (206, 45.3%), a graduate degree (76, 14.7%), or a professional degree (66, 14.5%). The majority of the sample was between the age of 21-50—while 31-40 was the most common (158, 34.7%). Lastly, a majority of the sample worked for a private company (269, 59.1%).

The descriptive statistics revealed heterogeneity in the data collected. The biggest concern was regarding the higher number females versus males, which is not representative of the actual IT work environment. However, a decision was made to proceed forwards due to the large sample size. The results were a good enough indicator the data has diversity and representative of the larger population. These results help

understand the generalizability of the data collected due to the varying years of experience, sex, education, age, and employment status.

**Table 7.** Sample Descriptive Statistics

		Frequency	Percent
Years in IT	1 or less	32	7.0
	2-3 years	91	20.0
	4-5 years	101	22.2
	6-7 years	62	13.6
	8-9 years	169	37.1
Sex	Male	208	45.7
	Female	246	54.1
	No response	1	0.2
Education	HSD	39	8.6
	AA/AS	63	13.8
	BA/BS	206	45.3
	Graduate	76	16.7
	Professional	66	14.5
	Other	5	1.1
Age	21-30	103	22.6
	31-40	158	34.7
	41-50	122	26.8
	51-60	58	12.7
	60+	14	3.1
Employment Status	Student	5	1.1
	Self	56	12.3
	Private	269	59.1
	Government	61	13.4
	Government contractor	14	3.1
	Non-profit	28	6.2
	Other	22	4.8

Note: N= 455

In addition, participants were also queried with demographic questions about their organization. The organizational descriptive statistics in Table 8 revealed demographic information about the environment for respondent who participated. The vast majority of



participants said their organization had defined IT policies (409, 89.9%). In addition, the vast majority of participants were aware of the security requirements (430, 94.5%).

Lastly, most of participants said their organization had a CISO (366, 80.4%). The results suggest participants have a basic understanding of IS security in their organization and are capable of providing reliable answers to IS security related questions.

**Table 8.** Organizations Descriptive Statistics

		Frequency	Percent
Defined IT Policies	Yes	409	89.9
	No	26	5.7
	Not sure	18	4.0
Aware of Security Requirements	Yes	430	94.5
	No	13	2.9
	Not sure	11	2.4
Organization has CISO	Yes	366	80.4
	No	62	13.6
	Not sure	27	5.9

Note: N=455, IT policies had two missing and Security requirements had one missing

### *Inferential Statistics for Model-level Results*

Inferential statistics involve the use of a sample of information to draw conclusions about a population (Mertler & Vannatta, 2013, p. 9). Various inferential statistical techniques were used to obtain model level results.

**Confirmatory Factor Analysis (CFA)** is an advanced statistical approach used to test a theory by measuring how well measurable variables represent unobservable constructs (Mertler & Vannatta, 2013, p. 245). A CFA is run to test the reliability of a construct (or latent variable) if the CR is more than the AVE the construct is deemed

valid. CFAs were run on the five construct scales to help validate them in this context. Beforehand, mean replacement was done for missing values in scale questions. The mean was substituted for missing data of two or less in order to optimize sample size. It should be noted that mean substitution is appropriate for continuous data (Allison, 2003).

The first CFA was run with all of the questions for the five scales in order to check for factor loading. A varimax rotation was used and an eigen cut of 1.25 was given to ensure a more conservative estimate on factor loading. In order for a factor to be considered cleanly loaded, the communality must be over 0.5, and it must have loaded on a factor over 0.4 with a 0.13 distance between the highest and next highest factor.

This CFA showed two cleanly loaded factors in Appendix E. The first was with the five PSP and the five ESO questions. This was not unexpected as they are derived from the same theoretical measures. The second was with ToL and RoL, again this was not unexpected as they are derived from the same theoretical measures. The five PSE questions did not load cleanly on either factor. Five subsequent factor analysis were run, one for each scale, to see if by themselves they would load together, and the results indicated a single factor for each scale, including PSE, which all loaded cleanly. Given the theoretical alignment—all five scales remained.

**Cronbach Coefficient Alpha.** Reliability assesses the confidence that the measuring instrument will yield the same results when subjected to the same measurement (Straub et al., 2004, p. 426). Cronbach Coefficient Alpha ( $\alpha$ ) is a reliability test that examines the consistency of respondent's answers to all the items in a measure (Sekaran & Bougie, 2013, p. 229). Cronbach's Alphas were run to ensure scale reliability with results. All measures produced a strong reliability score with a significant Cronbach Alpha

approximating .9 in Table 9, which is .2 above Straub et al. (2004) recommended .7 minimum. The results clearly demonstrated reliability in the research instrument.

**Table 9.** Scale Descriptive Statistics and Cronbach's Alpha

	Mean	SD	# Items	Alpha
ToL	32.53	7.69	6	0.917
RoL	32.21	7.36	6	0.909
PSE	33.34	7.02	6	0.913
PSP	34.05	6.52	6	0.917
ESO	34.19	6.7	6	0.899

Note: N=455

**Structural Equation Model with Full Mediation.** This study used several Goodness-of-Fit (GoF) measures to assess the proposed model in Figure 3 with SPSS AMOS. The following are the GoF measures selected Chi-square with degrees of freedom, the Goodness of Fit Index (GFI), Comparative Fit Index (CFI), Adjusted Goodness of Fit index (AGFI), and Root Mean Square Error of Approximation (RMSEA) model fit indices (Hair et al., 2017).

**Pearson's Chi-square.** The results revealed the Chi-square is  $\chi^2(5) = 75.88, p < .001$ , which means the model is a poor fit against the ideal model.

**Goodness-of-fit index (GFI).** The minimum accepted value for GFI is  $\geq .90$  (Hooper et al., 2008, p. 54). The results revealed the GFI was .946, which suggests the model was a good fit.

**Adjusted Goodness of Fit Index (AGFI).** The minimum accepted value for AFI is  $\geq .90$  (Hooper et al., 2008, p. 54). The results revealed the AGFI was .837, which means the model was not a good fit.

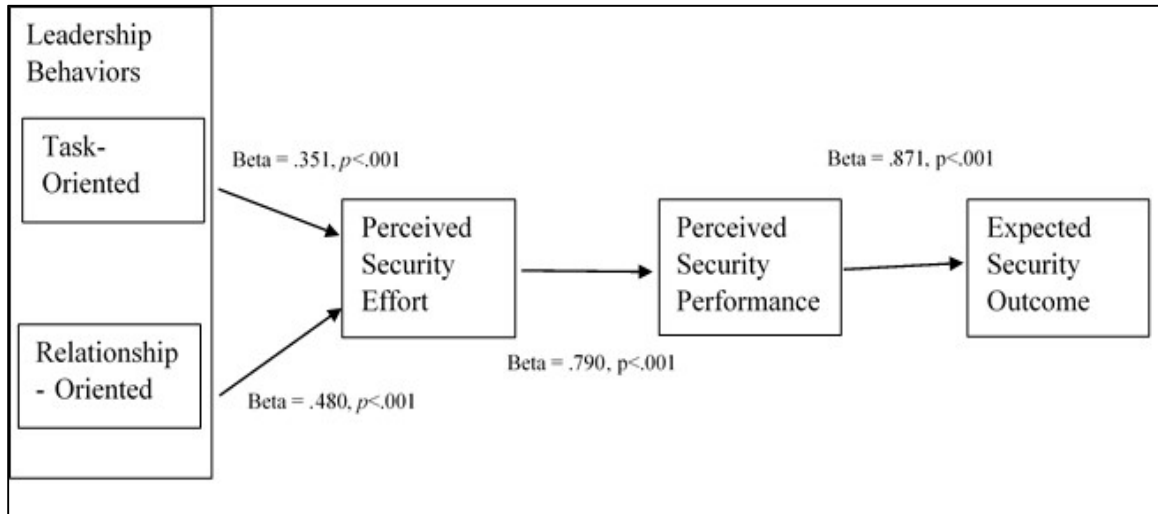
**Comparative Fit Index (CFI).** The minimum accepted value for CFI is  $\geq .95$  (Hooper et al., 2008, p. 55). The results revealed the CFI was .961, which indicates the model was a good fit.

**Root Mean Square Error of Approximation (RMSEA).** The minimum accepted value for RMSEA is  $<.08$  (Arapaci & Baloglu, 2016, p. 69; Hooper et al., 2008, p. 54). The results revealed the RMSEA was .177, which means the model was not a good fit.

According to Mulaik et al. (1989), it is possible to have acceptable models with nonsignificant chi-squares, goodness-of-fit indices in the high .90s, and parsimonious-fit indices in the .50s. A nonsignificant chi-square means that a model is statistically acceptable insofar as the constraints on its parameters are consistent with aspects of the data not used in the estimation of free parameters. Goodness-of-fit indices will always be near unity when chi-square is nonsignificant and may even be near unity when chi-square is significant, indicating that the model with its constrained and estimated parameters reproduces the data very well, although statistically there is a detectable discrepancy.

#### *Inferential Statistics for Individual-level Results*

Various inferential statistical techniques were also used to test the individual level results for hypothesis testing. ToL was a significant predictor of perceived security effort ( $B=.321, p<.001$ ). RoL was a significant predictor of perceived security effort ( $B=.458, p<.001$ ). PSE was a significant predictor of perceived security performance ( $B = .734, p < .01$ ). PSP was a significant predictor of expected security outcome ( $B=.839, p <.001$ ). However, the biggest issue is that the variables are so highly correlated that everything is significant in Figure 8 and Table 10, which was also supported by the CFA results in Appendix E.

