

WALL, JEFFREY DAVID, Ph.D. Toward a Behavioral Contingency Theory of Security-related Corruption Control: Understanding Informal Social Controls. (2015)  
Directed by Dr. Prashant Palvia. 240 pp.

Information security is increasingly important to organizations, as security breaches are costly. Organizational insiders can be assets or vulnerabilities in the battle to secure information systems. However, organizational insiders' security beliefs and behaviors are not well understood. In particular, little is known about how social influence affects insiders' security behaviors, yet studies have shown that social influence is shown to be a strong predictor of security behavior. A deeper understanding of social influence is needed in the literature. Additionally, many security studies only examine a cross-sectional period with no concern for changes in beliefs and behaviors over time. Thus, little is known about how learning in previous life periods (e.g., childhood/adolescence and tenure at a previous job) influences insiders' current security beliefs and behaviors.

This study examines the influence that informal information security controls exert on the information security behaviors of organizational insiders. This study also identifies how perceptions of previous social learning experiences influence current security beliefs and behaviors. In particular, this dissertation highlights four security behaviors: security risk-taking behavior and security damaging behavior, and security compliant behavior and proactive security behavior. Through a qualitative study, a model of the effect of social learning on security behavior is developed. A quantitative test is then presented to further confirm the results of the qualitative study. Through the quantitative study, an initial exploration of social learning across national boundaries is also provided. The study also

concerns itself with understanding how context influences information security beliefs and behaviors.

TOWARD A BEHAVIORAL CONTINGENCY THEORY OF  
SECURITY-RELATED CORRUPTION CONTROL:  
UNDERSTANDING INFORMAL  
SOCIAL CONTROLS

by

Jeffrey David Wall

A Dissertation Submitted to  
the Faculty of The Graduate School at  
The University of North Carolina at Greensboro  
in Partial Fulfillment  
of the Requirements for the Degree  
Doctor of Philosophy

Greensboro  
2015

Approved by

---

Committee Chair

© 2015 Jeffrey David Wall

To my wife Jennifer Wall for all of her support and encouragement

APPROVAL PAGE

This dissertation written by JEFFREY DAVID WALL has been approved by the following committee of the Faculty of The Graduate School at The University of North Carolina at Greensboro.

Committee Chair \_\_\_\_\_

Committee Members \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
Date of Acceptance by Committee

\_\_\_\_\_  
Date of Final Oral Examination

## TABLE OF CONTENTS

CHAPTER	Page
I. INTRODUCTION .....	1
Overview .....	1
Scope and Unit of Analysis.....	5
Research Direction and Research Questions .....	8
Research Agenda .....	11
II. LITERATURE REVIEW .....	13
Overview of Controls in Behavioral Information Security Research.....	13
Classifications of Information Security Controls .....	14
Typological Theorizing.....	17
Contingency Models .....	20
Developing a Typology of Security-Related Corruption Control.....	23
Structural Systems .....	31
Consequence Systems.....	37
Commitment Systems .....	42
Social Controls in InfoSec Research.....	47
III. THEORETICAL FOUNDATIONS .....	53
Social Structure and Social Process .....	53
Differential Association Theory .....	54
Akers' Social Learning Theory.....	55
IV. CONCEPTUAL MODEL.....	59
Conceptual Overview.....	59
Social Learning .....	60
Contingency Effects.....	63
V. THE QUALITATIVE STUDY .....	66
Research Design.....	66

VI. RESULTS OF THE QUALITATIVE STUDY.....	71
Qualitative Themes and Codes .....	71
Early Rule-Related Beliefs as the Foundation for Current Security	
Beliefs and Behaviors.....	87
Social Learning across Time.....	91
Explaining Differences between Early Rule-Related Beliefs and	
Current Security-Specific Beliefs .....	99
Trust among Coworkers.....	112
Managing Security Behavior .....	114
VII. THE QUANTIATIVE STUDY.....	122
Exploring Social Learning Internationally.....	123
Conceptual Model.....	125
Measures .....	128
Participants.....	131
VIII. RESULTS OF THE QUANTIATIVE STUDY .....	136
Two Stage Analysis Approach.....	137
Assessing the Psychometric Properties of the Higher Order	
Constructs .....	139
Assessing the Psychometric Properties of the Formative Constructs.....	140
Models 1 and 2: Security Assurance Behavior in the US and India.....	143
Models 3 and 4: Security Compliant Behavior in the US and India.....	159
Models 5 and 6: Security Risk-taking Behavior in the US and India.....	175
Models 7 and 8: Security Damaging Behavior in the US and India.....	187
IX. DISCUSSION.....	200
Theoretical Contributions .....	201
Managerial Contributions .....	209
Limitations and Future Research .....	211
X. CONCLUSION.....	214
REFERENCES .....	215
APPENDIX A. CODING OF INFOSEC RESEARCH.....	227

APPENDIX B. INTERVIEW QUESTIONS.....	231
APPENDIX C. SURVEY QUESTIONNAIRE.....	232

# CHAPTER I

## INTRODUCTION

### Overview

Information system security is an increasingly important topic for researchers and practitioners alike, as security breaches are costly to organizations and their clients. In 2012 in the US, data breaches cost organizations nearly \$200 per compromised record, and on average, breached organizations experience approximately 30,000 compromised records per incident (Ponemon, 2013). Major breaches can be even more devastating. For example, a recent security breach at Target, a major US-based retailer, resulted in the compromise of as many as 40 million credit and debit card numbers and upwards of \$18 billion in total damages to banks, retailers, and customers (Harris, Perloth, Popper, & Stout, 2014).

To manage external and internal threats to information systems (IS), organizations implement a variety of security controls. In the context of this study, *security controls* refer to formal and informal mechanisms that influence employees with the intent to protect the organization and its clients from internal and external security breaches. Organizations use three primary forms of security controls to protect IS and informational resources, including: technical controls, management controls, and operational controls (NIST, 2009). *Technical controls* refer to safeguards and countermeasures for

information systems that are executed through technical means, such as software and hardware (e.g., firewalls, anti-virus software, trusted platform module chips) (NIST, 2009). *Management controls* refer to safeguards and countermeasures for information systems designed to manage risk and manage security initiatives, such as vulnerability and risk assessments and security planning (NIST, 2009). *Operational controls*, also called procedural controls, refer to safeguards and countermeasures for information systems that are executed primarily by individuals, such as security education, training, and awareness (SETA) programs and sanctions (NIST, 2009).

Technical controls are heavily studied in IS research; however, management and operational controls are studied far less frequently (Siponen, Willison, & Baskerville, 2008). Although technical controls are necessary to protect IS from external and internal security threats, technical controls may not be sufficient to stop all attacks. Technical controls are particularly weak against threats posed by organizational insiders (Posey, Roberts, Lowry, Bennett, & Courtney, 2013; Warkentin & Willison, 2009; Willison & Warkentin, 2013; Workman & Gathegi, 2007). *Organizational insiders* refer to individuals within an organization, such as full- and part-time employees and board members, who are granted access to IS for legitimate work purposes (Posey et al., 2013). The trust invested in organizational insiders can lead to security breaches instigated by organizational insiders (e.g., stealing confidential records) or to vulnerabilities created by organizational insiders' negligent and careless behaviors (e.g., sharing passwords). Organizations establish operational controls to minimize the potential of security incidents caused by organizational insiders. Operational controls are also used to promote

positive security behavior (Bulgurcu, Cavusoglu, & Benbasat, 2010; Herath & Rao, 2009b).

Although the study of organizational insiders' security behaviors is an increasingly important topic in IS research (Guo, 2013; Posey et al., 2013; Willison & Warkentin, 2013), the body of research is in a nascent state (Crossler et al., 2013; Siponen et al., 2008). Much is still unknown about the way security controls, namely operational controls, influence employees' security behaviors. In particular, research about organizational insiders' risky and damaging security behaviors is underdeveloped (Guo, 2013; Guo, Yuan, Archer, & Connelly, 2011; Willison & Warkentin, 2013). Much more is known about positive security behavior (i.e., information security policy compliance). Understanding how controls influence organizational insiders' security behaviors can assist managers and security professionals in their efforts to improve existing security controls and develop new security controls to prevent internal threats to IS and maximize proactive security behavior. Thus, to extend existing knowledge of security behavior, this study seeks to understand how security controls, namely operational controls, influence organizational insiders security behaviors.

In this study, organizational insiders' deviant behavior is conceptualized according to the four types of behaviors identified by Guo (2013). The four types of behaviors include security assurance behaviors, hereafter referred to as proactive security behavior, security compliant behavior, security risk-taking behavior, and security damaging behavior. *Security assurance behavior* or *proactive security behavior* (PSB), refers to proactive, directed actions taken by an employee with the intent of protecting

organizational information. Proactive security behaviors go beyond requirements in information security policy (Guo, 2013; Workman, Bommer, & Straub, 2008). *Security compliant behavior* (SCB) refers to actions taken to comply with information security policy. Security compliant behavior is refraining from breaking protocols and procedures (Guo, 2013). *Security risk-taking behavior* (SRB) refers to intentional violations of organizational information security policies (ISP) that create vulnerabilities in IS, but do not directly cause harm to the organization (Guo, 2013). Examples of SRB include: logging onto insecure networks with organization information technology (IT), writing down passwords, sharing passwords, and inserting personal USB drives into organizational IT. *Security damaging behavior* (SDB) refers to intentional and malicious actions committed by organizational insiders that cause direct damage to the organization (Guo, 2013). Examples of SDB behaviors include: password cracking, data theft, intentional destruction of computer equipment, and intentional deletion of crucial data.

The body of literature pertaining to the study of organizational insiders' security behaviors is generally referred to as behavioral information security (InfoSec) research (Crossler et al., 2013). This study seeks to assess existing behavioral InfoSec research on organizational insiders' security behaviors to identify important directions for future research and to study some of these directions. To identify an area of behavioral InfoSec research that needs further study, a review of the research on organizational insiders' security behaviors was conducted.

Although positive compliant security behaviors have been studied more extensively, negative security behaviors have not. Thus, a typology of organizational

corruption controls was used and adapted (Lange, 2008) to classify the operational security controls currently studied in behavioral InfoSec research in relation to negative security behavior. *Organizational corruption controls* are operational controls in organizations that seek to minimize intentional misbehavior by employees (Lange, 2008). Corruption controls and organizational controls, controls that seek to maximize cooperation and efficiency in work processes (Cardinal, 2001; Lange, 2008), work together to minimize negative behavior and maximize positive security behavior. Given our focus on operational controls, Lange's typology of corruption controls provides a useful classification tool for the review. Operational security controls are conceptualized herein as security-related corruption controls. This study also examines operational controls designed to encourage positive security behaviors, such as ISP compliance. Positive and negative security behaviors are not simply two sides of the same coin (Guo, 2013). Similarly, the operational controls used to promote compliant security behavior are not the same as those used to deter noncompliant behavior (D'Arcy & Herath, 2011; Willison & Warkentin, 2013). Security-related corruption controls are a subset of the broader class of organizational corruption controls. Thus, *security-related corruption controls* are formal and informal operational interventions that seek to minimize negative security behavior.

### **Scope and Unit of Analysis**

This paper seeks to understand the influence security-related corruption controls and controls that promote positive security behavior exert on organizational insiders' security behaviors. Thus, the study is scoped to operational controls and individual

behavior. The unit of analysis in this study is at the individual-level. The choice to scope the study to operational controls and individual behavior is made for several reasons. First, technical security controls receive ample research attention, while operational controls are understudied (Siponen et al., 2008). Second, research on operational controls is in a nascent state (Crossler et al., 2013; Siponen et al., 2008). Much is still unknown about how operational controls influence security behavior. Third, our research focus is employee behavior, which is typically studied from the perspective of operational controls (e.g., Crossler et al., 2013; D'Arcy, Hovav, & Galletta, 2009; Puhakainen & Siponen, 2010; Siponen & Vance, 2010; Vance & Siponen, 2012). Management controls are frequently examined at the organizational level because management controls focus on organization-wide security requirements, plans, and assessments. Finally, research on SDB's and SRB's is underdeveloped (Guo, 2013; Guo et al., 2011; Warkentin, Straub, & Malimage, 2012; Willison & Warkentin, 2013). A single violation by an organizational insider can cause severe damage to an organization. Thus, understanding individual behavior is a crucial endeavor in behavioral InfoSec research. Conversely, organizational insiders' positive security behaviors can minimize threats to IS (Bulgurcu et al., 2010; Herath & Rao, 2009b).