**Figure 8.** Results of Structural Equation Model**Table 10.** Results of Structural Equation Model

			B	S.E.	Beta	P
PSE	<---	ToL_Sum	0.321	0.041	0.351	***
PSE	<---	RoL	0.458	0.043	0.48	***
PSP	<---	PSE	0.734	0.027	0.79	***
ESO	<---	PSP	0.839	0.028	0.817	***

Note: N=455

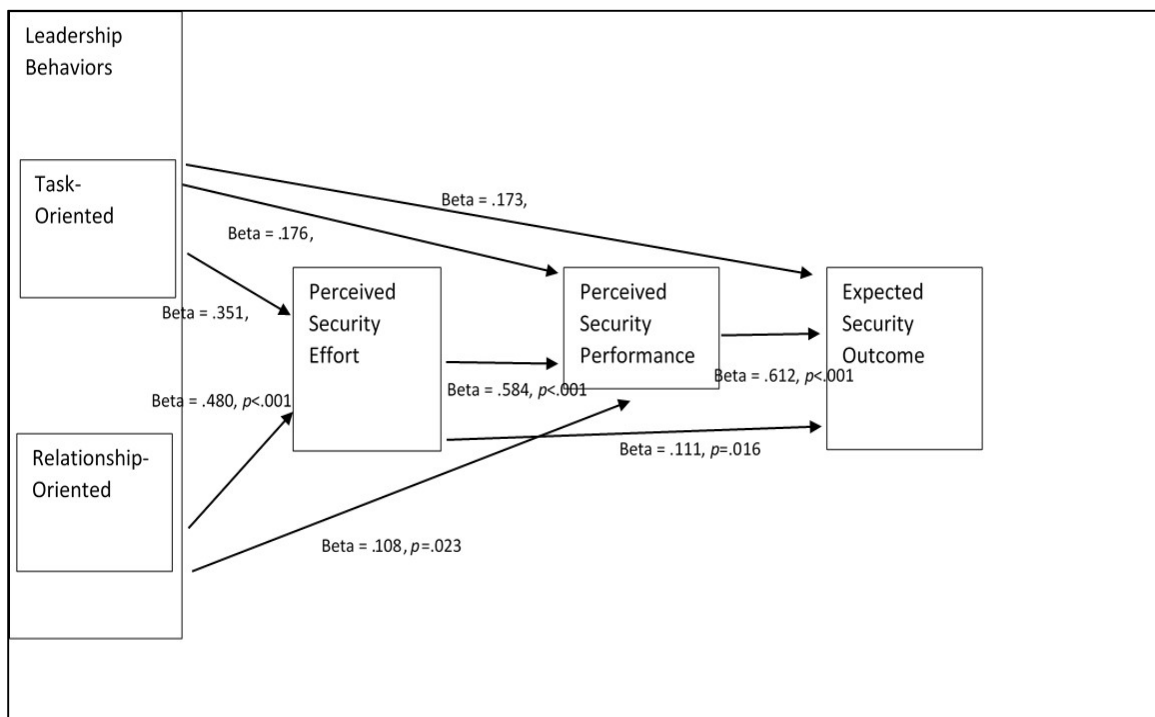
The correlation shows there is a strong linear relationship between the four IVs and ESO. The skewedness statistics for ESO is -1.136 (SE= .144) and the kurtosis is 1.286 (SE = .229), which are both within normal tolerances. Skew ranges from negative one to two and kurtosis ranges from negative three to three. But the Shapiro-Wilk test does show a significant value (S-W = .906,  $p < .001$ ), but this could also be a result of the larger sample size. The P-Plot in Figure 10 does have some deviations from the line, it's not overly deviated, which means the residuals are also fairly normally distributed.

#### *Inferential Statistics for Alternative Model-level Results*

**Alternative Structural Equation Model.** Alternative models were tested to identify a model better fit for the data. Alternative models included tests for partial mediation and

no mediation. For partial mediation, all potential relationships in the model were tested in Figure 9. Partial mediation showed that all variables except RoL had a direct significant relationship with the dependent variable (ESO). In addition, all independent variables (ToL, RoL, PSE, PSP) were tested against the dependent variable (ESO) with no mediation. These results suggest the partially mediated model is the best fit for the data.

**Figure 9.** Results of Alternative Structural Equation Model



**Table 11.** Complete SEM Model

DV	IV	B	S.E.	Beta	P
PSE	<--- ToL_Sum	0.32	0.04	0.35	***
PSE	<--- RoL	0.46	0.04	0.48	***
PSP	<--- ToL_Sum	0.15	0.04	0.18	***
PSP	<--- RoL	0.10	0.04	0.11	0.023
PSP	<--- PSE	0.54	0.04	0.58	***
ESO	<--- ToL_Sum	0.15	0.04	0.18	***
ESO	<--- RoL	0.00	0.04	0.00	0.933
ESO	<--- PSE	0.11	0.05	0.11	0.022
ESO	<--- PSP	0.63	0.05	0.61	***

The best model fit in Figure 9 suggests ToL has a better influence on ESO than RoL. The alternative model results in Table 13 suggest that ToL is the only leadership behavior that is a direct predictor of ESO, while RoL only influences ESO indirectly through mediating factors. Therefore, the best model fit involved partial mediation with three passed indices.

**Pearson's Chi-square.** The results revealed the Chi-square is  $\chi^2(5) = .007, p = .933$ , which means the model is a good fit against the alternative model.

**Comparative Fit Index (CFI).** The results revealed the CFI was 1.0, which indicates the model was a good fit.

**Root Mean Square Error of Approximation (RMSEA).** The results revealed the RMSEA was .633, which means the model was a good fit.

**Table 12.** Non-mediating SEM of ESO

DV	IV	B	S.E.	Beta	P	
ESO	<---	ToL_Sum	0.152	0.037	0.175	***
ESO	<---	RoL	-0.003	0.041	-0.004	0.933
ESO	<---	PSE	0.107	0.047	0.112	0.022
ESO	<---	PSP	0.63	0.045	0.613	***

*Inferential Statistics for Individual-level Results*

All individual items were significant for the direct paths in Table 13. There were indirect effects in this model as well. ToL indirectly impacts ESO both through PSE and PSP (Beta = .272), so PSE and PSP mediated the impact of ToL. ToL relationship were partially mediated since it also directly impacts ESO. RoL only indirectly impacts ESO through PSP and PSE (Beta = .291), so its relationship to ESO is only mediated. PSE indirectly impacted ESO through PSP (Beta = .357), so its relationship is partially mediated since it also directly impacts ESO.

**Table 13.** Alternative Path Model for Expected Security Outcome

DV		IV	B	S.E.	Beta	P
PSP	<---	PSE	0.542	0.041	0.584	***
ESO	<---	PSE	0.106	0.044	0.111	0.016
ESO	<---	PSP	0.629	0.045	0.612	***
PSE	<---	RoL	0.458	0.043	0.480	***
PSP	<---	RoL	0.095	0.042	0.108	0.023
PSE	<---	ToL_Sum	0.321	0.041	0.351	***
PSP	<---	ToL_Sum	0.149	0.038	0.176	***
ESO	<---	ToL_Sum	0.151	0.033	0.173	***

Note: N = 455, \*\*\*P<.001

**Regression Analysis.** Although not originally proposed, additional regression analyses were performed due to the model fit failures and overly correlated items. These analyses helped better understand the relationship between constructs as well as check some of the assumptions of regression. Three separate regression analyses were performed on each of the proposed hypotheses. The results are consistent with those found using SEM; the regression analysis in Appendix F found significant evidence supporting each of the individual relationships.

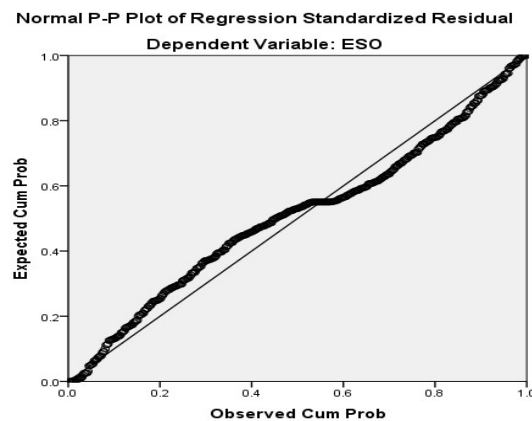
In addition, all variables were tested against the dependent variable in Table 14 to understand which variables had a significant relationship. The model was a significant predictor of ESO ( $F(4, 450) = 256.15, p < .001$ ). The model accounted for 69.2% of the variance in ESO. ToL was a significant predictor of ESO ( $B = .15, t(454) = 4.05, p < .001$ ). As ToL is increased, ESO is increased. PSE was a significant predictor of ESO ( $B = .11, t(454) = 2.29, p = .023$ ). As PSE is increased, ESO is increased. PSP was a significant predictor of ESO ( $B = .63, t(454) = 13.87, p < .001$ ). As PSP is increased, ESO is increased. RoL was the only variable that was not a significant predictor of ESO.



**Table 14.** Results of Regression Analysis

	B	Std. Error	Beta	p
(Constant)	4.34	0.96		***
ToL	0.15	0.04	0.17	***
RoL	0.00	0.04	0.00	
PSE	0.11	0.05	0.11	*
PSP	0.63	0.05	0.61	***
F			256.150	***
df			4, 450	
R2			0.692	

Note: N = 455, \*= $p < .05$ , \*\*= $p < .01$ , \*\*\*= $P < .001$

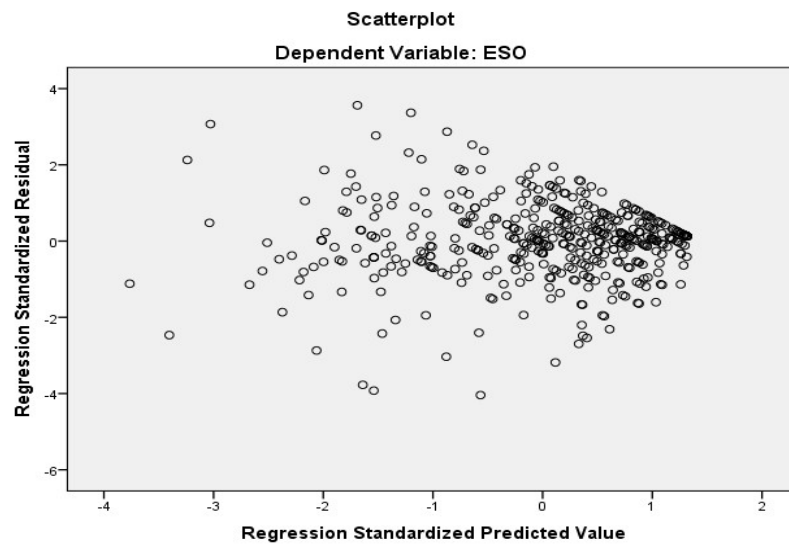
**Figure 10.** P-Plot of Regression Residuals

The correlations show the potential for issues of collinearity. This issue occurs when high intercorrelations exist between independent variables used for predictions (Mertler & Vannatta, 2013). Near collinearities adversely inflate the variance of the regression coefficients and amplify the effects of errors in the regression variables (Stewart, 1987). Variance of Inflation (VIF) a statistical approach to understand if the data are too intercorrelated to be useful was performed. Since VIFs were all below the cut of ten (Mertler & Vannatta, 2013, p. 167), which means there are no issues with collinearity.

There was also an aim to identify homoscedasticity. The issue of homoscedasticity is the assumption that the variability in scores for one continuous variable is roughly the

same at all values of another continuous variable ((Mertler & Vannatta, 2013). The Figure 11 scatterplot identified homoscedasticity, which could be part of the problem with the SEM. Transformation of the DV was considered as a way to compensate for this issue, but neither creating a standardized score nor log transformation was appropriate as they made the ESO more skewed.

**Figure 11.** Scatterplot of Regression Residuals



Lastly, there was a test for autocorrelations. This issue occurs when residuals are not independent of each other. The Durbin-Watson test is used to test for autocorrelations with a cutoff value between zero and four, while the generally accepted score is between 1.5 and 2.5 (Garson, 2012). The Durbin-Watson test showed there were no issues with autocorrelation (DB = 1.827).

### 4.3. Findings

This empirical study examined the behavioral influences of leaders on employees' security compliance. Organizations can use leadership concepts in the field of Information Systems (IS) security. This study created a path model using leadership concepts with the Expectancy Theory to test the influence of leadership behaviors on IS security policy compliance. The original path model had issues loading with a factor analysis: ToL cleanly loaded with RoL, and PSP cleanly loaded with ESO. Out of five model fit indices, three failed and two passed. These results suggested questionable reliability and validity of the path model. Either the instrument should have been better developed to measure constructs in the research model, or the theory is not a good fit. The results suggested the original path model developed for this study is not the best fit. It did not fail all tests, but it did not pass enough to be considered a good fit. However, an alternative model with partial mediation was tested that produced a model with a better fit. The alternative model tested all variables, and RoL was the only variable that did not show a direct significant relationship with ESO. The following are the findings linked to the research question and results in the proposed hypotheses.

For H<sub>1a</sub> the aim was to examine if ToL behaviors are positively associated with perceived security efforts. Individual level SEM results revealed ToL was a significant predictor of perceived security effort ( $B=.321, p<.001$ ).

For H<sub>1b</sub> the aim was to examine if RoL was positively associated with perceived security efforts. RoL was a significant predictor of perceived security effort ( $B=.458, p<.001$ ).

For H<sub>2</sub> the aim was to examine if perceived security efforts will be positively associated with perceived security performance. Perceived security effort was a significant predictor of performance ( $B = .734, p < .01$ )

For H<sub>3</sub> the aim was to examine if perceived security performance will be positively associated with the expected security outcome of employee policy compliance. Performance was a significant predictor of expected security outcomes ( $B=.839, p <.001$ ).

The research question investigated: *what leadership behaviors influence the expected security outcomes of IS security policy compliance?* The model was a significant predictor of ESO ( $F(4, 450) = 256.15, p<.001$ ). The model accounted for 69.2% of the variance in ESO. As ToL is increased, ESO is increased. RoL was the only variable with only an indirect influence through mediating factors instead of a direct significant influence on ESO. The final results of the analyses suggest ToL is the best fit leadership behavior with a direct and indirect influence on the expected outcome of IS security policy compliance.

#### **4.4. Summary**

This chapter addressed the results on data collected to understand the behavioral influences of leaders on the expected outcome of IS security policy compliance. The introduction briefly explained the results section. The data analysis section explained the results from the different phases of data collection. The findings section mapped the results to the research question and hypotheses. The major takeaway was that the original structural model developed using the expectancy theory is not the best fit for the data—which means the null hypotheses of test results are due to chance rather than an actual

relationship. However, an alternative structural model that was partially mediated produced better fit indices. In addition, individual level results revealed empirical evidence to suggest ToL behaviors are better suited for encouraging employee adherence to policy. The next chapter provided a conclusion to the research study.

## **Chapter 5**

### **Conclusion**

#### **5.1. Introduction**

The primary purpose of this chapter was to present findings and conclude the research study. After previous chapters have provided an introduction, literature review, methodology, and results—this chapter offers a conclusion with implications, limitations, recommendations. Section 5.2 initiates with a discussion that summarizes the entire research study. Section 5.3 provides implications to practitioners and researchers with a connection to how findings contribute to the IS discipline's body of knowledge. Section 5.4 outlines factors that limited the research study. Section 5.5 offers recommendations for future research. Lastly, Section 5.6 provides an overall summary of dissertation.

#### **5.2. Discussion**

This empirical study examined the behavioral influences of leaders on employees' security compliance. Organizations can use leadership concepts in the field of IS security. Despite the adoption of technical and managerial approaches, organizations still face issues motivating employee IS security compliance. This dissertation argued that organizations need strong leadership to encourage employees. Using the expectancy theory, this paper created a theoretical model to help understand the influence of task and relationship-oriented leadership behaviors on nontechnical controls IS security compliance. The conceptual underpinnings translated into perceived security effort,

perceived security performance, and expected security outcomes. The theoretical model was validated using Structural Equation Modeling (SEM) and Confirmatory Factor Analysis (CFA).

The model-level results revealed a structural model that suggests task-oriented leadership is better suited for motivating IS security compliance. In addition, individual-level results provide additional support that task-oriented leadership was the only leadership behavior with a direct relationship with IS security compliance. These findings contribute to the body of knowledge that compliance behaviors are extrinsically motivated. Future research should aim to further examine the role of intrinsic motivators, and the indirect influence of relationship-oriented leadership behaviors on IS security policy compliance with more rigorous approaches. The next sections offer considerations for practitioners and research as well as recommendations for how these results can be strengthened.

### **5.3. Implications**

The findings of the current study are practically relevant and can be linked to existing IS literature. Herath and Rao (2009) explained that there are two distinct schools of thought regarding IS security policy compliance: (1) suggests compliance influenced extrinsically; (2) suggests compliance is influenced intrinsically. IS literature supports there are both extrinsic and intrinsic factors that influence IS security compliance. Padayachee (2012) published a taxonomy of compliant information security behavior that further argued there is a role for extrinsic and intrinsic motivation in IS security compliance. Although both factors have evidence demonstrating their significance, the question becomes understanding if extrinsic or intrinsic factors have a more significant

influence on IS security compliance. This question is unclear in IS literature—most research studies evaluate one or the other instead of both at the same time to discern the difference. These underlying factors are fundamental in understanding IS security compliance. For years, researchers consistently aimed to understand the relationship of extrinsic and intrinsic motivation and IS security compliance. Oftentimes, research findings reveal conflicting results in literature.

Son (2011) found evidence that while extrinsic factors are important, intrinsic factors have an increased chance of motivating security compliance. These findings are similar to that of (Bulgurcu et al., 2010), which suggests an intrinsic approach would likely be more successful because individuals are rationally influenced to comply with security policies based on normative beliefs, self-efficacy, and attitudes. This is also consistent with Safa et al. (2016) that found attitude to IS security policies to have a significant influence with compliance behaviors—and attitude is influenced by commitment and personal norms. While earning a reputation and gaining a promotion are considered extrinsic motivators, curiosity and satisfaction are intrinsic motivators (Safa & Von Solms, 2016). In addition, all measures are expected to fall short without user awareness (Siponen & Kajava, 1998); it is important for user's education and training to develop intrinsic motivation to encourage security compliance these findings contradict (Siponen, 2000). However, other studies suggest extrinsic factors is a significant factor influencing IS security compliance. Vance et al. (2012) suggests that non-compliant behavior is often formed out of bad habits, and organizations must ensure security controls are in place to mitigate those habits. Furthermore, Safa and Von Solms (2016) found extrinsic motivation to have a more significant influence on attitudes towards compliance than



intrinsic motivation.

Leadership behaviors are divided into similar concepts related to extrinsic and intrinsic motivation (Northouse, 2016). The current study examines ToL which aligns extrinsically, and RoL which aligns intrinsically. As a result, this study's research question: "*what leadership behaviors influence the expected security outcomes of IS security policy compliance?*" examines if ToL or RoL have a more significant influence on IS security compliance. This translates to understanding if IS security compliance is more extrinsically or intrinsically motivated.

This study provided researchers and practitioners evidence that found ToL have a more significant direct influence than RoL behaviors on IS security policy compliance. The current findings are consistent with the findings of Humaidi and Balakrishnan (2015), which found that transactional leadership has a direct and indirect influence on IS security compliance behavior, while transformational leadership's influence was only indirect. While transactional leadership takes a strict approach with enforced behavioral adherence in the culture environment, transformational leaders are more actively engaged with an aim to motivate employees (Humaidi & Balakrishnan, 2015). The transactional leadership style is closely related to ToL, while RoL is closely related to transformation leadership. This means transactional leadership which focuses more on task-oriented actions may be better suited in motivating IS security compliance. Researchers suggest the perceived benefit often overshadows the perceived risk during the process of rationally calculating security compliance (Hu et al., 2011).

The results of the current study also indicated RoL behaviors have no direct significant relationship with IS security compliance. The current findings are consistent

with the findings of Humaidi and Balakrishnan (2015), which found transformational leadership to have no direct significant relationship with IS security compliance. It is unclear why RoL has no direct influence on IS security compliance. While RoL behaviors has a positive influence in other areas of business, for instance organizational climate, to increase commitment and reduce turnover (Holloway, 2012), it does not appear to have a significant influence on IS security compliance. Since other research suggests that organizational commitment influences IS security compliance (Herath & Rao, 2009; Safa et al., 2016), it could be that RoL has a mediating or moderating influence on IS security commitment. This study further supports that RoL may indirectly influence IS security compliance.

Researchers can use this study to guide their understanding of the relationship between leadership behaviors and IS security compliance. Leadership behaviors should be conceptualized more in IS security leadership. Practitioners should focus on encouraging ToL approaches into there is security programs—leveraging strong security policies, awareness, and enforcement (Knapp & Ferrante, 2012). Guhr et al. (2019) found evidence suggesting transformational leadership, with more relationship-oriented behaviors, does have a positive association with IS security compliance. However, ToL should remain the primary focus in IS security compliance until addition research on RoL is conducted. Although there are mixed results found in literature, researchers and practitioners should take this into consideration when proceeding forwards.

#### **5.4. Limitations**

Sekaran and Bougie (2013) recommends all research reports should outline the limitation that confounded the study. These limitations should cover topics such as

sampling, data collection, instrument, and other areas that affected the results. For the current study, there were a couple potential limitations that can be mitigated in future studies.

The theoretical model developed did not pass all GoF indices, which means the model could have been more predictive. In addition, there were some concern about homoscedasticity in the data, which could have an effect on the analysis. A more rigorous approach could have been provided to further develop the research instrument. Quantitative data screening techniques during the study could have been used (DeSimone, 2015). For instance, a different substantive validity analysis may have help reduce better results by evaluating two indicators. The first is the portion of substantive agreement, which is “the proportion of respondents who assign an item to its intended construct” (Anderson & Gerbing, 1991, p. 734; Hinkin, 1998, p. 108). The proportion of substantive agreement is calculated by dividing the number of participants who correctly assign an item to its intended construct by the total number of participants. However, the downfall of this indicator is that it does not explain to us the degree in which an item is reflected in other undesignated constructs (Anderson & Gerbing, 1991). In addition, the second indicator, the substantive validity coefficient is preferred. The substantive validity coefficient is “the degree to which each rater assigned an item to its intended construct” more than other constructs (Hinkin, 1998, p. 108). To calculate the substantive validity coefficient, a researcher will subtract “the highest number of assignments of the item to any other construct in the set” (p. 734) from the number of participants who correctly assign an item to its intended construct and divide the result by the total number of participants (Anderson & Gerbing, 1991).

The strategy for substantive validity analysis involves the plan of construct definitions, the provision of all items nominated for validation in a randomized order without tying them to a construct and asking participants to align the items to the constructs based on their understanding of the definition of the constructs. Since values for substantive-validity coefficient range from -1.0 to 1.0, larger values are indicative of a substantive validity. Secondly, a sizable, but negative number indicates substantive validity as well, but shows that the validity is for an unintended construct (Anderson & Gerbing, 1991). The underpinning in Anderson and Gerbing (1991) is that alteration of an item and/or the construct definition is allowed if an item fails to obtain sufficiently high substantive-validity coefficient. The lack of a more rigorous approach to construct validity likely contributes to the high levels of correlation in the research model.

In addition, the sampling of women exceeded the sampling of men which is not representative of the IT environment. This could be a concern since males and females tend to have some differences in their security compliance behaviors (Anwar et al., 2017); except research suggest women tend to favor relationship-oriented behaviors (Carless, 1998). However, this is a minor concern considering how both genders reported in favor of ToL.