This study also adopts a contingency perspective to study security-related corruption controls. Contingency theories seek to understand how phenomena operate in different contexts and under different constraints. The contingency perspective works under the assumption that context is a crucial predictor of how phenomena are manifested. Contingency theories can be conceptualized in many different ways, such as

through mediation, moderation, and profile deviation (Baron & Kenny, 1986; Venkatraman, 1989).

Based on our review of the behavioral InfoSec research, most security studies about organizational insiders rely on mediation to explain security behavior. Mediated models explain average levels of a phenomenon across a variety of situations and circumstances (Baron & Kenny, 1986). In this way, mediation lacks specificity in predictions and explanations (Venkatraman, 1989). In a security context, this suggests that most of the behavioral InfoSec research explains and predicts the average relationship between key independent and mediating variables and organizational insiders' security behaviors. Thus, most security research is unable to provide a nuanced view of how security behaviors differ in different contexts. For example, few studies examine how interactions between security controls influence organizational insiders' security behaviors (Chen & Wen, 2012) or how context influences the effectiveness of security controls (D'Arcy & Herath, 2011). Yet, such research is necessary to assist managers in developing appropriate portfolios of security controls for their particular organizational contexts. Thus, different contingency perspectives, such as moderation and profile deviation, are needed to extend explanations of security behavior to particular contexts. Using other means of exploring contingencies, such as profile deviation and moderation, allow researchers to explain optimal levels of a phenomenon for different situations and circumstances (Barki, Rivard, & Talbot, 2001; Baron & Kenny, 1986; Mintzberg, 1979, 1983; Venkatraman, 1989).

Developing a contingency theory of the influence of security controls on security behaviors that accounts for context could assist researchers and practitioners in developing security controls suited for specific environments and employees. Further, contingency models, namely models with moderation, allow researchers to examine how controls interact to influence security behavior (Lange, 2008). Appropriate combinations of controls can maximize the effectiveness of control, while inappropriate combinations may diminish the effectiveness of control (Chen & Wen, 2012; Lange, 2008). Thus, this study adopts a contingency perspective to examine the influence that combinations of security controls exert on organizational insiders' security behaviors in different contexts.

### **Research Direction and Research Questions**

Studying the effects that operational security controls exert on security behaviors in different organizational contexts is a broad topic. Some narrowing of the topic is necessary to make the project manageable. As depicted in Appendix A, the behavioral influence of many types of security controls has been examined in the literature, particularly sanctions and training. However, many important forms of control have received little attention. Based on our literature review, informal social controls have received little attention. Yet, in criminology and sociology, informal social controls are shown to exert a strong influence on behavior (R L Akers, 1985; Ronald L. Akers, 2009; Krohn, Skinner, Massey, & Akers, 1985). Thus, it is important to understand the influence of informal social controls in a security context. *Informal social controls* refer to operational controls that are transmitted socially or culturally rather than through formal administrative channels (Lange, 2008). The literature suggests that informal social

controls (e.g., norms, social sanctions, social learning) are represented by a few simple constructs and that few prominent theories of social control are employed in the literature. Research on informal social controls is absent from research on both positive and negative security behaviors. Thus, this study explores how informal social controls influence organizational insiders' security behaviors. This paper also examines how informal social controls influence the development and effectiveness of formal administrative controls by relying on a contingency perspective.

Other avenues of research are possible. The literature review identified multiple directions for future research; however, to develop a manageable project, the project was scoped to informal social controls. The other avenues for research will be study in other projects. Similarly, only a few contingency factors were selected for examination; however, such choices are necessary to maintain the parsimony of the model presented herein.

To study informal social controls in relation to security behavior, this study draws from the theoretical perspectives of Akers' social learning theory (R L Akers, 1985; Ronald L. Akers, 2009). Akers' social learning theory (ASLT) is a sociological theory in criminology that explains how individuals learn deviant values and behaviors through social interaction. ASLT counters early criminological research, which provided biological explanations of deviant behavior. Similarly, ASLT provides different insight than cognition-based theories of deviant behavior, such as rational choice theory. While cognitive-based theories examine individual's cognitions, ASLT describes how those cognitions are formed and influenced by social interaction. ASLT remains a prominent

theory of social corruption control (Ronald L. Akers, 2009). Although ASLT is used as a guiding theory, other theories were also considered, such as Bandura's social learning theory, rational choice theory, and deterrence theory. Other concepts arose from the qualitative interviews conducted for this study.

ASLT is an extension of Sutherland's differential association theory (Sutherland, 1947). ASLT and differential association theory (DAT) posit that individuals learn to be deviant in the same manner that they learn compliant behavior. ASLT and DAT argue that individuals who have more contact with norms and beliefs that favor deviance will be more likely to engage in deviant behavior. While DAT suggests that behaviors are learned, ASLT explicates important learning mechanisms that influence the social learning of norms and behaviors (Ronald L. Akers, 2009). ASLT is a general theory of deviance, meaning it can explain multiple forms of deviant behavior (Ronald L. Akers, 2009; Pratt et al., 2010). ASLT can explain intentional behaviors with malicious or neutral motives, such as interpersonal violence or smoking, respectively (Pratt et al., 2010). As such, ASLT provides an ideal theoretical perspective for our study of SDB and SRB in the security domain. ASLT is also based on the assumption that deviant behaviors form similar to compliant behaviors (Ronald L. Akers, 2009). Thus, ASLT may provide a lens for examining proactive and compliant security behavior as well.

ASLT is founded on a few key variables. ASLT suggests that individuals will have different levels of exposure to definitions in favor of deviance or in favor of compliance. In ASLT, *definitions* refer to beliefs, values, and rationalizations that are learned by individuals which either favor compliant behavior or favor deviant behavior

(R L Akers, 1985; Sutherland, 1947). Definitions can be general, such as definitions of deviance, or specific, such as definitions of appropriate security behavior (Ronald L. Akers, 2009). Thus, specific definitions should be explored for each research context. The differential exposure to definitions in favor of deviant behavior, known as *differential association*, influences the likelihood that an individual will adopt the definitions and engage in deviant behavior. ASLT proposes two primary mechanisms through which the behavior is learned and reinforced. First, ASLT proposes that behavior is learned through mimicry. Second, ALST suggests that definitions and behaviors are reinforced through mechanisms, such as punishment and rewards that incentivize or disincentivize certain behaviors. Though ALST makes no differentiation between informal reinforcement (e.g., social shaming) and formal reinforcement (e.g., administrative sanctions), this study examines both informal and formal reinforcement.

The research questions explored herein are founded on the premises of ASLT.

The questions are:

- 1) How do informal social processes influence security behaviors in the workplace?
- 2) What general and security-specific definitions of deviance and compliance exist among employees in organizational settings?
- 3) Where do employee's security beliefs originate?

### **Research Agenda**

The remainder of this study proceeds as follows. First, a literature review is provided to discuss the typology and contingency perspective adopted herein. Second, the

theoretical foundations of the dissertation are described in greater detail. Third, a conceptual model and hypotheses are presented. Fourth, the methods that will be used to test the conceptual model are explained. Finally, a discussion of the potential contributions of the dissertation is provided.

## **CHAPTER II**

### **LITERATURE REVIEW**

#### **Overview of Controls in Behavioral Information Security Research**

A review of the literature suggests that security controls play a secondary role in many behavioral InfoSec studies. Many studies seek to explain why individuals commit deviant security-related behaviors, but fail to actively study the characteristics of security controls that help to mitigate the deviant behaviors. For example, some studies examine employees' psychological or moral predispositions in a security context (e.g., D'Arcy & Devaraj, 2012; Myyry, Siponen, Pahlila, Vartiainen, & Vance, 2009). Other studies measure the potential behavioral outcomes of security controls while ignoring characteristics of the controls themselves. Bulgurcu et al. (2010), for example, measures the effect that information security awareness has on compliance intentions and discusses the role that security education, training, and awareness (SETA) programs have in developing security awareness. However, the study does not measure or control for the use of SETA programs in the organizations sampled. Similarly, Herath and Rao (2009b) examines concerns about security breaches using protection-motivation theory and discusses the role that fear appeals have in prompting protective behavior. Again, the study does not measure or control for the use of fear appeals in the organizations sampled. Further, many studies examine security-related social norms (e.g., Bulgurcu et al., 2010; Gagne & Deci, 2005; Guo et al., 2011; Herath & Rao, 2009b);

however, very little empirical work has examined ways that organizations can harness these security-related norms to influence employee behavior. We call for a more intimate study of the characteristics of security controls. In response to these findings, this study provides a more intimate examination of informal social controls herein.

### **Classifications of Information Security Controls**

A number of scholars have classified information security controls for different purposes and from different perspectives. The simplest distinction between security controls is the difference between technical and operational controls (Hovav & D'Arcy, 2012). Technical controls are computerized countermeasures (e.g., firewalls, anti-virus software, intrusion detection systems, computer monitoring, etc.) that detect and/or stop harmful computer behaviors committed by organizational insiders and those external to the organization. However, technical controls are often not enough to stop abuse from organizational insiders, as insiders have greater access to information and computer systems (Ng, Kankanhalli, & Xu, 2009; Siponen et al., 2008; Warkentin & Willison, 2009; Workman & Gathegi, 2007). To further combat internal abuse, organizations develop and deploy operational controls. Operational controls are interventions (security policies, sanctions, rewards, security training, etc.) that attempt to motivate appropriate or discourage inappropriate behavior from employees. Given that distinctions between technical and operational controls are well defined (Hovav & D'Arcy, 2012; Warkentin & Willison, 2009), and technical controls are well studied (Warkentin & Willison, 2009; Zafar & Clark, 2009), this study focuses on distinctions between different types of operational controls.

Some typologies of security controls focus on temporal aspects of control (D. Straub & Welke, 1998; Willison & Warkentin, 2013). Most recently, Willison and Warkentin (2013) adapted Straub and Welke's (1998) security action cycle. Straub and Welke's (1998) security action cycle suggests that organizations first attempt to deter abusive behavior. When deterrence fails, organizations attempt to prevent abusive behavior. If abuse occurs despite attempts to deter and prevent it, organizations attempt to detect and then remedy the abuse. Willison and Warkentin (2013) extended the security action cycle by pointing to the importance of understanding the thought processes and events that lead individuals to engage or intend to engage in abusive behavior. These action cycles offer a useful view of the temporal nature of control. However, they do not capture the characteristics of controls that catalyze security behavior. Organizational controls are established to catalyze specific reactions in employees (e.g., fear, commitment, shame, etc.). To effectively link controls to employee behavior, researchers must understand the behavioral catalyzing characteristics of controls (Lange, 2008).

Some attempts have been made to develop simple typologies of the behavioral catalyzing characteristics of controls. However, these attempts are not the sole focus of the papers; therefore, they are underdeveloped and piecemeal. Chen et al. (2012), for example, provide a distinction between two types of controls—coercive and remunerative controls. Coercive controls include threats and punishments, while remunerative controls are reward systems (e.g., bonuses, praise, recognition, etc.). The distinction between punishment and reward is important and has been studied in many security studies (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Bulgurcu et al., 2010; Chen & Wen, 2012).

At their core, however, punishment and rewards are different forms of consequence systems (Lange, 2008). Consequence systems seek to extrinsically motivate behavior through deterrence or by aligning employees' behaviors with organizational objectives through rewards. Though consequence systems are important, other systems of behavioral control exist within organizations.

Others have studied the distinction between formal and informal controls or administrative and social controls. Administrative controls are established by formal entities within organizations and include formal consequence systems and bureaucratic systems of rules, policies, procedures, and training. Social controls are less formal and may be emergent or manipulated by the organization (Johnson & Gill, 1993; Lange, 2008). In information security research, the distinction between formal and informal control systems is mostly studied as the difference between formal policies and social norms (Herath & Rao, 2009b; Warkentin, Johnston, & Shropshire, 2011) and the difference between formal sanctions and informal sanctions (D'Arcy & Devaraj, 2012; Siponen & Vance, 2010; Vance & Siponen, 2012). As evident in our review, studies of social control systems are highly understudied in information security research and are not well understood. Social control is an important form of control that is becoming more prevalent in postbureaucratic organizations (Lange, 2008; Tompkins & Cheney, 1985). Understanding social control will be an important endeavor for future information security research. Clearly, progress has been made in understanding important characteristics of security controls. However, understanding is currently dispersed across

studies. This study provides a typology that brings together important behavioral catalyzing characteristics of controls to provide a single and holistic reference point.