## **5.5. Recommendations**

This is the only known study that aimed to examine the influence of ToL and RoL behaviors on IS security compliance. A similar study examined the role of leadership styles, transactional and transformational, on IS security compliance (Humaidi & Balakrishnan, 2015). The main findings reveal ToL has a direct significant influence on IS security compliance, while RoL was only indirect. These results are consistent with

the findings from Humaidi and Balakrishnan (2015) who identified transactional leadership has a direct significant relationship with IS security compliance, while transformational was only indirect. IS research studies should aim to produce results that have theoretical and practical relevance (Rosemann & Vessey, 2008). Despite the limitations, these findings are relevant to both practitioners and scholars.

This research study strengthens the argument that practitioners should focus on leveraging extrinsic motivators with ToL and transactional leadership. This means IS security programs should focus on ToL with an emphasis on rewards outside the individual. This can be achieved by enforcing strict IS security controls with an emphasis on rewards, threat certainty/severity, and punishments.

Scholars should leverage more rigorous approaches understand the role of intrinsic motivation with RoL and transformational leadership. There are several studies that suggest this approach has an influence on IS security compliance. Conversely, it appears when measured against the opposite end of the spectrum—intrinsic approaches fall short in test results. The results of the current study indicate the relationship between RoL and IS security compliance may not be direct like ToL. Additional research is necessary to identify potential mediating or moderating relationships for RoL behaviors. This makes sense since the intrinsic motivates that influence RoL are more difficult to measure. Instead of directly influencing IS security compliance, it is very likely that RoL has a indirect (mediating or moderating) relationship or influences other factors.

## **5.6. Summary**

This chapter concluded the empirical research study that examined the behavioral influences of leaders on employees' security compliance. The conclusion provided a brief

summary of the study arguing for organizations to use strong leadership concepts in the field of IS security. This study identified that individual level results reveal empirical evidence to suggest ToL behaviors are better suited for encouraging employee adherence to policy. This study can be linked existing IS security compliance literature related to extrinsic and intrinsic motivation as well as transaction and transformational leadership. The results suggest that extrinsic motivation and transactional leadership should be the focus of IS security programs. Although the results were not as strong as expected, a future replication of this study is advised to develop a stronger instrument. In addition, future research should further examine extrinsic motivators similar to RoL behavior to understand the indirect influence on factors like IS security commitment.

## Appendices

## Appendix A: Approval Letter from Institutional Review Board



### MEMORANDUM

To: **Marcus A Winkfield**

From: **Ling Wang, Ph.D.,  
Center Representative, Institutional Review Board**

Date: **April 16, 2019**

Re: **IRB #: 2019-230; Title, "Information Systems Security Leadership: An Empirical Study of Behavioral Influences of Leaders on Employees' Security Compliance"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under 45 CFR 46.101(b) (Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies). You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

- 1) **CONSENT:** If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.
- 2) **ADVERSE EVENTS/UNANTICIPATED PROBLEMS:** The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.
- 3) **AMENDMENTS:** Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

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

Cc: **Gurvirender P Tejay, Ph.D.  
Ling Wang, Ph.D.**



## Appendix B: Results of Content Validity Ratio

Item #	# of Essential	# of Useful but not Essential	# of Not Essential	Percent of Essential Selection	CVR (ne-N/2)/N/2)	Type of Data	
Q1-Q3	-	-	-	-	-	Demographic	
Q4	7	1	0	87.50%	0.75		
Q5	1	3	4	12.50%	<b>-0.75</b>		
Q6	2	5	1	25.00%	<b>-0.50</b>		
Q7	5	3	0	62.50%	<b>0.25</b>		
Q8	4	2	2	50.00%	<b>0.00</b>		
Q9	3	4	1	37.50%	<b>-0.25</b>		
Q10	6	1	1	75.00%	0.50		
Q11	8	0	0	100.00%	1.00		
Q12	8	0	0	100.00%	1.00		
Q13	4	4	0	50.00%	<b>0.00</b>		
Q14	-	-	-	-	-		-
Q15	5	2	0	71.43%	<b>0.42</b>		Main Study
Q16	5	0	1	83.33%	0.66		
Q17	5	0	2	71.43%	<b>0.42</b>		
Q18	6	0	1	85.71%	0.71		
Q19	6	1	0	85.71%	0.71		
Q20	6	1	0	85.71%	0.71		
Q21	3	4	0	42.86%	<b>-0.14</b>		
Q22	7	0	0	100.00%	1.00		
Q23	6	1	0	85.71%	0.71		
Q24	4	3	0	57.14%	<b>0.14</b>		
Q25	6	1	0	85.71%	0.71		
Q26	6	1	0	85.71%	0.71		
Q27	6	1	0	85.71%	0.71		
Q28	6	1	0	85.71%	0.71		
Q29	7	0	0	100.00%	1.00		
Q30	6	1	0	85.71%	0.71		
Q31	5	1	1	71.43%	<b>0.42</b>		
Q32	5	1	0	83.33%	0.66		
Q33	7	0	0	100.00%	1.00		
Q34	6	1	0	85.71%	0.71		
Q35	6	0	1	85.71%	0.71		

Q36	5	2	0	71.43%	<b>0.42</b>
Q37	5	0	1	83.33%	0.66
Q38	5	1	1	71.43%	<b>0.42</b>
Q39	7	0	0	100.00%	1.00
Q40	5	1	0	83.33%	0.66
Q41	6	0	1	85.71%	0.71
Q42	6	1	0	85.71%	0.71
Q43	6	1	0	85.71%	0.71
Q44	6	1	0	85.71%	0.71
Q45	-	-	-	-	-
Q46	-	-	-	-	-

Note: N=6-8; For missing values, calculations were adjusted. CVRs below the minimum requirement are grayed and bolded.

**Appendix C: Minimum Values for Content Validity Ratio**

<b>No. of Panellists</b>	<b>Minimum Value</b>
5	.99
6	.99
7	.99
8	.75
9	.78
10	.62
11	.59
12	.56
13	.54
14	.51
15	.49
20	.42
25	.37
30	.33
35	.31
40	.29

---

CVR table adapted from Lawshe (1975)

## **Appendix D: Survey Instrument for Pretest and Main Study**

### **An Empirical Study of Behavioral Influences of Leaders on Employees Security Compliance**

---

#### **Start of Block: Introduction**

*Q0 Information Systems Security Leadership: An Empirical Study of Behavioral Influences of Leaders on Employees' Security Compliance*

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

##### **Who is doing this research study?**

The person doing this study is Marcus Winkfield with Nova Southeastern University's College of Engineering and Computing. He will be helped by Dr. Gurvirender Tejay.

##### **Why are you asking me to be in this research study?**

You are being asked to take part in this research study because you are a business professional in a field related to Information Technology (IT).

##### **Why is this research being done?**

The purpose of this study is to understand the influence of task and relationship leadership behaviors on nontechnical controls in IS security compliance. This study develops a theoretical model, and the results used to test the model can help advance future research in the field of IS security.

##### **What will I be doing if I agree to be in this research study?**

You will be taking a one-time, anonymous survey. The survey will take approximately 15 – 20 minutes to complete.

##### **Are there possible risks and discomforts to me?**

This research study involves minimal risk to you. To the best of our knowledge, the items covered will be doing have no more risk of harm than you would have in everyday life.

##### **What happens if I do not want to be in this research study?**

You can decide not to participate in this research and it will not be held against you. You can exit the survey at any time.

##### **Will it cost me anything? Will I get paid for being in the study?**

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

##### **How will you keep my information private?**

Your responses are anonymous. Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law Information we

learn about you in this research study will be handled in a confidential manner, within the limits of the law and will be limited to people who have a need to review this information. Survey data will be collected on Qualtrics. This website is dedicated to the creation, collection, and management of survey data using various forms of encryption to protect the data. This data will be available to the researcher, the Institutional Review Board and other representatives of this institution, and any regulatory and granting agencies (if applicable). If we publish the results of the study in a scientific journal or book, we will not identify you. All confidential data will be kept securely on Qualtrics' data center. All data will be kept for 36 months from the end of the study and destroyed after that time by deletion via website features.

**Who can I talk to about the study?**

If you have questions, you can contact:

**Primary Contact:**

Marcus Winkfield – [mw1558@mynsu.nova.edu](mailto:mw1558@mynsu.nova.edu)

**Secondary Contact:**

Dr. Gurvirender Tejay – [tejay@nova.edu](mailto:tejay@nova.edu)

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

**Do you understand, and do you want to be in the study?**

If you have read the information above and voluntarily wish to participate in this research study, please proceed.

**End of Block: Introduction**

---

**Start of Block: Preliminary Question to Participate**



Q1

Do you work in Information Technology (IT)?

(or)

Do you work closely with IT professionals?

Yes (1)

No (2)

*Skip To: End of Block If Do you work in an information technology or closely related field? \*\*If not, you will not be able... = No*

### End of Block: Preliminary Question to Participate

---

### Start of Block: Demographic Items

**These following items will help obtain an understanding of the demographic from which data was collected.**

-----

Q2 Years in IT or closely related field?

- 1 year or shorter (1)
  - 2 - 3 years (2)
  - 4 - 5 years (3)
  - 6 - 7 years (4)
  - 8 - 9 years (5)
  - 10 years or more (6)
- 

Q3 My organization has defined information security policies that are made available to employees?

- Yes (1)
  - No (2)
  - Not Sure (3)
-

Q4 I am aware of the basic information security requirements in my organization?

- Yes (1)
  - No (2)
  - Not Sure (3)
- 

Q5 My organization has a Chief Information Security Officer (CISO) who is responsible for the organization's information security program?

- Yes (1)
  - No (2)
  - Not Sure (3)
- 

Q6 Sex?

- Male (1)
  - Female (2)
  - No Response (3)
-

Q7 Highest level of education (degree) completed?

- None (1)
  - High school or equivalent (2)
  - Associate Degree (3)
  - Bachelor Degree (4)
  - Graduate Degree (5)
  - Professional Degree (6)
  - Other (7)
- 

Q8 Age Range?

- 20 years and younger (1)
  - 21 - 30 years (2)
  - 31 - 40 years (3)
  - 41 - 50 years (4)
  - 51 - 60 years (6)
  - 61 years and older (7)
-



Q9 Employment Category?

- Student (1)
- Self-employment (2)
- Private organization (3)
- Government employment (4)
- Government contractor (5)
- Non-profit organization (6)
- Other (7)

**End of Block: Demographic Items**

---

**Start of Block: Main Items**

**Answer the following items based on the behaviors of leaders in your organization.**

-----

Q10 Sets standards of performance for group members.

- Never (1)
  - Hardly Ever (2)
  - Seldom (3)
  - Occasionally (4)
  - Often (5)
  - Usually (6)
  - Always (7)
-

Q11 Defines roles and responsibilities for each group member.

-----

Q12 Clarifies his or her own role within the group.

-----

Q13 Provides a plan for how work is to be done.

-----

Q14 Makes his or her perspective clear to others.