### **Typological Theorizing**

Typologies are common in research. However, some confusion and contention exists around the value of typologies. To some, typologies are simple classification mechanisms that reduce a complex phenomenon into ideal types of the phenomenon (Doty & Glick, 1994; Posey et al., 2013). In this way, classification systems help researchers to identify a particular entity or phenomenon and compare it to other entities or phenomena (Posey et al., 2013). However, typologies can be used for more than classification; typologies can be used to theorize about phenomena (Doty & Glick, 1994; Hollenbeck, Beersma, & Schouten, 2012). Typological theories capture the effect that types of an entity exert on a dependent variable. For example, we are concerned with the effect that types of security-related corruption controls exert on organizational insiders' security behaviors, particularly SDB and SRB. We are also concerned with how security-related corruption controls interact with controls that promote compliant and proactive behavior. Thus, typological theorizing moves beyond classification to making theoretical statements about ideal types and their underlying dimensions.

Typological theorizing provides different ways to conceptualize the relationships between ideal types and the dependent variable (Doty & Glick, 1994). A common form of typological theorizing suggests that influence on the dependent variable will be greater to the extent that the characteristics of an actual object or phenomenon align with the theoretical dimensions of an ideal type. This is known as profile deviation (Barki et al.,

2001; Venkatraman, 1989). Under profile deviation, a security-related corruption control is most effective to the extent that the actual control aligns perfectly with a profile of an ideal control type. Deviations in levels of the dimensions of an actual object or phenomenon as compared to the dimensions specified for an ideal type decrease the effectiveness of the object or phenomenon. Profile deviation is useful because it explains complex, non-linear relationships (Barki et al., 2001; Doty & Glick, 1994). Profile deviation is used to examine individual instances of an object and its fit with an ideal type. Profile deviation could assist researchers in understanding the effectiveness of a particular control given a particular contingency factor. However, controls do not exist in isolation. Organizations use multiple controls to manage security behavior. Profile deviation is less than ideal for studying sets of controls unless higher-level entities are established to represent ideal types of control sets. Unfortunately, establishing profiles for sets of controls from a behavioral perspective is difficult, because little is known about how controls interact to influence individual behavior (Chen & Wen, 2012; Lange, 2008). Thus, in our agenda, profile deviation is only recommended for the study of individual types of control. To understand the coexistence of controls and optimal control sets, another type of theorizing is necessary, namely moderation.

Moderation in typological theorizing examines the effect that contingency factors have on the relationship between ideal types and the dependent variable (Doty & Glick, 1994). Moderation allows researchers to understand phenomenon at a level of specificity that mediation and profile deviation cannot (Venkatraman, 1989). Because so little information exists regarding the interaction between controls, this study is primarily

concerned with typological theorizing using moderation. Moderation in contingency-based typological theorizing seeks to understand which ideal types should be actualized to maximize the level of the dependent variable (Doty & Glick, 1994). In developing the typology, we seek to examine how contingency factors within the organizational environment influence the behavioral catalyzing effectiveness of security-related corruption controls and controls that promote positive security behavior in order to recommend appropriate controls for different situations and circumstances.

Typological theories can also be specified conceptually or empirically. Conceptual specification of ideal types is best for developing theories (Doty & Glick, 1994). Empirical specification of ideal types is prone to weaknesses that limit theorizing. First, empirical specification of ideal types is usually based on a single study to identify ideal types. Although the ideal types are grounded in practice, the theory is contextualized to the sample, as in grounded theory (Doty & Glick, 1994). There is no guarantee that the typology is representative or robust, though random selection may provide a more representative sample. Conceptual specification of ideal types, however, relies on results from multiple studies and experts. Thus, conceptual specification benefits from a multitude of perspectives and years of theoretical development and testing. Second, empirically specified typologies are limited to the ideal types that exist within practice (Doty & Glick, 1994). Conceptual specification, however, allows researchers to identify ideal types that may not exist within practice, but are theoretically possible. In this way, conceptual specification is amenable to design science and the development of new types of an object. Because our paper our purpose is to provide

direction to develop a theory of security-related corruption control, the investigation relies on conceptual specification to identify ideal types. This study draws from years of research on organizational controls to develop a typology of security-related corruption controls. This is done because SRB and SDB are understudied. Much more is known about controls to enhance positive security behavior. Although the typology is primarily concerned with categorizing security-related corruption controls, the dimensions of the controls also pertain to organizational controls that seeks to promote positive behavior.

### **Contingency Models**

Contingency models seek to explain how phenomena manifest differently in different contexts. In contingency models, context is represented by contingency factors. Contingency factors are aspects of the context that are likely to influence actors' thoughts, attitudes, and behaviors. Some common contingency factors include organizational size, national culture, and organizational culture. The literature review suggests that contingency models are primarily represented as mediation models in behavioral InfoSec research. However, we are not the first to examine or promote moderation-based contingency models in a security setting. First, several behavioral InfoSec studies examine the influence of contingency factors on relationships between different types of perceptions about security phenomenon. For example, Leonard et al. (2004) examine employees' attitudes toward ethical behaviors and employees' intentions to behave ethically or unethically. They examine the moderating effect that the perceived importance of an ethical issue has on the relationship between attitude and behavioral intentions. Similarly, Li et al. (2010) study how employees' perceptions of the risk of

violating Internet use policy influence policy compliance intentions. They find that personal norms moderate the relationship between perceptions of risk and compliance intentions. Ng et al. (2009) examine the influence employees' beliefs about security threats exert on computer security behavior. They find that the perceived severity of a security breach moderates the relationship between threat beliefs and security behavior. These studies explain how employee perceptions interact; however, they do not provide direction toward a contingency theory that links characteristics of controls with employee behavior.

Second, some studies examine the influence of contingency factors on the use of controls by managers. For example, Straub and Nance (1990) examine how managers adjust the certainty and severity of sanctions based on contingency factors such as organizational size and industry. They find that managers use controls differently in different contexts. These types of studies provide useful insight into the application of controls. However, behavior is not directly measured in these types of studies, meaning that researchers cannot suggest controls that maximize the behavioral catalyzing effectiveness of the controls for different contexts.

Finally, some studies examine the influence of contingency factors on the relationship between the use of controls and employee behavior. Hovav and D'Arcy (2012), for example, examines the effect technical and procedural security controls have on information systems (IS) misuse intentions. They find that national culture moderates the relationship between security controls and IS misuse intentions. Similarly, Harrington (1996) examines the use of codes of ethics on computer abuse intentions. She found that

employees' denial of responsibility moderates the relationship between the use of codes of ethics and computer abuse intentions. Chen et al. (2012) examines the effect of punishment and reward on compliance intentions. They find that perceptions of the certainty of control moderate the relationship between punishment and reward and compliance intentions. They also offer a unique perspective of control by examining the behavioral catalyzing effectiveness of two types of controls when the controls coexist in a single environment. Thus, Harrington and Chen et al. are exemplar studies for those interested in developing contingency models in security contexts. Though Harrington and Chen et al. provide exemplar studies, a systematic agenda to arrive at a contingency theory doesn't exist. This paper provides an agenda to arrive at such as theory.

Another concern that arises in contingency models is how to examine contingency factors. Examining the influence of contingencies can be done quantitatively or qualitatively. Both quantitative and qualitative research allow for the comparison of phenomenon across situations. In quantitative research, comparisons can be made by examining the relative frequency of phenomena (e.g., D. W. J. Straub & Nance, 1990), introducing interaction terms in statistical analyses (e.g., Chen & Wen, 2012), and statically comparing identical structural equation models differentiated by a contingency factor (e.g., Hovav & D'Arcy, 2012). In qualitative studies, theoretical replication in the selection of cases allows for the comparison of phenomena based on conceptual criteria (Yin, 2002). Although many methods exist for examining contingency factors, the figures in this study depict traditional models of moderation (Baron & Kenny, 1986) to simplify the presentation of our ideas.

## **Developing a Typology of Security-Related Corruption Control**

This study has identified several ways security controls have been classified. Although each classification offers useful information about how controls influence behavior, behavioral catalyzing aspects of controls are not directly specified in these classifications. Without a clear conceptual link between employee behavior and characteristics of controls that catalyze employee behavior, it is difficult to develop controls that maximize behavioral outcomes (Lange, 2008). Thus, behavioral InfoSec research is in need of a typology grounded in control characteristics that are directly related to employee behavior. Such a typology could provide direction for the improvement and development of new security-related corruption controls.

To develop a typology of security-related corruption control, we first conducted a search of general management literature to find articles on organizational control. In particular, the search was focused on typologies of control. The search consisted of the terms: “typology,” “taxonomy,” “review,” and “organizational control.” Typology and taxonomy were included, as these terms are often used interchangeably (Doty & Glick, 1994). Although several papers were found, only one paper focused on corruption controls (Lange, 2008). Lange’s paper provided us with an initial set of dimensions that are not well explicated in information security research. After selecting Lange’s typology as a foundation, behavioral information security research was collected and an initial coding of the articles was conducted to determine how well the different dimensions of Lange’s typology fit within the security domain.

The article collection process began by searching the basket-11 journals identified by Clark et al. (2011). These journals are identified as high quality mainstream IS journals. Terms such as: “computer abuse,” “policy violation,” “security,” and “information security policy,” “noncompliance” and “compliance” were used. Although the focus of the typology is negative security behavior (i.e., SDB’s and SRB’s), literature that examined compliance was also examined, as many of these studies discuss noncompliance as well. After reviewing and coding the articles found in the basket-11 journals, the first author examined the references in the articles found in the basket-11 journals. This review of references was limited to papers that focused on deviant security behavior. The literature search was extended because research on noncompliance and computer abuse is less prevalent in the basket-11 journals than research on compliance. Only empirical studies were examined in the review. Theoretical papers were reviewed for insight, but were not coded. Empirical papers were coded to ensure that the results represent the research that is well-supported with evidence. Theoretical works require empirical testing to ensure that the underlying concepts are sound. In total, 35 articles were coded. The first author coded each of the articles according to the types of controls that were present in the articles. The coding represents a conservative estimate, and likely overestimates the study of each type of control. Most of the studies treat controls as a secondary concern and do not directly measure different characteristics of controls.

After an initial reading of the literature, it was determined that some of the assumptions in Lange’s typology were not sufficiently nuanced to capture security-related misbehavior. Thus, some revisions were made to the typology. After revising the

typology the lead author coded the articles again to determine what types of security-related corruption controls have been examined in the literature. We now present Lange's typology and discuss the changes made to the typology.