-----

Q15 Tells group members what they are expected to do.

-----

Q16 Shows flexibility in making decisions.

-----

Q17 Responds favorably to suggestions made by others.

-----

Q18 Helps others in group feel comfortable.

-----

Q19 Discloses thoughts and feelings to group members.

-----

Q20 Shows concern for the well-being of others.

-----

Q21 Communicates actively with group members.

---

**Answer the following items based on the perception of your organization.**

---

Q22 I believe my organization encourages strong commitment and trust.

---

Q23 I think my organization encourages top management support.

---

Q24 I believe my organization encourages user participation.

---

Q25 I think my organization focuses on policy decisions.

---

Q26 I believe my organization focuses on analysis and design.

---

Q27 I believe my organization focuses on process improvement.

---

**Answer the following items based on the perception of your organization.**

---

Q28 I think my organization's security program produces noticeable results.

---

Q29 I believe my organization's security program prevents security incidents.

---

Q30 I believe my organization's security program has strong implementation.

---

Q31 I think my organization's security program has strong performance.

---

Q32 I think my organization's security program prevents security threats.

---

Q33 I believe my organization's security program operates effectively.

---

**Answer the following items based your expectations of employees within your organization.**

---

Q34 Employees within your organization follow security policies for access control.

---

Q35 Employees within your organization follow security policies for physical and environment.

---

Q36 Employees within your organization follow security policies that limit individual access.

---

Q37 Employees within your organization follow security policies for incident response.

---

Q38 Employees within your organization obtain physical access to resources when required.

---

Q39 Employees within your organization report incidents where security polices are violated.

## Appendix E: Results of Confirmatory Factor Analysis

### *Initial CFA*

	Communalities	Rotated Component Matrix	
		1	2
TOL1	0.530	0.380	<b>0.621</b>
TOL2	0.631	0.379	<b>0.698</b>
TOL3	0.580	0.316	<b>0.693</b>
TOL4	0.628	0.343	<b>0.714</b>
TOL5	0.612	0.295	<b>0.725</b>
TOL6	0.604	0.318	<b>0.709</b>
ROL1	0.599	0.240	<b>0.736</b>
ROL2	0.612	0.250	<b>0.741</b>
ROL3	0.672	0.303	<b>0.762</b>
ROL4	0.541	0.237	<b>0.696</b>
ROL5	0.635	0.359	<b>0.711</b>
ROL6	0.634	0.357	<b>0.712</b>
PSE1	0.625	0.548	0.569
PSE2	0.573	0.480	0.586
PSE3	0.572	0.508	0.560
PSE4	0.565	0.556	0.506
PSE5	0.484	0.574	0.393
PSE6	0.622	0.589	0.525
PSP1	0.622	0.660	0.432
PSP2	0.646	<b>0.710</b>	0.377
PSP3	0.611	<b>0.700</b>	0.348
PSP4	0.707	<b>0.766</b>	0.347
PSP5	0.627	<b>0.749</b>	0.255

PSP6	0.658	<b>0.746</b>	0.319
ESO1	0.616	<b>0.734</b>	0.278
ESO2	0.624	<b>0.738</b>	0.282
ESO4	0.558	<b>0.673</b>	0.325
ESO3	0.657	<b>0.769</b>	0.255
ESO5	0.592	<b>0.705</b>	0.308
ESO6	0.501	<b>0.657</b>	0.263

---

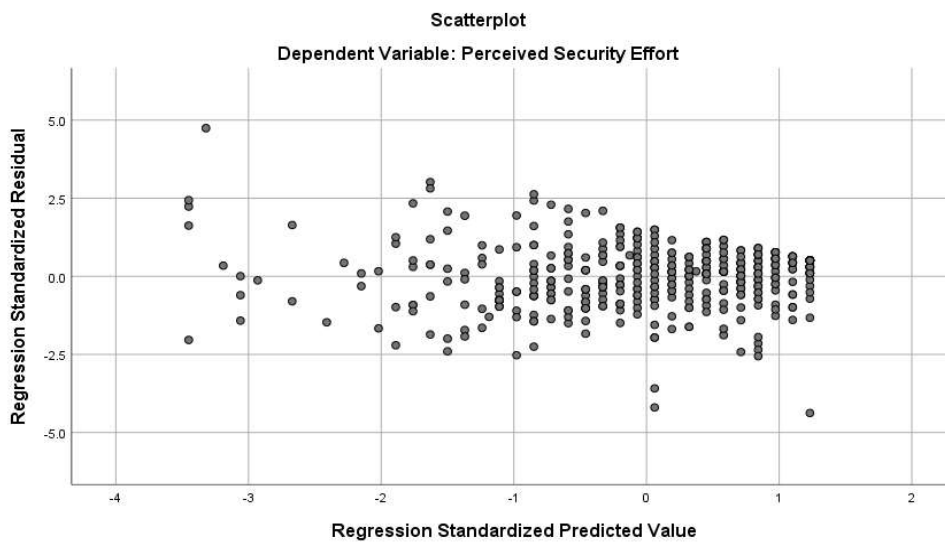
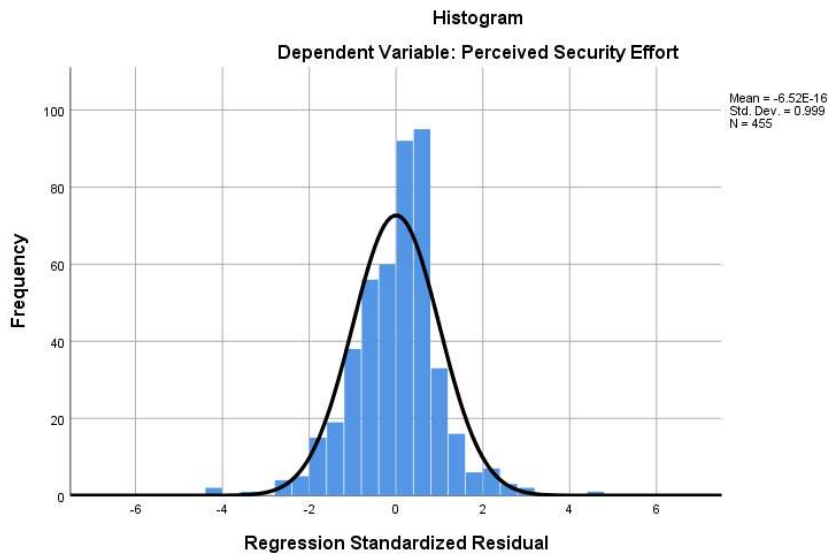
Notes: Bold indicates the question loaded cleanly on a single factor.

Extraction Method: Principal Component Analysis.

Rotation converged in 3 iterations.

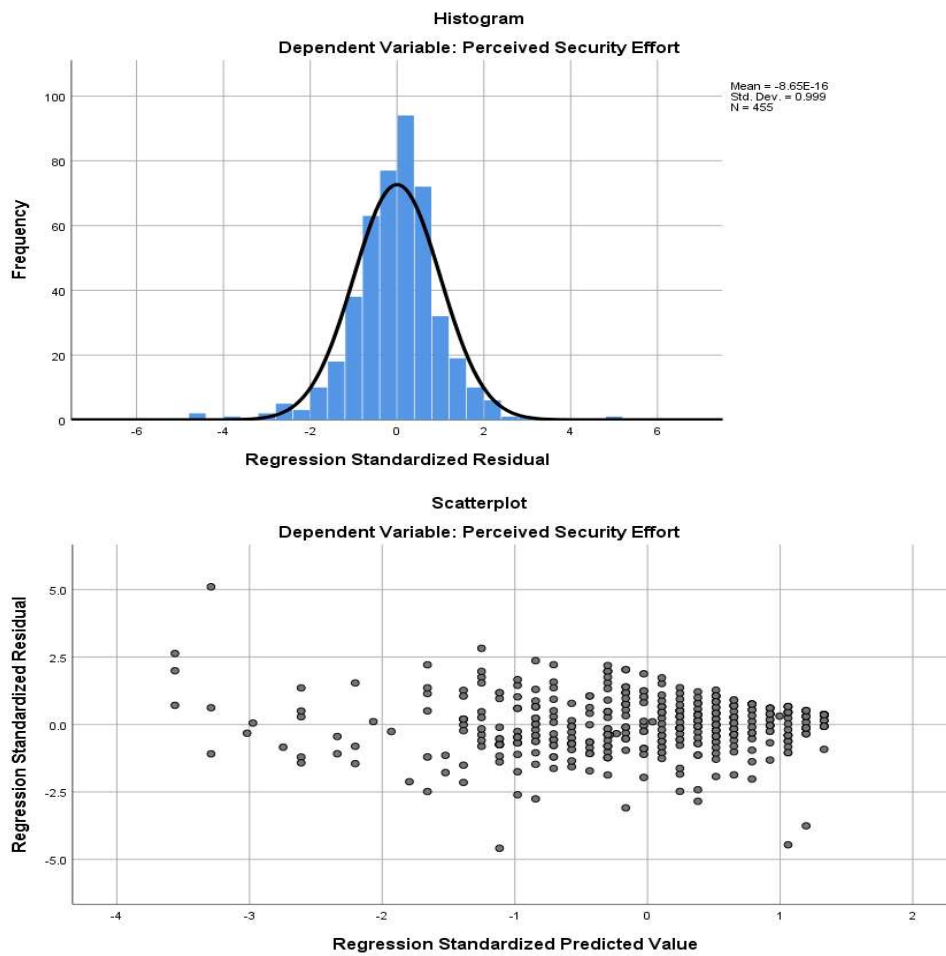
## Appendix F: Regression Analysis for Hypotheses Testing