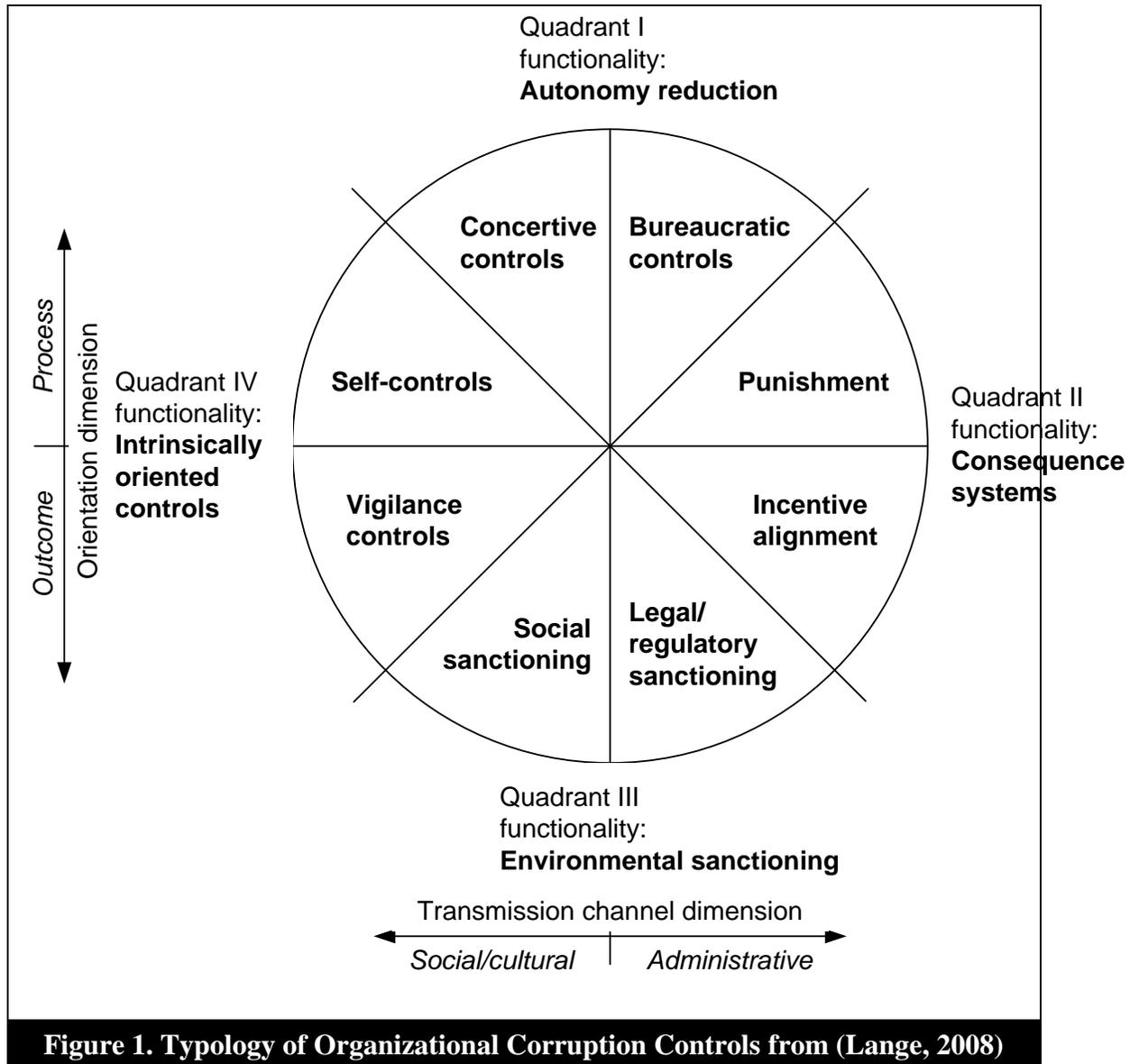
### ***Lange's Typology of Corruption Control***

Lange (2008) suggests that corruption controls should be examined across two dimensions—the behavioral orientation of the control and the transmission channel of the control. Behavioral orientation can be outcome oriented or process oriented (Lange, 2008; Lehman & Ramanujam, 2009). Outcome oriented controls focus on aligning employee behavior with desired outcomes, while process oriented, also referred to as procedural controls, focus on the antecedent behaviors or cognitions that lead to a particular outcome. *Transmission channel* refers to the structures in the organization through which controls are broadcast and enacted. Transmission channels can be administrative—formal channels established through legitimate organizational structures—or social—informal channels established through social structures. The two dimensions create four types of controls: outcome oriented controls transmitted socially, outcome oriented controls transmitted administratively, procedural controls transmitted socially, and procedural controls transmitted administratively (Lange, 2008).

Lange (2008) further separates corruption control types by their functionality—the way controls regulate behavior. He identifies four major types of functionality—autonomy reduction, consequence systems, environmental sanctioning, and intrinsically oriented controls. By combining the four functionalities with the two dimensions mentioned above, Lange (2008) identifies eight types of corruption control. The controls

consist of: bureaucratic controls, punishment, incentive alignment, legal/regulatory sanctioning, social sanctioning, vigilance controls, self-controls, and concertive controls.

Figure 1 depicts Lange's typology.



### ***Re-envisioning Lange's Typology for Security Controls***

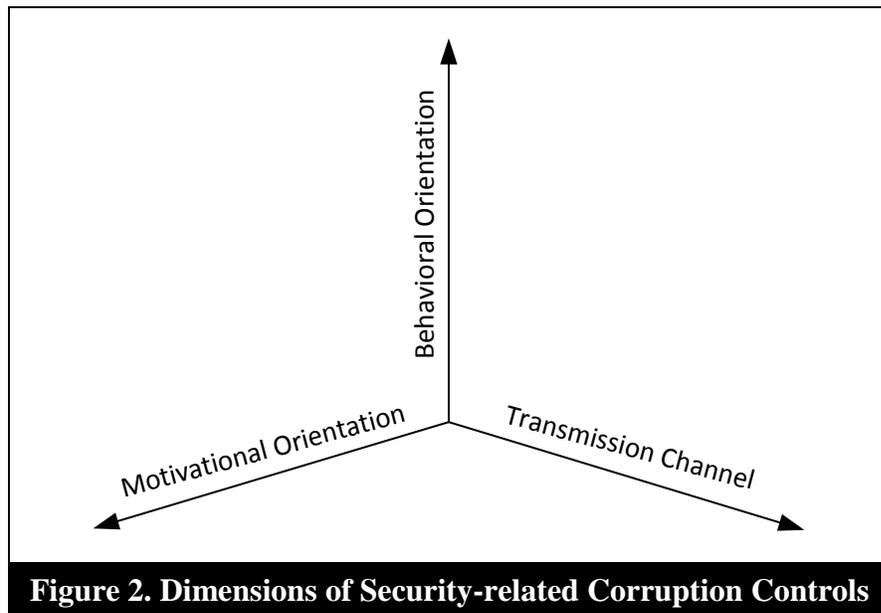
Two aspects of Lange's (2008) typology were questioned for studying corruption controls—the usefulness of functionality as a discriminator of corruption control types and the rigid classification of controls based on the behavioral orientation dimension.

First, functionality as used by Lange (2008) is an inappropriate discriminator for security control types. Environmental sanctioning—the interpretation and transmission of external pressures to organizational insiders (Lange, 2008)—is not at the same level of distinction as the other functionalities. Environmental sanctioning serves the function of reducing autonomy and establishing and executing consequences through external regulating bodies. Further, environmental sanctions are embedded into organizational routines, procedures, and consequence systems through the managerialization of law (Lehman & Ramanujam, 2009). Therefore, environmental sanctioning is subsumed in the autonomy reduction and consequence system functions. That is, environmental sanctioning is a type of autonomy reduction and consequence system. Moreover, the focus of Lange's typology is organizational controls. Environmental sanctioning is the most incongruent with this focus. Finally, organizations rarely report employees' security misbehaviors to external entities (Guo et al., 2011; D. W. J. Straub & Nance, 1990). Further, functionality is further removed from employee behavior than the underlying dimension guiding the functionalities, namely motivation. Each functionality represents different forms of motivation. These limitations warrant the replacing functionality with another dimension.

This paper argues that a third dimension—motivational orientation—better captures the nature of functionality for the security context. Motivation is a common theme in behavioral information security research (e.g., Bulgurcu et al., 2010; Guo et al., 2011; Herath & Rao, 2009b). In fact, compliance intention is often defined as a “motivational state” that occurs prior to engaging in a security behavior (D'Arcy et al., 2009; Hovav & D'Arcy, 2012). Further, motivation figures prominently in theories of behavior and compliance (e.g., Bénabou & Tirole, 2003; Deci, Koestner, & Ryan, 1999; Eisenberger, Pierce, & Cameron, 1999; Frey, 1997; Gagne & Deci, 2005; Ryan & Deci, 1985, 2000; Son, 2011; Vance, Siponen, & Pahlila, 2012; Vroom, 1964). *Motivational orientation* refers to the way in which a control is intended to encourage or discourage employee behavior. The remaining three functionalities in Lange’s typology—consequence systems, intrinsically oriented controls, and autonomy reduction—represent extrinsic, intrinsic and covert motivational orientations, respectively. Corruption controls, such as sanctions and punishment are designed to extrinsically motivate appropriate behavior (Lange, 2008). Some controls are intrinsically oriented (Lange, 2008). Additionally, other controls, such as bureaucratic controls are intended to naturalize behavior, and may be so deeply embedded in the fabric of organizational life that they become invisible and taken for granted (March & Simon, 1958). Therefore, the motivational orientation of these controls is covert. Figure 2 presents the three dimensions of our typology.

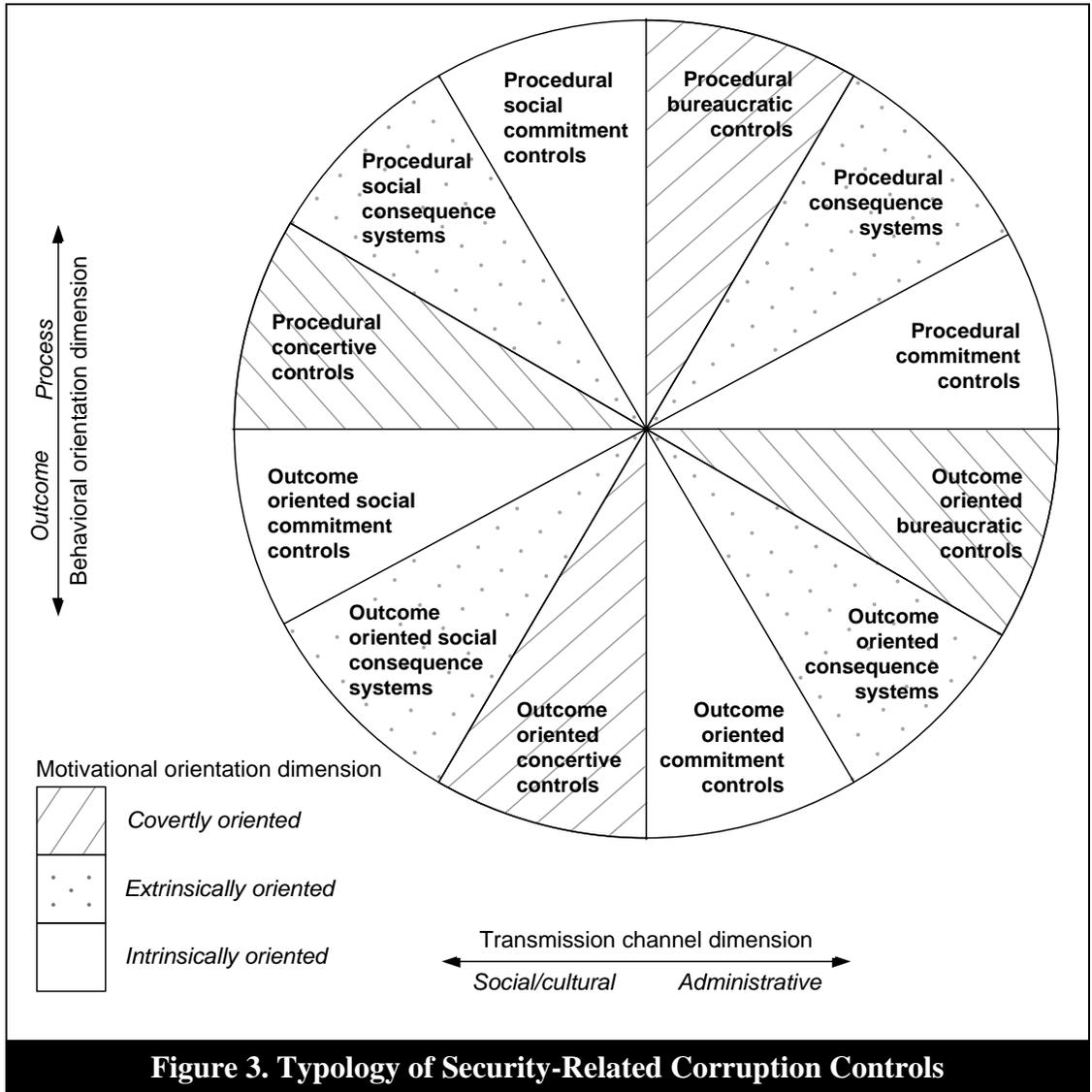
Second, a more nuanced view of outcome oriented and procedural controls is necessary. Important nuances of control are missed by the current typology. For example,

bureaucratic controls are often thought of as being procedural in nature and are represented as such in Lange's typology. However, bureaucratic controls, such as law and policy can be outcome oriented (Lehman & Ramanujam, 2009). Boss et al. (2009), for example, study precaution taking behaviors which capture both procedural and outcome oriented behaviors. This paper extends Lange's typology by adding flexibility in the use of the behavioral orientation dimension. Thus, our typology provides a clearer distinction between procedural and outcome oriented controls than in Lange (2008).