**H1a: Task-oriented leadership behavior are positively associated with perceived security efforts.**

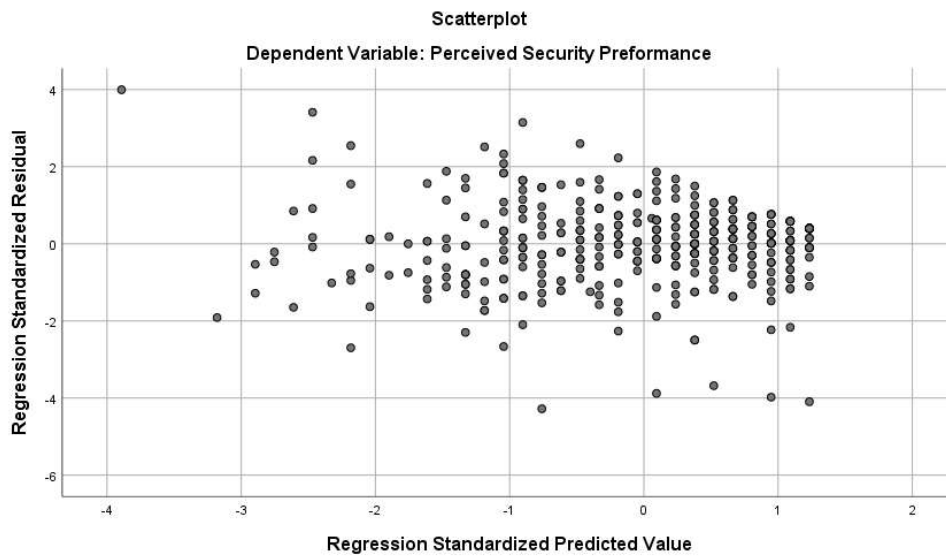
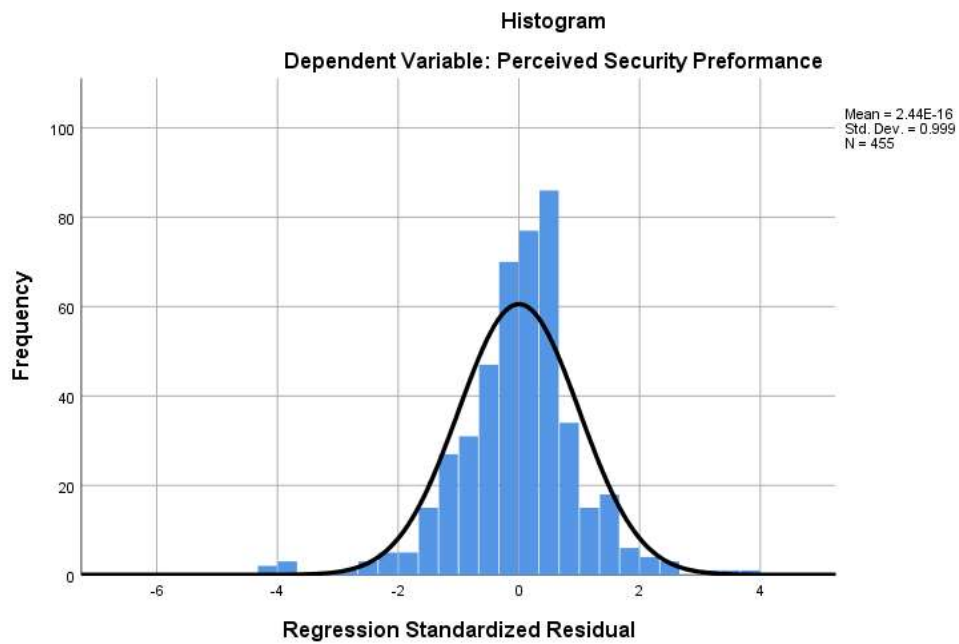




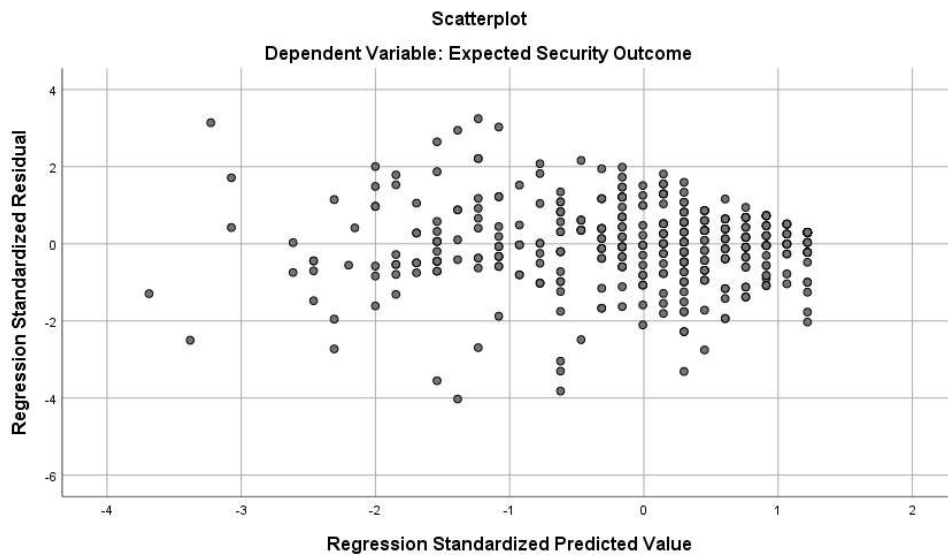
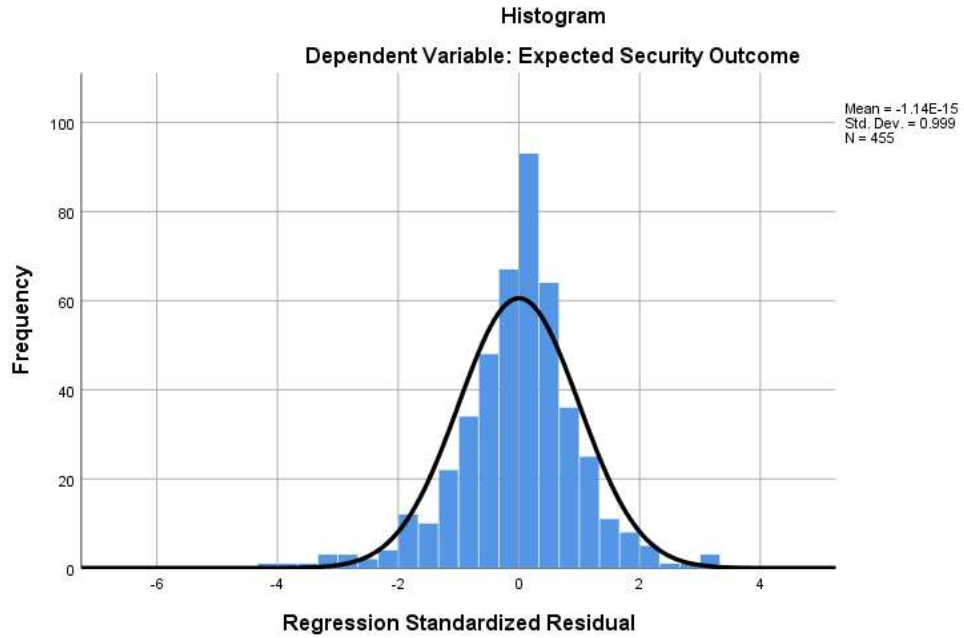
**H1b: Relationship-oriented leadership behavior are positively associated with perceived security efforts.**



**H2: Perceived security efforts are positively associated with perceived security performance.**



**H3: Perceived security performance are positively associated with the expected security outcome of employee policy compliance.**



## References

- Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12), 40-46.
- Agrafiotis, I., Nurse, J. R., Buckley, O., Legg, P., Creese, S., & Goldsmith, M. (2015). Identifying attack patterns for insider threat detection. *Computer Fraud & Security*, 2015(7), 9-17.
- Allison, P. D. (2003). Missing data techniques for structural equation modeling. *Journal of Abnormal Psychology*, 112(4), 545.
- Alter, S., & Sherer, S. A. (2004). A general, but readily adaptable model of information system risk. *Communications of the Association for Information Systems*, 14(1), 1.
- Anderson, J. C., & Gerbing, D. W. (1991). Predicting the performance of measures in a confirmatory factor analysis with a pretest assessment of their substantive validities. *Journal of Applied Psychology*, 76(5), 732.
- Anderson, R., & Moore, T. (2009). Information security: Where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 367(1898), 2717-2727.
- Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437-443.
- Arpaci, I., & Baloğlu, M. (2016). The impact of cultural collectivism on knowledge sharing among information technology majoring undergraduates. *Computers in Human Behavior*, 56, 65-71.
- Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy?. *Computers & Security*, 39, 396-405.
- Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1-13.
- Balozian, P., Leidner, D., & Warkentin, M. (2019). Managers' and employees' differing responses to security approaches. *Journal of Computer Information Systems*, 59(3), 197-210.
- Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security*, 59, 9-25.

- Baskerville, R. (1988). *Designing information systems security*. New York, NY: John Wiley.
- Baskerville, R. (1991). Risk analysis: An interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems*, 1(2), 121-130.
- Bell, E., Bryman, A., & Harley, B. (2019). *Business research methods: Fifth edition*. United Kingdom: Oxford University Press.
- Berezina, K., Cobanoglu, C., Miller, B. L., & Kwansa, F. A. (2012). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *International Journal of Contemporary Hospitality Management*, 24(7), 991-1010.
- Bhattacharya, D. (2011). Leadership styles and information security in small businesses. *Information Management & Computer Security*, 19(5), 300-312.
- Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. *Proceedings New Security Paradigms*. Retrieved from [http://ns2.datacontact.dc.hu/~mfelegyhazi/courses/EconSec/readings/03\\_Blakley2001infosec.pdf](http://ns2.datacontact.dc.hu/~mfelegyhazi/courses/EconSec/readings/03_Blakley2001infosec.pdf)
- Blau, G. (1993). Operationalizing direction and level of effort and testing their relationships to individual job performance. *Organizational Behavior and Human Decision Processes*, 55(1), 152-170.
- Blunch, N. (2012). *Introduction to structural equation modeling using IBM SPSS statistics and AMOS*. Thousand Oaks, CA: Sage Publications.
- Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information security and risk management. *Communications of the ACM*, 51(4), 64-68.
- Boell, S. K., & Cecez-Kecmanovic, D. (2015). What is an information system?. *HICSS 2015 Proceedings*. Retrieved from <http://ieeexplore.ieee.org/abstract/document/7070407/>
- Bojanc, R., & Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, 28(5), 413-422.
- Borgatta, E. F., Bales, R. F., & Couch, A. S. (1954). Some findings relevant to the great man theory of leadership. *American Sociological Review*, 19(6), 755-759.

- Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164.
- Bradbury, D. (2011). A Day in the Life of a CISO. *Infosecurity, 8*(3), 24-27.
- Brock, L., & Levy, Y. (2013). The market value of information system (IS) security for e-banking. *Online Journal of Applied Knowledge Management, 1*(1), 1.
- Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long range planning, 48*(4), 265-276.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.
- Burke, C. S., Stagl, K. C., Klein, C., Goodwin, G. F., Salas, E., & Halpin, S. M. (2006). What type of leadership behaviors are functional in teams? A meta-analysis. *The Leadership Quarterly, 17*(3), 288-307.
- Burton, F. G., Chen, Y. N., Grover, V., & Stewart, K. A. (1992). An application of expectancy theory for assessing user motivation to utilize an expert system. *Journal of Management Information Systems, 9*(3), 183-198.
- Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431-448.
- Carless, S. A. (1998). Gender differences in transformational leadership: An examination of superior, leader, and subordinate perspectives. *Sex Roles, 39*(11-12), 887-902.
- Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004). Economics of IT security management: Four improvements to current security practices. *Communications of the Association for Information Systems, 14*65-75.
- Chen, F. F. (2007). Sensitivity of goodness of fit indexes to lack of measurement invariance. *Structural Equation Modeling, 14*(3), 464-504.
- Cheng, L., Li, W., Zhai, Q., & Smyth, R. (2014). Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. *Computers in Human Behavior, 38*, 220-228.
- Chiang, C. F., & Jang, S. S. (2008). An expectancy theory model for hotel employee motivation. *International Journal of Hospitality Management, 27*(2), 313-322.