The three dimensions of corruption control—behavioral orientation, transmission channel, and motivational orientation—form 12 types of security-related corruption controls and three major systems of control. Although the dimensions are particularly designed for a typology of security-related corruption controls, they are also relevant to controls that seek to promote positive behavior. Promoting positive behavior can be done

through administrative or social channels, can be accomplished through different forms of motivation (e.g., intrinsic or extrinsic), and can be focused on security outcomes or security procedures. Thus, the typology is also pertinent to controls that promote positive security behavior, such as PSB and SCB. The three major systems of control include: structural systems, consequence systems, and commitment systems. The three major systems of control are derived from the motivational orientation dimension. Motivational orientation explains how controls catalyze behavior and why controls influence behavior, while transmission channel and behavioral orientation only explain who administers controls and what is administered. Thus, motivational orientation provides the most theoretically interesting distinction between control types. Each of three major systems is described below. Figure 3 presents the dimensions and types of security corruption controls.



### Structural Systems

*Bureaucratic controls* include rules, routines, policies, and hierarchical structures established by formal entities within the organization with legitimate power. Conversely, *concertive controls* include social norms and values and social structures established through interaction among peers. Thus, bureaucratic controls are administratively transmitted, while concertive controls are socially transmitted. In this typology, two types

of bureaucratic control (i.e., type 1 and type 2) and two types of concertive control (i.e., type 3 and type 4) were identified.

### ***Procedural Bureaucratic Controls (Type 1)***

Procedural bureaucratic controls are process oriented and administratively transmitted with a covert motivational orientation. *Procedural bureaucratic controls* refer to management interventions which seek to standardize work processes and procedures by controlling employees' perceptions of what should or should not occur in their work routines. Bureaucratic controls tend to be procedural in nature, though they may also be outcome oriented. Rules, for example, can be oriented toward procedures or outcomes, which promote different types of behavior (Lehman & Ramanujam, 2009). Bureaucratic controls become deeply embedded in the fabric of organizational life so that they are often taken for granted (March & Simon, 1958), making their motivational orientation covert. Further, organizational routines and processes may be embedded in information systems, making them even less overt (Gosain, 2004). In this way, bureaucratic controls minimize violations and abuse by naturalizing security behaviors. However, despite the existence of procedural bureaucratic controls, many employees still engage in deviant behavior. Procedural bureaucratic controls are often accompanied by other controls, such as sanctions and rewards, which deter noncompliance and incentivize compliance, respectively (Bulgurcu et al., 2010; Chen & Wen, 2012; D'Arcy et al., 2009).

Behavioral information security research tends to focus heavily on procedural bureaucratic controls, primarily in the form of ISP. In fact, all 35 articles reviewed in our study examine some form of procedural bureaucratic control. Studies primarily consider

how other types of controls affect compliance and noncompliance with ISP (e.g., Bulgurcu et al., 2010; D'Arcy et al., 2009; Herath & Rao, 2009b) and how awareness of ISP affects security behavior (e.g., Bulgurcu et al., 2010). D'Arcy et al. (2009) examine the effect awareness of security countermeasures have on intentions to misuse an organizations information assets. ISP is a procedural bureaucratic control to the extent that the policies focus on rules, work processes, and other antecedent behaviors that lead to secure systems.

### ***Outcome Oriented Bureaucratic Controls (Type 2)***

Outcome oriented bureaucratic controls are outcome oriented and administratively transmitted with a covert motivational orientation. *Outcome oriented bureaucratic controls* refer to management interventions which seek to standardized employees' perceptions of desired security outcomes by providing a formal and official vision of the outcomes. Outcome oriented bureaucratic controls are likely to take the form of rules and policies that are oriented toward desired outcomes rather than toward the antecedent behaviors of the desired outcomes. Thus, they may appear more like goals or high-level objectives than as rules that designate appropriate behavior. Importantly, outcome oriented rules and policies may lead to fewer rule and policy violations than procedural rules and policies (Lehman & Ramanujam, 2009). Outcome oriented bureaucratic controls minimize violations and abuse by naturalizing the pursuit of desired outcomes and the avoidance of undesired outcomes.

No security study to our knowledge directly examines outcome oriented rules and policies or other forms of outcome oriented bureaucratic controls. However, some studies

discuss outcome oriented policies indirectly through the study of outcome oriented behavior. Boss et al. (2009) and Bulgurcu et al. (2010), for example, define compliance with policy in terms of outcomes (e.g., secure computers and protected information technology resources) and not procedures. This is contrasted with studies that focus on procedural behaviors (e.g., logging off computers and using secure wireless connections). Studies that rely on protection motivation theory also tend to view compliance as outcome oriented (Herath & Rao, 2009b). In total, 13 studies examined outcome oriented security behaviors related to policy. However, it should be noted that these studies focus on the behavior and not on the characteristics of the particular control, namely ISP. Future research should examine outcome oriented policy to extend the work that has been done on outcome oriented behaviors.

### ***Procedural Concertive Controls (Type 3)***

Procedural concertive controls are process oriented and socially transmitted with a covert motivational orientation. *Procedural concertive controls* refer to socially constructed structural systems which seek to standardize work processes and procedures by controlling employees' normative perceptions of what should or should not occur in their work routines. Whereas outcome oriented concertive controls focus on socially generated values, procedural concertive controls focus on the socially generated rules systems that are likely to develop from the social values (Barker, 1993). Thus, procedural concertive controls focus on the informal social rules and policies that guide and constrain employee behavior. Procedural concertive controls minimize violations and abuse by naturalizing security behaviors through the development of social norms. Like

procedural bureaucratic controls, procedural concertive controls are likely to be accompanied by deterrents and incentives, such as social shaming or the granting of in-group status, respectively.

Several security studies examine social norms, which are a form of procedural concertive control (e.g., Bulgurcu et al., 2010; Herath & Rao, 2009b; Johnston & Warkentin, 2010). In total, 12 studies examined procedural concertive controls. However, these studies examine the effect of social norms on compliance or noncompliance with bureaucratic policy. Future studies should examine the antecedents of compliance and noncompliance with concertive policies and procedures. That is, social norms should be considered as an important dependent variable in information security research. This is particularly true when studying postbureaucratic organizations, as postbureaucratic organizations tend to rely more heavily on social control than administrative control (Lange, 2008; Van Alstyne, 1997). Examining concertive controls may also be important when studying decentralized organizations, where bureaucratic controls may be less efficacious (Lange, 2008).

#### ***Outcome Oriented Concertive Controls (Type 4)***

Outcome oriented concertive controls are outcome oriented and socially transmitted with a covert motivational orientation. *Outcome oriented concertive controls* refer to socially constructed values which seek to standardize employees' perceptions of desired security outcomes by providing a social and cultural vision of the outcomes. Outcome oriented concertive controls are established through a process of negotiation that leads to consensually generated values (Barker, 1993; Tompkins & Cheney, 1985).

Barker (1993) suggests that structural systems are likely to result from the values identified during social negotiations; however, these structural systems are procedural in nature and represent procedural concertive controls. Like bureaucratic controls, concertive controls may be deeply embedded within the social structures in an organization, which help to naturalize the values and associated rules systems. This is the premise of critical and postmodern theories (Fairclough, Mulderrig, & Wodak, 1997; Lincoln, Lynham, & Guba, 2011). That is, social values, norms, and structures crystallize and become taken for granted (Lincoln et al., 2011; Stahl, Doherty, & Shaw, 2012). Outcome oriented concertive controls may manifest as security-related aspects of organizational culture or subcultures. Outcome oriented concertive controls minimize violations and abuse by naturalizing the pursuit of values related to security, such as the protection of organizational information or protection of clients.

Many information security studies examine the effect that social norms have on security behavior. When social norms focus on outcomes, norms represent a form of outcome oriented concertive control. Subjective and descriptive norm (Bulgurcu et al., 2010; Herath & Rao, 2009b), social influence (Johnston & Warkentin, 2010), organizational norms (Li et al., 2010), and workgroup norms (Guo et al., 2011) are some conceptualizations of concertive controls found in security research. However, these conceptualizations are mostly procedural in nature. Only one study in our review directly discussed outcome oriented concertive controls. Leonard et al. (2004) describe the importance of establishing an ethical climate which promotes outcomes such as caring. However, ethical climate was not operationalized or empirically evaluated in the study.

Understanding the effect socially constructed values have on employee behavior is an important direction for future research.

### **Consequence Systems**

Consequence systems are high-level control systems that motivate action through extrinsically oriented rewards or punishments. Consequence systems can be transmitted administratively through formal sanctions and rewards or socially through social shaming and rejection or by granting individuals in-group status. Further, consequence systems can be procedural or outcome oriented. That is, consequence systems may offer positive or negative consequences for compliance or noncompliance with procedures and for accomplishing or failing to accomplish specified outcomes. In our typology, four types of consequence systems (i.e., type 5, type 6, type 7, and type 8) exist.

#### ***Procedural Consequence Systems (Type 5)***

Procedural consequence systems are process oriented and administratively transmitted with an extrinsic motivational orientation. *Procedural consequence systems* refer to management interventions which seek to deter noncompliance or incentivize compliance with formal work processes and procedures by providing punishment or reward for noncompliant or compliant behavior, respectively. Procedural consequence systems include punishment and rewards disseminated by formal, legitimate entities in the organization (Lange, 2008). Thus, they are administratively transmitted. Punishments, such as organizational sanctions, focus on deterring misbehavior, while rewards attempt to incentivize correct behavior (Chen & Wen, 2012). Procedural consequence systems

minimize violations and abuse by providing external motivation to engage in specified behaviors.

Lange (2008) suggests that punishment is process oriented, while rewards are outcome oriented. Sanctions are more likely to be process oriented; however, rewards are always outcome oriented. Sanctions are deterrent controls that are intended to discourage negative behavior and not necessarily to encourage positive behavior (D'Arcy & Herath, 2011). Therefore, punishment is likely to assume a process orientation. Still, punishment can be administered for undesirable outcomes rather than undesirable behaviors (Lehman & Ramanujam, 2009). Rewards, however, can be given for complying with procedural policies and work processes or for accomplishing specified outcomes (Boss et al., 2009; Cardinal, 2001). Thus, rewards may easily be designed as either process or outcome oriented. When rewards are used to incentivize behaviors that are antecedent to the expected outcomes of the behaviors, rewards represent procedural consequence systems.

Consequence systems are a strong focus of behavioral information security studies. In our review, 24 of the 35 studies examined some form of procedural consequence system, primarily sanctions. Many studies use general deterrence theory (Blumstein, 1978) to explain how perceptions of sanctions can affect compliance with ISP (e.g., D'Arcy et al., 2009; Hovav & D'Arcy, 2012; Siponen & Vance, 2010; D. W. J. Straub & Nance, 1990). Additionally, Boss et al. (2009) suggest that both process oriented and outcome oriented rewards can influence perceptions of the mandatoriness of ISP and subsequent compliance with ISP.

### ***Outcome Oriented Consequence Systems (Type 6)***

Outcome oriented consequence systems are outcome oriented and administratively transmitted with an extrinsic motivational orientation. *Outcome oriented consequence systems* refer to management interventions which seek to align employees' goals with desired security outcomes by providing punishment or reward for failing to achieve or achieving the desired outcomes, respectively. Outcome oriented consequence systems differ from procedural consequence systems in behavioral orientation. As suggested earlier, outcome oriented consequence systems are more likely to take the form of rewards rather than punishment. However, sanctions designed to punish failed objectives are considered outcome oriented consequence systems. Punishment for failed security objectives has not been considered in information security research, though it has received some attention in general management literature (e.g., Lehman & Ramanujam, 2009). Outcome oriented consequence systems minimize violations and abuse by providing external motivation to work toward security outcomes specified by the organization.

Security studies have examined outcome oriented consequence systems as outcome oriented rewards. Boss et al. (2009) study both outcome and behavioral rewards. Similarly, Bulgurcu et al. (2010) study rewards in terms of outcome beliefs. Fear appeals are outcome oriented consequence systems. Fear appeals attempt to motivate action by highlighting the natural consequences of insecure behavior (Johnston & Warkentin, 2010) and fear appeals focus on security outcomes (i.e., threats to the security and

protection of organizational information). Only four articles in our review examined outcome oriented consequence systems.

### ***Procedural Social Consequence Systems (Type 7)***

Procedural social consequence systems are process oriented and socially transmitted with an extrinsic motivational orientation. *Procedural social consequence systems* refer to socially or culturally derived mechanisms with the organization which seek to deter noncompliance or incentivize compliance with formal work processes and procedures or social structural systems by providing punishment or reward for noncompliant or compliant behavior, respectively. Procedural social consequence systems seek to punish or reward individuals for noncompliance or compliance with socially generated rules or formal procedural policies. Procedural social consequence systems minimize violations and abuse by providing socially derived external motivation to engage in socially or administratively defined behaviors.

Procedural social consequence systems are studied as informal sanctions in information security research (D'Arcy & Devaraj, 2012; Li et al., 2010; Siponen & Vance, 2010; Vance & Siponen, 2012). Four studies in our review examine social consequence systems. No study to our knowledge examines procedural consequence systems as social reward systems. Social reward systems might include receiving or maintaining in-group status and receiving socially generated praise and recognition. Social praise and recognition does not include administratively transmitted praise and recognition, which is the typical focus of research on rewards. Socially generated reward systems might be studied in future research.

### ***Outcome Oriented Social Consequence Systems (Type 8)***

Outcome oriented social consequence systems are outcome oriented and socially transmitted with an extrinsic motivational orientation. *Outcome oriented social consequence systems* refer to socially or culturally derived mechanisms which seek to align employees' goals and values with desired security outcomes and security-related values by providing social punishment or reward for failing to achieve or achieving the desired outcomes and failing to uphold or upholding the security-related values, respectively. The socially derived mechanisms include actions such as shaming, expressing disapproval, and denying or granting in-group status to individuals. Social consequence systems may be established to monitor compliance with socially generated values (Barker, 1993) or with outcome oriented policies (e.g., Bulgurcu et al., 2010; Herath & Rao, 2009b; Johnston & Warkentin, 2010; Siponen & Vance, 2010). However, social consequence systems often emerge to punish the failure to adopt social values or to reward the adoption of social values (Wright & Barker, 2000). Thus, outcome oriented social consequence systems minimize violations and abuse by providing socially derived external motivation to work toward administratively defined security outcomes or to uphold social values established by peers, respectively.

In security studies, informal sanctions are a form of social consequence system. Siponen and Vance (2010) and D'Arcy and Devaraj (2012) suggest that informal sanctions may decrease intentions to misuse information resources. Informal sanctions include "the disapproval of friends or peers for a given action" (Siponen & Vance, 2010, p. 491). As suggested by this quote, the informal sanctions studied in Siponen and Vance

(2010) are likely procedural in nature as they focus on “given actions” rather than on outcomes or social values. Based on our review, security studies have not examined social consequence systems with an outcome oriented behavioral orientation. This is an area for future research.

### **Commitment Systems**

Commitment systems are another form of high-level systems of control. Unlike consequence systems, which are oriented toward extrinsic motivation, commitment systems seek to engender intrinsic motivation to avoid negative behavior and engage in positive behavior. Commitment systems may be administrative or social in nature and may also be process or outcome oriented. In general, commitment systems seek to engage employees in improving security-related policies, norms, work processes, and goals or educating and promoting moral behavior. Four types of commitment systems exist (i.e., type 9, type 10, type 11, and type 12).

#### ***Procedural Commitment systems (Type 9)***

Procedural commitment systems are process oriented and administratively transmitted with an intrinsic motivational orientation. *Procedural commitment systems* refer to management interventions which seek to internalize motivation to engage in formal work processes and to follow formal procedures. Developing intrinsic motivation to engage in tasks is an important managerial concern. Intrinsically driven behaviors can lead to better outcomes and well-adjusted employees (Gagne & Deci, 2005; Ryan & Deci, 1985, 2000). Procedural commitment systems include countermeasures such as training, codes of ethics, and encouraging participation in the development of policy.

Procedural commitment systems are formal management interventions, and thus, are under direct control of the organization. Procedural commitment systems minimize violations and abuse by strengthening employees' internal psychological commitment to accept and follow the organization's security policies and to avoid noncompliance with the policies.

A total of 19 studies examined some form of control that improves commitment to procedural aspects of ISP or measured employees' commitment to ISP. Based on the review, diverse methods for gaining commitment exist. Theories of user buy-in may be appropriate explanations for internal commitment to procedural policies and rules (Spears & Barki, 2010). Employee participation in the design of security controls may help to increase commitment to the policies of the organization (Spears & Barki, 2010). Additionally, commitment to security policies may increase when organizational policies are congruent with employees self-identity (Guo et al., 2011). Aligning employees' self-identity with the organization's security requirements may be accomplished through codes of ethics (Harrington, 1996). Security training may also help to align employees' knowledge and beliefs with those of the organization (Puhakainen & Siponen, 2010). However, when training is used to promote sanctions for misbehavior, training becomes a part of an organization's consequence systems.

### ***Outcome Oriented Commitment systems (Type 10)***

Outcome oriented commitment systems are outcome oriented and administratively transmitted with an intrinsic motivational orientation. *Outcome oriented commitment systems* refer to interventions which seek to internalize motivation to achieve

desired security outcomes as defined by the organization. While procedural commitment systems focus on developing internal commitment to policies and procedures, outcome oriented commitment systems seek to develop commitment to the goals and desired outcomes of the organization. Again, buy-in and participation may be the key to establishing commitment to security outcomes. Once commitment is achieved, employees may experience an internal drive to ensure the security of organizational assets (Spears & Barki, 2010). Commitment to the organization may also affect commitment to security objectives, as employees' concern for the well-being of the organization may drive them to protect information assets (Herath & Rao, 2009b). Thus, organizations might develop controls that focus on building commitment to the organization. Outcome oriented commitment systems minimize violations and abuse by strengthening employees' internal psychological commitment to the organization's security goals and desired security outcomes.

Ten studies in our review examined outcome oriented commitment systems. Again, a diverse set of controls were used. Along with improving compliance to procedural policy, Spears and Barki (2010) find that allowing employees to participate in the design of security objectives improves the extent to which security objectives and business objectives align, thus creating stronger commitment to the security objectives. Ethics training may also lead to values that commit employees to secure outcomes (Myrsky et al., 2009). Other studies focused on outcome oriented variables, but didn't examine them in relation to a security control. For example, Herath and Rao (2009b) find that organizational commitment leads to increased policy compliance intentions.

However, Herath and Rao (2009b) don't consider the antecedent conditions that lead to organizational commitment. Similarly, Xue et al. (2011) examine satisfaction in relation to ISP compliance intentions; however, they do not study ways that organizations can create satisfaction. Thus, future research should examine or develop controls that lead to feelings of commitment to the organization or satisfaction with information technology (IT).

### ***Procedural Social Commitment systems (Type II)***

Procedural social commitment systems are process oriented and socially transmitted with an intrinsic motivational orientation. *Procedural social commitment systems* refer to socially or culturally derived mechanisms with an organization which seek to internalize motivation to engage in formal work processes and follow formal procedures, and to follow socially and culturally derived structural systems. Internal commitment to social norms within the organization may be greater when social norms are congruent with *hypernorms*—culturally accepted behavioral norms (Lange, 2008). Thus, developing social norms that conform to employees' existing normative beliefs can improve commitment to the social norms. Additionally, organizational culture and social learning systems may lead to improved behavior (Warkentin et al., 2011). Procedural social commitment systems minimize violations and abuse by strengthening employees' internal psychological commitment to the organization's policies and social norms and structural systems.

A total of four studies in our review examined procedural social commitment systems. Whistleblowing can decrease computer abuse (Lowry, Moody, Galletta, &

Vance, 2012). Whistleblowing may focus on outcomes oriented complaints or procedural complaints. Therefore, whistleblowing fits as both an outcome oriented and procedural control depending on its behavioral orientation. Similarly, Hu et al. (2012) examine the effect that organizational cultural beliefs about rules have on security behaviors. They find that beliefs about rules affect security behaviors. Myyry et al. (2009) suggest that at certain levels of moral reasoning, individuals' commitment to social groups causes improved behavior. Lastly, Warkentin et al. (2011) examine social learning systems. They find that learning from peers can lead to improved beliefs about compliance and affect security behaviors.

### ***Outcome Oriented Social Commitment systems (Type 12)***

Outcome oriented social commitment systems are outcome oriented and socially transmitted with an intrinsic motivational orientation. *Outcome oriented social commitment systems* refer to socially or culturally derived mechanisms which seek to internalize motivation to achieve formally specified security outcomes or uphold social values. The commitment systems previous discussed are concerned with effecting change through management interventions. Social commitment systems, however, are concerned with effecting intrinsically driven change through social and cultural means. Engendering an organizational culture that is open to whistleblowing is an important form of an outcome oriented social commitment system (Lange, 2008). Whistleblowers dissent from social norms to improve organizational outcomes, which requires strong intrinsic motivation (Warren, 2003). Thus, outcome oriented social commitment systems minimize violations and abuse by strengthening employees' internal psychological

commitment to the organization's desired security outcomes and social and cultural values.

Two studies in our review examined outcome oriented social commitment systems. Lowry et al. (2012) examines whistleblowing through information systems in the context of computer abuse related to the Sarbanes-Oxley Act. They find that perceptions of trust, anonymity, and risk are important in whistleblowing contexts. This suggests that organizational cultures must be cultivated to decrease social risks and increase trust. Similarly, Hu et al. (2012) describe the importance of organizational culture in producing secure behaviors. They examine both goal-oriented and rule-oriented aspects of culture. They find that organizational culture is important in promoting secure behavior. They also find that organizational culture can affect employees' personal beliefs. Given the small amount of attention given to outcome oriented social commitment systems, future research should examine these controls further.

### **Social Controls in InfoSec Research**

Based on the coding of the behavioral InfoSec studies in Appendix A, informal social controls are underrepresented in the literature. Informal social controls include types 3, 4, 7, 8, 11, and 12 and span the three major corruption-control systems identified in the typology (i.e., rule systems, consequence systems, and commitment systems). In other fields, social control has been identified as a highly influential form of behavioral control (R L Akers, 1985; Ronald L. Akers, 2009; Sutherland, 1947). Further, theories of social control, namely ASLT, exhibits stronger effect sizes than general deterrence theory and rational choice theory (Pratt et al., 2010). General deterrence theory and rational

choice theory are heavily studied in behavioral InfoSec research (Bulgurcu et al., 2010; D'Arcy & Herath, 2011). Therefore, theories of social control deserve future attention in behavioral InfoSec research. Informal social control is primarily represented by two constructs in behavioral InfoSec research, social norms and informal sanctions. However, a few studies integrated more robust theories of social control. We now examine these constructs and theories in greater detail.

### ***Social Norms***

Social norms in behavioral InfoSec research are conceptualized in several ways, such as: normative beliefs, workgroup norms, subjective norm, descriptive norm, and social influence (Bulgurcu et al., 2010; Guo et al., 2011; Herath & Rao, 2009a, 2009b; Johnston & Warkentin, 2010). Though the influence of social norms on behavior assumes many names, the varied conceptualizations can be reduced to two primary types of normative control. The first type is labeled subjective norm and the second type is labeled descriptive norm. *Subjective norm* refers to an employee's perception of how others in the organization believe the employee should act, and *descriptive norm* refers to an employee's perception of how others in the organization act (Herath & Rao, 2009b). Together, subjective and descriptive norm capture a more complete conceptualization of employees' perceptions of concertive controls than either can alone. Studies also examine personal norms and moral beliefs (e.g., Myyry et al., 2009); however, these are not measures of social controls. Personal norms and moral beliefs are the normative attitudes and beliefs that are assimilated through personal experience and social interaction (Ronald L. Akers, 2009). Thus, they are the result of social controls.

Studies of social norms in InfoSec research are primarily rooted in the theory of reasoned action and its derivative theories (e.g., Bulgurcu et al., 2010; Guo et al., 2011; Herath & Rao, 2009a, 2009b; Lee, Lee, & Yoo, 2004). These theories suggest that behavior is planned and that cognitive and normative functions influence intentions to participate in a particular behavior (Ajzen, 1985; Fishbein & Ajzen, 1975). While these theories acknowledge the influence of norms on behavior and behavioral intentions, the theories offer a weak description of social control and mostly fail to describe how norms are formed and adopted. To arrive a fuller understanding of social processes, theories of social influence must be consulted, such a social cognitive theory (Bandura, 1986), differential association theory (Sutherland, 1947), and Akers' social learning theory (R L Akers, 1985). From a managerial perspective, understanding how norms form and are adopted is a crucial concern. If managers understand the development of norms, they may be able to manipulate social processes to promote behaviors that benefit the organization (Lange, 2008).