- Choi, M. (2016). Leadership of Information Security Manager on the Effectiveness of Information Systems Security for Secure Sustainable Computing. *Sustainability*, 8(7), 638.
- Collmann, J., & Cooper, T. (2007). Breaching the security of the Kaiser Permanente Internet patient portal: the organizational foundations of information security. *Journal of the American Medical Informatics Association*, 14(2), 239-243.
- Colwill, C. (2009). Human factors in information security: The insider threat—Who can you trust these days? *Information Security Technical Report*, 14(4), 186-196.
- Cram, W. A., & D'Arcy, J. (2016). Teaching Information Security in Business Schools: Current Practices and a Proposed Direction for the Future. *Communications of the Association for Information Systems*, 39(1), 3.
- Creswell, J. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*. Thousand Oaks, CA: Sage Publications.
- Cronin Jr, J. J., & Taylor, S. A. (1992). Measuring service quality: A reexamination and extension. *The Journal of Marketing*, 55-68.
- Cuganesan, S., Steele, C., & Hart, A. (2018). How senior management and workplace norms influence information security attitudes and self-efficacy. *Behaviour & Information Technology*, 37(1), 50-65.
- D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, 22(5), 474-489.
- D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics*, 89(1), 59-71.
- Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196-207.
- DeSimone, J. A., Harms, P. D., & DeSimone, A. J. (2015). Best practice recommendations for data screening. *Journal of Organizational Behavior*, 36(2), 171-181.
- Dhillon, G., & Backhouse, J. (1996). Risks in the use of information technology within organizations. *International Journal of Information Management*, 16(1), 65-74.
- Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, 11(2), 127-153.

- Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, 16(3), 293-314.
- Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal*, 19(4), 391-412.
- Dunkerley, K., & Tejay, G. (2009). Developing an information systems security success model for egovernment context. *AMCIS 2009 Proceedings*. Retrieved from <http://aisel.aisnet.org/amcis2009/346/>
- Elahi, G., & Yu, E. (2007). A goal oriented approach for modeling and analyzing security trade-offs. *Conceptual Modeling-ER 2007*. Retrieved from [https://link.springer.com/chapter/10.1007/978-3-540-75563-0\\_26](https://link.springer.com/chapter/10.1007/978-3-540-75563-0_26)
- Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science & Information Technology*, 6.
- Ellis, T. J., & Levy, Y. (2012). Data sources for scholarly research: towards a guide for novice researchers. *Proceedings of Informing Science & IT Education Conference*. Retrieved from <http://proceedings.informingscience.org/InSITE2012/InSITE12p405-416Ellis0114.pdf>
- Eloff, J. H. P., Labuschagne, L., & Badenhorst, K. P. (1993). A comparative framework for risk analysis methods. *Computers & Security*, 12, 597-603.
- Falkner, E. M., & Hiebl, M. R. (2015). Risk management in SMEs: A systematic review of available evidence. *The Journal of Risk Finance*, 16(2), 122-144.
- Faul, F., Erdfelder, E., Buchner, A., & Lang, A. G. (2009). Statistical power analyses using G\* Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, 41(4), 1149-1160.
- Feng, N., & Li, M. (2011). An information systems security risk assessment model under uncertain environment. *Applied Soft Computing*, 11(7), 4332-4340.
- Fitzgerald, T. (2007). Clarifying the roles of information security: 13 questions the CEO, CIO, and CISO must ask each other. *Information Systems Security*, 16(5), 257-263.
- Florêncio, D., & Herley, C. (2013). Sex, lies and cyber-crime surveys. *Economics of Information Security and Privacy III*, 35-53.



- 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.
- Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security, 59*, 26-44.
- Furnell, S., & Thomson, K. L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud & Security, 2009(2)*, 5-10.
- Garson, G. D. (2012). *Testing statistical assumptions*. Asheboro, NC: Statistical Associates Publishing.
- Georg, L. (2017). Information security governance: Pending legal responsibilities of non-executive boards. *Journal of Management & Governance, 21(4)*, 793-814.
- Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management, 46(7)*, 404-410.
- Goode, S., & Lacey, D. (2011). Detecting complex account fraud in the enterprise: The role of technical and nontechnical controls. *Decision Support Systems, 50(4)*, 702-714.
- Gravetter, F. J., & Wallnau, L. B. (2009). *Statistics for the behavioral sciences: Eighth edition*. Belmont, CA: Wadsworth Cengage Learning.
- Green, D., & Hanbury, M. (2019). If you bought anything from these 12 companies in the last year, your data may have been stolen. *Business Insider*. Retrieved from <https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1>
- Groysberg, B., Kelly, L. K., & MacDonald, B. (2011). The new path to the C-suite. *Harvard Business Review, 89(3)*, 60-68.
- Guhr, N., Lebek, B., & Breitner, M. H. (2019). The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. *Information Systems Journal, 29(2)*, 340-362.
- Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Thousand Oaks, CA: Sage Publications.

- Halliday, S., Badenhorst, K., & Von Solms, R. (1996). A business approach to effective information technology risk analysis and management. *Information Management & Computer Security*, 4(1), 19-31.
- Hann, I. H., Hui, K. L., Lee, S. Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems*, 24(2), 13-42.
- Haqaf, H., & Koyuncu, M. (2018). Understanding key skills for information security managers. *International Journal of Information Management*, 43, 165-172.
- Hardekopf, B. (2015). Data breaches of 2014. *Forbes*. Retrieved from <http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/>
- Hazari, S., Hargrave, W., & Clenney, B. (2008). An empirical investigation of factors influencing information security behavior. *Journal of Information Privacy and Security*, 4(4), 3-20.
- Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165.
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106-125.
- Hinkin, T. R. (1998). A brief tutorial on the development of measures for use in survey questionnaires. *Organizational Research Methods*, 1(1), 104-121.
- Hollander, E. P., & Offermann, L. R. (1990). Power and leadership in organizations: Relationships in transition. *American Psychologist*, 45(2), 179.
- Holloway, J. B. (2012). Leadership Behavior and organizational climate: An empirical study in a non-profit organization. *Emerging Leadership Journeys*, 5(1), 9-35.
- Hooper, D., Coughlan, J., Mullen, M. (2008). Structural equation modelling: Guidelines for determining model fit. *Electronic Journal of Business Research Methods*, 6(1), 53-60.
- Horenbeeck, M. (2017). The key to better cybersecurity: Keep employee rules simple. *Harvard Business Review*. Retrieved from <https://hbr.org/2017/11/the-key-to-better-cybersecurity-keep-employee-rules-simple>
- Höne, K., & Eloff, J. H. P. (2002). Information security policy—what do international information security standards say?. *Computers & Security*, 21(5), 402-409.

- Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security—a neo-institutional perspective. *The Journal of Strategic Information Systems*, 16(2), 153-172.
- Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees?. *Communications of the ACM*, 54(6), 54-60.
- 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.
- Hu, Q., West, R., & Smarandescu, L. (2015). The Role of Self-Control in Information Security Violations: Insights from a Cognitive Neuroscience Perspective. *Journal of Management Information Systems*, 31(4), 6-48.
- Humaidi, N., & Balakrishnan, V. (2015). Leadership Styles and Information Security Compliance Behavior: The mediator effect of information security awareness. *International Journal of Information and Education Technology*, 5(4), 311.
- Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, 51(1), 69-79.
- Imenda, S. (2014). Is there a conceptual difference between theoretical and conceptual frameworks?. *Journal of Social Sciences*, 38(2), 185-195.
- Isaac, R. G., Zerbe, W. J., & Pitt, D. C. (2001). Leadership and motivation: The effective application of expectancy theory. *Journal of Managerial Issues*, 212-226.
- ISO/IEC 27002:2013: Code of practice for information security controls. (2018). Retrieved from <http://www.iso27001security.com/html/27002.html>
- Johnson, M. E., & Goetz, E. (2007). Embedding information security into the organization. *IEEE Security & Privacy*, (3), 16-24.
- Johnson, M. E., Goetz, E., & Pfleeger, S. L. (2009). Security through information risk management. *IEEE Security & Privacy*, 7(3), 45-52.
- Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, 52(1), 126-129.
- Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549-566.

- Johnston, A. C., Warkentin, M., & Siponen, M. T. (2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric. *MIS Quarterly*, 39(1), 113-134.
- Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, 25(3), 231-251.
- Karabacak, B., & Sogukpinar, I. (2004). ISRAM: information security risk analysis method. *Computers & Security*, 24(2), 147-159.
- Knapp, K. J., & Ferrante, C. J. (2012). Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations. *Journal of Management Policy and Practice*, 13(5), 66-80.
- Knapp, K. J., Marshall, T. E., Kelly Rainer, R., & Nelson Ford, F. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security*, 14(1), 24-36.
- Kokolakis, S. A., Demopoulos, A. J., & Kiountouzis, E. A. (2000). The use of business process modelling in information systems security analysis and design. *Information Management & Computer Security*, 8(3), 107-116.
- Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security*, 33, 3-11.
- Koskosas, I. V., & Asimopoulos, N. (2011). Information system security goals. *International Journal of Advanced Science and Technology*, 27, 15-26.
- Kotter, J. P. (1990). *Force for change: How leadership differs from management*. New York, NY: Simon and Schuster.
- Kutsch, E., Denyer, D., Hall, M., & Lee-Kelley, E. L. (2013). Does risk matter? Disengagement from risk management practices in information systems projects. *European Journal of Information Systems*, 22(6), 637-649.
- Lawshe, C. H. (1975). A quantitative approach to content validity 1. *Personnel Psychology*, 28(4), 563-575.
- Lebek, B., Guhr, N., & Breitner, M. (2014). Transformational Leadership and Employees' Information Security Performance: The Mediating Role of Motivation and Climate. *ICIS 2014 Proceedings*. Retrieved from <http://aisel.aisnet.org/icis2014/proceedings/ISSecurity/21/>
- Lee, A. S., & Baskerville, R. L. (2003). Generalizing generalizability in information systems research. *Information Systems Research*, 14(3), 221-243.

- Lee, C. H., Geng, X., & Raghunathan, S. (2016). Mandatory standards and organizational information security. *Information Systems Research*, 27(1), 70-86.
- Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. *MIS Quarterly*, 59-87.
- Liu, S. H., Liao, H. L., & Zeng, Y. T. (2007). Why people blog: An expectancy theory analysis. *Issues in Information Systems*, 8(2), 232-237.
- Liu, Y., Li, Y., Zhang, H., & Huang, W. W. (2017). Gender differences in information quality of virtual communities: A study from an expectation-perception perspective. *Personality and Individual Differences*, 104, 224-229.
- Longstaff, T. A., Chittister, C., Pethia, R., & Haimes, Y. Y. (2000). Are we forgetting the risks of information technology?. *Computer*, 33(12), 43-51.
- Lyxell, B., Borg, E., & Olsson, I. S. (2009). Cognitive skills and perceived effort in active and passive. *Sound, Mind, and Emotion*, 91.
- Maner, J. K., & Mead, N. L. (2010). The essential tension between leadership and power: when leaders sacrifice group goals for the sake of self-interest. *Journal of Personality and Social Psychology*, 99(3), 482.
- Marques, J. F. (2010). Awakened leaders: born or made?. *Leadership & Organization Development Journal*, 31(4), 307-323.
- Matsui, T., Okada, A., & Mizuguchi, R. (1981). Expectancy theory prediction of the goal theory postulate: The harder the goals, the higher the performance. *Journal of Applied Psychology*, 66(1), 54.
- Mulaik, S. A., James, L. R., Van Alstine, J., Bennett, N., Lind, S., & Stilwell, C. D. (1989). Evaluation of goodness-of-fit indices for structural equation models. *Psychological Bulletin*, 105(3), 430.
- Merhi, M., & Ahluwalia, P. (2015). Top management can lower resistance toward information security compliance. *ICIS 2015 Proceedings*. Retrieved from <http://aisel.aisnet.org/icis2015/proceedings/SecurityIS/3/>
- Mertler, C. & Vannatta, R. (2013). *Advanced and multivariate statistical methods—practical application and interpretation: Fifth edition*. Glendale, CA: Pyrczak Publishing.
- Miller, J., & Doyle, B. A. (1987). Measuring the effectiveness of computer-based information systems in the financial services sector. *MIS Quarterly*, 107-124.