### ***Informal Sanctions***

Informal sanctions and other forms of informal behavioral reinforcement are also studied in behavioral InfoSec research. However, informal sanctions are studied far less than social norms. Informal social norms include the social and self-imposed costs accrued for engaging in a deviant act (D'Arcy & Devaraj, 2012). Social costs have been studied as social desirability pressures (D'Arcy & Devaraj, 2012), loss of respect from peers (Siponen & Vance, 2010; Vance & Siponen, 2012), disapproval of peers (Li et al., 2010). Self-imposed costs have been studied as shame (D'Arcy & Herath, 2011; Siponen

& Vance, 2010) and moral beliefs (D'Arcy & Devaraj, 2012). The behavioral influence of informal sanctions has received mixed support. Some studies found that informal sanctions have some influence (D'Arcy & Devaraj, 2012; Vance & Siponen, 2012). Other studies found no statistical support for the behavioral influence of informal sanctions (Li et al., 2010). Further, one study found that the influence of both formal and informal sanctions is statistically insignificant when neutralizing behaviors are considered (Siponen & Vance, 2010). The mixed findings are found in other fields as well. Pratt et al. (2010), for example, conducted a statistical meta-analysis of research on Akers' social learning theory. They found that statistical support for the assertion that reinforcement mechanisms (i.e., formal and informal sanctions) influence behavior was weak and inconsistent. Despite mixed results, social sanctions are shown across several studies to be more influential on behavior than formal sanctions (D'Arcy & Devaraj, 2012; Pratt, Cullen, Blevins, Daigle, & Madensen, 2006; Siponen & Vance, 2010). These findings provide further evidence of the need to explore informal controls in behavioral InfoSec research.

### ***Theories of Social Control in InfoSec Research***

A few behavioral InfoSec studies explore social variables in greater depth by incorporating theories of social control. Lee et al. (2004) examined social control theory in an information security context. Social control theory suggests that an individual's bond to society prevents the individual from engaging in deviant behavior (Agnew, 1991; Hirschi, 1969). In social control theory, delinquency is the result of weak social bonds. Lee et al. (2004) suggested that the strength of an individual's trust in organizations, a

type of social bond, explains computer abuse behaviors in organizations. They found partial support for social control theory in a security context.

Warkentin et al. (2011) examined Bandura's social learning theory in a security context. Bandura's social learning theory suggests that an individual's self-efficacy—the individual's belief that the individual is capable of performing a specific task (Bandura, 1977a, 1977b)—influences the individual's ability to perform the task. Bandura's social learning theory suggests that self-efficacy is developed socially through verbal persuasion, situational support, and vicarious experience (Warkentin et al., 2011). Though Warkentin et al. (2011) employs a theory of social influence, the outcome variable was positive security behavior. Our focus is positive and negative behavior, as research on deviant security behavior is underrepresented (Warkentin et al., 2012). Other theories of social control may be better suited for explaining and predicting deviant security behavior than Bandura's social learning theory. Deviant behavior, particularly negligent behavior, may require less skill and effort than positive behavior; therefore, self-efficacy may lose explanatory and predictive power for many types of deviance (Ronald L. Akers, 2009). Additionally, Herath and Rao (2009b) found that subjective norm has a larger effect size than self-efficacy and that descriptive norm has a similar effect size to self-efficacy. Thus, theories of norms and norm development, such as Akers' social learning theory, may provide stronger explanatory and predictive power.

Siponen and Vance (2010) use neutralization theory to explain intentions to violation information security policy. Neutralization theory (Sykes & Matza, 1957) suggests that individuals develop rationalizations for deviant behavior to accommodate

for the negative stigmas attached with committing deviant behaviors. These rationalizations make deviant behavior possible. Siponen and Vance (2010) found support to suggest that neutralizations negate the positive effects of formal and informal sanctions on computer behavior. Neutralization theory offers interesting insight into social influence. However, neutralization is incorporated into more extensive and robust theories of social control, such as Akers' social learning theory.

## **CHAPTER III**

### **THEORETICAL FOUNDATIONS**

#### **Social Structure and Social Process**

Theories of social control tend to emphasize social structures or social processes, though some, such as social learning and social structure theory (SSSL), attempt to incorporate both perspectives (Ronald L. Akers, 2009). Theories of social structure seek to explain how social structures produce environments conducive to deviant behavior. Strain theory (Merton, 1938), for example, is a common and influential structural theory of deviance. Strain theory suggests that societies promote specific goals (e.g., financial independence, happiness, etc.) and that individuals strive to achieve these goals. Strain theory posits that when individuals experience strain that limits their ability to achieve societal goals through legitimate means, they seek for unconventional ways to achieve the goals. Strain is depicted as emanating primarily from conditions (e.g., poverty) caused by social structures. Theories of social process, however, explain how individuals learn deviant values and behavior. Differential association theory (Sutherland, 1947), for example, is an influential theory of social process. Differential association theory suggests that individuals learn to behave in certain ways through their associations with family and peers by assimilating definitions favorable or unfavorable to deviance. Though understudied in InfoSec research, theories of social structure and social process are represented in a few InfoSec studies (Lee et al., 2004; Warkentin et al., 2011).

## **Differential Association Theory**

Differential association theory (Sutherland, 1947) is a prominent theory of social corruption control in criminology (Ronald L. Akers, 2009). Differential association theory (DAT) suggests that individuals learn to be deviant. DAT assumes that individuals learn deviant behavior in the same way that they learn compliant behavior. The learning process occurs as a focal individual has repeated interactions with important and respected individuals. During interactions with others, the focal individual comes in contact with definitions. In DAT, *definitions* refer to beliefs, values, and rationalizations that either favor compliant behavior or favor deviant behavior (R L Akers, 1985; Sutherland, 1947). In DAT, general definitions of the favorability of compliance and deviance develop at a young age; however, social learning is also situational and occurs at later stages of life as well (Ronald L. Akers, 2009). Social learning can occur in specific environments and situations, and related to specific norms and rules through socialization within that particular environment. Thus, definitions of behavior learned in childhood can change over time and general definitions of compliance and deviance may not influence specific definitions in new situations. Further, DAT posits that close-knit relationships with family and peers are more influential on social learning than weak relationships. DAT predicts that the ratio of contact with definitions that favor compliance compared to definitions that favor deviance determine the likelihood that a person will engage in compliant or deviant behavior. The ratio of contact an individual has with compliant definitions to deviant definitions is known as *differential association*. For example, if an individual comes into contact with more definitions that favor deviant

behavior than compliant behavior, the individual will be more likely to engage in deviant behavior. Many studies support the premise that differential association influences behavior (Ronald L. Akers, 2009; Pratt et al., 2010).

Since its original conception, DAT has been extended in many ways.

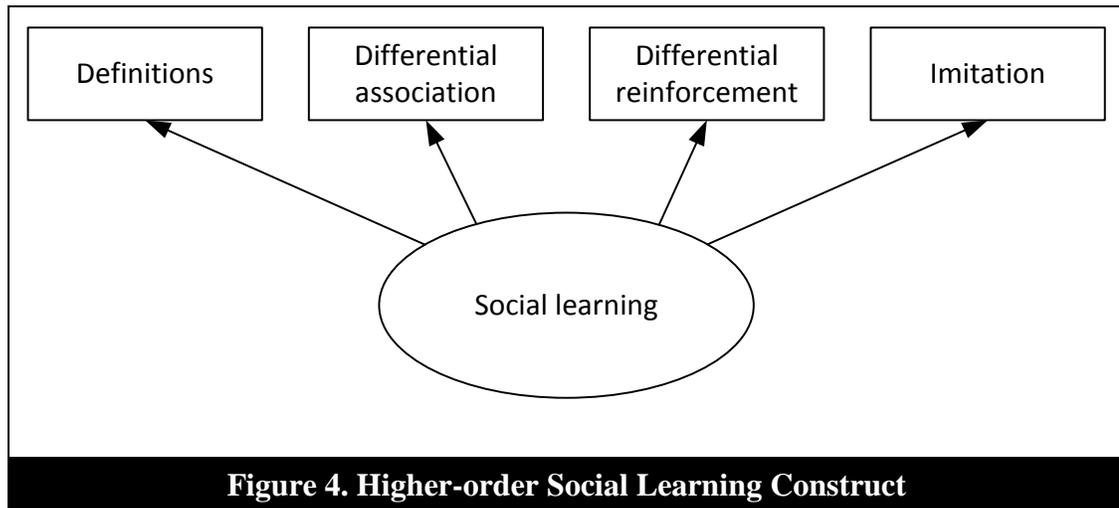
Neutralization theory (Sykes & Matza, 1957), for example, is an extension of DAT that focuses on Sutherland's concept of definitions (Ronald L. Akers, 2009). Neutralization theory frames definitions as rationalizations for deviant behavior. In neutralization theory, rationalizations of behavior are predicted to increase engagement in deviant behavior (Siponen & Vance, 2010). Akers' social learning theory (R L Akers, 1985; Ronald L. Akers, 2009) is another prominent extension of DAT. Akers' Social learning theory (ASLT) is a more comprehensive extension of DAT that incorporates the major premises of DAT, concepts from neutralization theory, and concepts from behavioral conditioning and learning.

### **Akers' Social Learning Theory**

ASLT, like DAT, suggests that individuals learn deviant values and behavior through differential association with close others (e.g., family, peers, and coworkers). However, ASLT specifies learning mechanisms. That is, ASLT explains how individuals learn deviant values and behavior. DAT only specifies that learning occurs; DAT does not offer deep insight into learning mechanisms (Ronald L. Akers, 2009). ASLT specifies two primary learning mechanisms, differential reinforcement and imitation (R L Akers, 1985). *Differential reinforcement* refers to the "frequency, amount, and probability of experienced and perceived contingent rewards and punishments" (Ronald L. Akers, 2009,

p. 52, pp. 52). *Imitation* refers to the observations and modeling of others' behaviors and the associated consequences of the behaviors (Ronald L. Akers, 2009). Imitation in ASLT is similar to modeling in Bandura's social learning theory (Bandura, 1977b). Imitation is important when an individual is first introduced to a new behavior; however, imitation becomes less important as the individual engages in the behavior and experiences differential reinforcement (Ronald L. Akers, 2009). Thus, ASLT is primarily concerned with four variables: differential association, definitions, differential reinforcement, and imitation. In ASLT, imitation and differential reinforcement occur within the context of differential associations and influence individuals' definitions (Ronald L. Akers, 2009). A recent meta-analysis of 133 empirical studies that employed ASLT found that the effect sizes for differential association and definitions are strong, while effect sizes for differential reinforcement and imitation are moderate to weak (Pratt et al., 2010).

With advances in statistical analysis, namely structural equation modeling, the four primary variables in ASLT are regularly represented as reflections of a higher-order construct, social learning (Ronald L. Akers, 2009; R L Akers & Lee, 1996; Morris & Higgins, 2010). Representing social learning as a higher-order construct allows researchers to examine social learning at different time periods. Findings suggest that social learning which occurs earlier in an individual's life or earlier in a sequence of learning interactions influences social learning later in life or in later learning interactions (Ronald L. Akers, 2009; R L Akers & Lee, 1996). Figure 4 presents the higher-order representation of social learning.



The relationships between some of the variables in social learning theory are reciprocal (Ronald L. Akers, 2009). Most importantly, differential association has been examined as an exogenous and endogenous variable. As an exogenous variable, differential association influences the definitions individuals are exposed to and the reinforcement individuals receive (Krohn, 1999; Krohn et al., 1985). That is, associations with peers influence individuals' values and behaviors. As an endogenous variable, differential association is influenced by anticipated reinforcement (R L Akers, 1998; Krohn, 1999). That is, individuals select who they associate with based on the values and behaviors that their peers display. This reciprocal relationship has been demonstrated through non-recursive structural equation modeling (Krohn, Lizotte, Thornberry, Smith, & McDowall, 1996). The complex relationships between social differential association and other variables presents another reason for constructing a simplified, higher-order social learning construct. Further, reflective measurement assumes that the measures or factors are mutually reinforcing, whereas formative measurement assumes that the

measures or factors are distinct (Diamantopoulos & Siguaaw, 2006; Petter, Straub, & Rai, 2007). Thus, representing social learning as a second order construct consisting of reflective factors is in-line with the reinforcing nature of ASLT variables.