- Milne, G. R., & Bahl, S. (2010). Are there differences between consumers' and marketers' privacy expectations? A segment-and technology-level analysis. *Journal of Public Policy & Marketing*, 29(1), 138-149.
- Momeni, N. (2009). The relation between managers' emotional intelligence and the organizational climate they create. *Public Personnel Management*, 38(2), 35-48.
- Montesino, R., Fenz, S., & Baluja, W. (2012). SIEM-based framework for security controls automation. *Information Management & Computer Security*, 20(4), 248-263.
- Moynihan, D. P., Pandey, S. K., & Wright, B. E. (2012). Setting the table: How transformational leadership fosters performance information use. *Journal of Public Administration Research and Theory*, 22(1), 143-164.
- Munteanu, A. (2006). Information security risk assessment: The qualitative versus quantitative dilemma. *Managing Information in the Digital Economy: Issues & Solutions-Proceedings of the 6th International Business Information Management Association Conference*. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=917767#](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=917767#)
- Myyry, L., Siponen, M., Pahnla, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, 18(2), 126-139.
- Newsted, P. R., Huff, S. L., & Munro, M. C. (1998). Survey instruments in information systems. *MIS Quarterly*, 22(4), 553.
- Northouse, P. G. (2015). *Leadership: Theory and Practice*. Thousand Oaks, CA: Sage publications.
- Northouse, P. G. (2016). *Leadership: Theory and practice*. Thousand Oaks, CA: Sage publications.
- Oladimeji, E. A., Supakkul, S., & Chung, L. (2006). Security threat modeling and analysis: A goal-oriented approach. *Proceedings of the 10th IASTED International Conference on Software Engineering and Applications*. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=917767#](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=917767#)
- Ong, M. H. A., & Puteh, F. (2017). Quantitative data analysis: Choosing between SPSS, PLS and AMOS in social science research. *International Interdisciplinary Journal of Scientific Research*, 3(1), 14-25.

- Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research, 2*(1), 1-28.
- Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security, 31*(5), 673-680.
- Paswan, A. (2009). *Confirmatory factor analysis and structural equations modeling. An introduction*. Department of Marketing and Logistics, COB, University of North Texas, USA.
- Pearlson, K., & Saunders, C. (2013). *Managing & using information systems: A strategic approach*. Danvers, MA: John Wiley & Sons.
- Perloth, N. (2014). A tough corporate job asks one question: Can you hack it?. *New York Times*. Retrieved from [http://www.nytimes.com/2014/07/21/business/a-tough-corporate-job-asks-one-question-can-you-hack-it.html?\\_r=0](http://www.nytimes.com/2014/07/21/business/a-tough-corporate-job-asks-one-question-can-you-hack-it.html?_r=0)
- Pinsonneault, A., & Kraemer, K. (1993). Survey research methodology in management information systems: an assessment. *Journal of Management Information Systems, 10*(2), 75-105.
- Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security, 23*(8), 638-646.
- Rainer Jr, R. K., Snyder, C. A., & Carr, H. H. (1991). Risk analysis for information technology. *Journal of Management Information Systems, 8*(1), 129-147.
- Reinhardt, L., & Wahba, M. A. (1975). Expectancy theory as a predictor of work motivation, effort expenditure, and job performance. *Academy of Management Journal, 18*(3), 520-537.
- Romanow, D., Rai, A., & Keil, M. (2018). CPOE-Enabled Coordination: Appropriation for Deep Structure Use and Impacts on Patient Outcomes. *MIS Quarterly, 42*(1), 189-212.
- Rosemann, M., & Vessey, I. (2008). Toward improving the relevance of information systems research to practice: the role of applicability checks. *MIS Quarterly, 1-22*.
- Ryan, J. J., Mazzuchi, T. A., Ryan, D. J., De la Cruz, J. L., & Cooke, R. (2012). Quantifying information security risks using expert judgment elicitation. *Computers & Operations Research, 39*(4), 774-784.
- Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442-451.

- Safa, N. S., Von Solms, R., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud & Security*, 2016(2), 15-18.
- Safa, N. S., Von Solms, R., & Futcher, L. (2016). Information security policy compliance model in organizations. *Computers & Security*, 2016(56), 70-82.
- Salkind, N. (2012). *Exploring research*. Upper Saddle River, NJ: Pearson Education.
- Salmela, H. (2008). Analysing business losses caused by information systems risk: a business process analysis approach. *Journal of Information Technology*, 23(3), 185-202.
- Schiff, J. (2013). 7 Biggest IT compliance headaches and how CIOs can cure them. *CIO*. Retrieved from <https://www.cio.com/article/2382445/compliance/7-biggest-it-compliance-headaches-and-how-cios-can-cure-them.html>
- Sekaran, U., & Bougie, R. (2013). *Research methods for business: Sixth Edition*. UK: John Wiley & Sons Ltd.
- Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment. *Computers & Security*, 57, 14-30.
- Sharma, R., & Yetton, P. (2003). The contingent effects of management support and task interdependence on successful information systems implementation. *MIS Quarterly*, 533-556.
- Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49, 177-191.
- Singleton, J. P., McLean, E. R., & Altman, E. N. (1988). Measuring information systems performance: experience with the management by results system at Security Pacific Bank. *MIS Quarterly*, 325-337.
- Siponen, M. T., & Kajava, J. (1998). Ontology of organizational IT security awareness- from theoretical foundations to practical framework. *WET ICE 1998 Proceedings*. Retrieved from <http://ieeexplore.ieee.org/document/725713/>
- Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 31-41.
- Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM*, 49(8), 97-100.
- Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 487-



502.

- Siponen, M., Pahlila, S., & Mahmood, M. A. (2010). Compliance with information security policies: an empirical investigation. *Computer*, 43(2), 64-71.
- Skinner, R., Nelson, R. R., Chin, W. W., & Land, L. (2015). The Delphi method research strategy in studies of information systems. *Communications of the Association for Information Systems*, 37, 2.
- Smith, T. A. (2014). Security leadership in a changing healthcare world. *Journal of healthcare protection management: Publication of the International Association for Hospital Security*, 30(1), 1-7.
- Snead, K. C., & Harrell, A. M. (1994). An application of expectancy theory to explain a manager's intention to use a decision support system. *Decision Sciences*, 25(4), 499-510.
- Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, 48(7), 296-302.
- Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215-225.
- Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, 503-522.
- Spurling, P. (1995). Promoting security awareness and commitment. *Information Management & Computer Security*, 3(2), 20-26.
- Stewart, G. W. (1987). Collinearity and least squares regression. *Statistical Science*, 2(1), 68-84.
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, 147-169.
- Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, 13(1), 24.
- Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 441-469.
- Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information systems*, 13(1), 24.

- Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information & Computer Security*, 25(5), 494-534.
- Talib, M. A., El Barachi, M., Khelif, A., & Ormandjieva, O. (2012). Guide to ISO 27001: UAE case study. *Issues in Informing Science and Information Technology*, 7, 331-349.
- Terrell, S. R. (2012). *Statistics translated: A step-by-step guide to analyzing and interpreting data*. New York, NY: The Guildford Press.
- Terrell, S. R. (2015). *Writing a proposal for your dissertation: Guidelines and examples*. New York, NY: The Guildford Press.
- Ullman, J. B., & Bentler, P. M. (2003). *Handbook of Psychology Structural equation modeling: Second Edition*. New York, NY: John Wiley.
- Vaast, E. (2007). Danger is in the eye of the beholders: Social representations of Information Systems security in healthcare. *The Journal of Strategic Information Systems*, 16(2), 130-152.
- Vance, A., Siponen, M., & Pahnla, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, 49(3), 190-198.
- Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, 37(1), 21-54.
- Verhagen, T., Van Den Hooff, B., & Meents, S. (2015). Toward a better use of the semantic differential in IS research: An integrative framework of suggested action. *Journal of the Association for Information Systems*, 16(2), 108.
- Vitale, M. R. (1986). The growing risks of information systems success. *MIS Quarterly*, 327-334.
- Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23(5), 371-376.
- Von Solms, B. (2006). Information security—the fourth wave. *Computers & Security*, 25(3), 165-168.
- Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security—what goes where?. *Information & Computer Security*, 26(1), 2-9.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102.

- Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, 23(3), 191-198.
- Vroom, V. (1964). *Work and motivation*. New York, NY: John Wiley.
- Vroom, V. (1995). *Work and motivation*. New York, NY: John Wiley.
- Wang, H., Tsui, A. S., & Xin, K. R. (2011). CEO leadership behaviors, organizational performance, and employees' attitudes. *The Leadership Quarterly*, 22(1), 92-105.
- Wang, T. S., Lin, Y. M., Werner, E. M., & Chang, H. (2018). The relationship between external financing activities and earnings management: Evidence from enterprise risk management. *International Review of Economics & Finance*, (58) 312-329.
- Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, 18(2), 101.
- Weathersby, G. B. (1999). Leadership vs. management. *Management Review*, 88(3), 5.
- Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, xiii-xxiii.
- Weston, R., & Gore Jr, P. A. (2006). A brief guide to structural equation modeling. *The Counseling Psychologist*, 34(5), 719-751.
- Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM*, 46(8), 91-95.
- Whitten, D. (2008). The chief information security officer: An analysis of the skills required for success. *Journal of Computer Information Systems*, 48(3), 15.
- Willcocks, L., & Margetts, H. (1994). Risk assessment and information systems. *European Journal of Information Systems*, 3(2), 127-138.
- Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization*, 16(4), 304-324.
- Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 37(1), 1-20.
- Wu, H., & Leung, S. O. (2017). Can likert scales be treated as interval scales?—A simulation study. *Journal of Social Service Research*, 43(4), 527-532.

- Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems, 92*, 36-46.
- Yin, D., Bond, S. D., & Zhang, H. (2014). Anxious or angry? Effects of discrete emotions on the perceived helpfulness of online reviews. *MIS Quarterly, 38*(2), 539-560.
- Zainudin, D., Hamid, T., & Ur-Rahman, A. (2016). Leadership by example in e-government security management system. *International Journal of Computer Applications, 144*(4), 10-17.
- Zang, W. L. (2014). Research of information security quantitative evaluation method. *Applied Mechanics and Materials, 513*, 369-372.