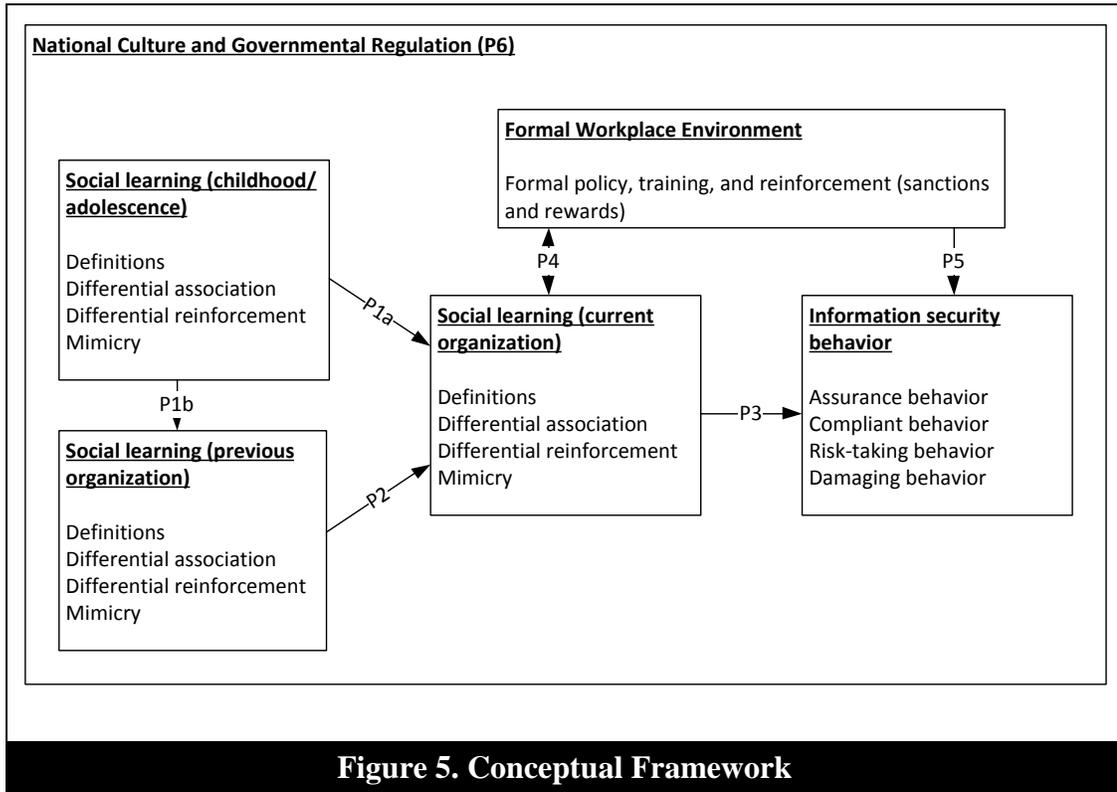
ASLT has been used in a few instances to examine security-related topics. Several of the studies examine college students' online behaviors. For example, Skinner and Fream (1997) studied ASLT in the context of computer crime among college students. Using a survey and regression analysis, they found support of the influence of imitation, differential association, reinforcement, and definitions across different behaviors (e.g., software piracy and password guessing). Morris and Higgins (2010) also found that ASLT explains digital piracy among college students. Similarly, ASLT can explain e-cheating behavior by college students (Stogner, Miller, & Marcum, 2013). Rogers (2001) examined ASLT in the context of computer crime by studying convicted criminals' records and survey responses from general criminals (i.e., not computer criminals) and non-criminals' responses to a survey. Rogers was unable to collect data directly from computer criminals. Rogers found that convicted criminals had associated with more deviant individuals and had encountered more definitions in favor of crime than non-criminals. However, the data for computer crimes was assessed from criminal records and not through surveys. Further, no data is offered to suggest whether the computer criminals were organizational insiders or external hackers. Nor did the data suggest that the attacks were levied against organizations. The data for non-criminals was collected through surveys. These studies show the potential for ASLT to be used in behavioral InfoSec research to study employees' negative security behaviors.

## **CHAPTER IV**

### **CONCEPTUAL MODEL**

#### **Conceptual Overview**

The model presented herein is founded primarily on ASLT. Additionally, we incorporate variables of formal controls (i.e., formal sanctions and formal training) and environmental factors (i.e., national origin) in an attempt to further develop a contingency theory of security-related corruption control. Thus, we examine how social learning influences PSB, SCB, SRB, and SDB in different cultures and in the presence of formal administrative controls. We adopt the higher-order social learning construct (Ronald L. Akers, 2009; R L Akers & Lee, 1996; Morris & Higgins, 2010) in order to examine how learning in early social interactions influence learning in later interactions. Specifically, we seek to understand how general tendencies toward deviant or compliant behavior learned in childhood and adolescence influence the learning of security-specific values and behaviors developed through interaction with peers at an individual's organization. We also consider how security-specific social learning at an individual's previous organization influences the individual's social learning at the individual's current organization. Figure 5 presents the conceptual framework that guides the examination herein.



## Social Learning

### *Social Learning Overtime Time*

Social learning is both stable and situational. That is, values and behaviors learned in childhood and adolescence are likely to have a strong effect on the adoption of values and behaviors in adulthood; however, situational factors may influence the adoption of values and behaviors contrary to those learned in childhood and adolescence (Ronald L. Akers, 2009). Although this is assumed in ASLT, few studies have examined how consistent beliefs are over time. For example, it is assumed that an individual who learned in adolescence that deviant behavior is highly valued and rewarded will likely develop general tendencies toward deviance in adulthood. However, deviant tendencies

developed in adolescence may not influence all forms of behavior. An individual with deviant tendencies can learn positive security behaviors (i.e., PSB and CSB) through differential association with others who value security. Conversely, individuals with compliant tendencies developed in adolescence can learn deviant security behaviors through differential association with others who value SRB and SDB.

We posit that general values toward deviance or compliance learned in childhood and adolescence influence social learning in organizational contexts. This may occur for several reasons. First, individuals who learn deviant values in their childhood and adolescence are more likely to associate with peers that favor deviance (Ronald L. Akers, 2009). Thus, individuals with deviant tendencies may seek out close relationships with deviant co-workers, while avoiding close relationships with highly compliant co-workers. Conversely, those who learn compliant values may be more likely to associate with compliant co-workers. Second, individuals with tendencies toward deviance or compliance may be more likely to associate with deviant or compliant peers outside of the workplace. If non-work peers exhibit negative values toward information security or workplace policies and share stories about SRB or SDB, the focal individual may be influenced more by these non-work peers than by work peers. This may occur because close peer relationships, such as friendships, have greater influence on social learning than casual relationships, such as work relationships (R L Akers, 1985; Sutherland, 1947). Non-work relationships and values learned in childhood and adolescence do not figure into existing behavioral InfoSec research. Studies of norms in existing behavioral InfoSec research limit normative influence strictly to individuals within the target

employee's organization. This simplistic view of norms and social influence fails to acknowledge that social learning is a historical and ongoing process. In summary, we posit:

*Proposition 1a and 1b: General tendencies toward deviance or compliance learned in childhood will influence social learning perceptions in the workplace (previous and current organizations).*

Social learning that occurs during an individual's tenure at a prior organization is also likely to influence the social learning of security values and behaviors at the individual's current organization. This may occur for several reasons. First, social learning in the individual's prior organization will include specific learning related to organizational policy and information security. This is contrasted with general values, beliefs, and behaviors developed in childhood and adolescence. Not every organization adopts the same security values, norms, policies and procedures. If an individual learns deviant or compliant security behaviors in a prior organization through imitation reinforcement, the individual may carry the values and behaviors from the previous organization to the current organization. Deviant or compliant security behaviors learned in the prior organization may persist unless strong reinforcement and modeling of the opposite kind is encountered in the current organization. However, as we discuss later, with time, prior behaviors may be dropped to accommodate the norms of the new organization. By examining the behavior learned in previous and current organizations, we seek to understand how individuals carry behaviors from organization to organization. In summary, we posit:

*Proposition 2: Secured values, beliefs, and behaviors learned in previous organizations will influence the social learning process in an employee's current organization.*

### ***Social Learning and Security Behavior***

According to ASLT, a deviant or compliant behavior is learned by adopting definitions in favor of the deviant or compliant behavior through differential association (R L Akers, 1985; Ronald L. Akers, 2009). The behavior is learned through imitation and differential reinforcement (Ronald L. Akers, 2009). In organization settings, learning occurs through association with managers and coworkers (Ruiz-Palomino & Martinez-Cañas, 2011; Zey-Ferrell & Ferrell, 1982). During the socialization process which occurs when an employee joins an organization, the employee learns definitions regarding what is appropriate and inappropriate security behavior. Individuals learn more from peers with close relationships than from peers with weak relationships. The learning of deviant or compliant values and behaviors produces the foundations and motivations to engage in deviant or compliant behavior (Ronald L. Akers, 2009). Based on the premises of ASLT, we propose:

*Proposition 3: values, beliefs, and behaviors learned through social interaction in the workplace will influence information security behaviors.*

### **Contingency Effects**

#### ***The Intervening Role of the Formal Workplace Environment***

ASLT suggests that reinforcement mechanisms influence social learning (R L Akers, 1985). In ASLT, differential reinforcement consists of formal and informal

reinforcement. However, we separate formal reinforcement from informal reinforcement. We examine social learning strictly from the perspective of informal learning through informal learning mechanisms. We do this to understand the different effects that administratively and informal social control exerts on employee behavior. We seek to understand how social learning influences perceptions of administrative mechanisms and how administrative mechanisms influence social learning. Social learning is an organic process between peers, but the organic social learning process can be influenced by administrative influence, such as formal sanctions and formal training. Through formal sanctions, organizations provide reinforcement to deter deviant behavior (D'Arcy et al., 2009; D. W. J. Straub & Nance, 1990). Similarly, formal rewards provided by the organization can reinforce positive security behavior (Boss et al., 2009; Bulgurcu et al., 2010). Further, organizations can disseminate their own definitions of appropriate and inappropriate behavior through security policy and formal training. Through training, employees learn definitions in favor of compliant behavior (Puhakainen & Siponen, 2010) and against noncompliant behavior (D'Arcy et al., 2009). Similarly, social learning consists of definitions that favor different perspectives. Deviant social learning is likely to lead to negative attitudes toward formal controls and compliant social learning is likely to lead to positive attitudes toward formal controls. Thus, we propose:

*Proposition 4a and 4b: Social learning will influence employees' perceptions of administrative controls and administrative controls will influence social learning.*

### ***The Intervening Role of National Origin***

Although ASLT is not a cultural theory of deviance (R L Akers, 1996), social learning happens much the same way in different national cultures (Hwang & Akers, 2003; Jensen & Akers, 2003; Wang & Jensen, 2003). Although the process of social learning may be similar across cultures, the content of social learning (i.e., the values and behaviors learned) is likely to differ across cultures. Social learning takes place within different cultural and political environments throughout the world. That is, social learning occurs within the value systems supported by different cultures and governments. Social learning occurs within the legal systems supported by governments of different nations. Laws differ across nations. Thus, legal definitions influence individuals differently across nations. For example, copyright violations may be less of a concern in China than in the US due to weak governmental restrictions and the creation of a copycat culture (Harney, 2011). Thus, national culture may influence how security behaviors are learned in different nations. Because national culture subsumes organizational culture and IT culture (Leidner & Kayworth, 2006), national culture is likely to influence the relationships between social learning from childhood and throughout an individual's employment. Thus, we propose:

*Proposition 5: Social learning takes place in cultural and political national environments. These environments influence what is learned and what is considered deviant or compliant.*

## **CHAPTER V**

### **THE QUALITATIVE STUDY**

#### **Research Design**

ASLT consists of four primary variables: definitions, differential association, differential reinforcement, and imitation. Although the process of social learning may be similar in different settings (Hwang & Akers, 2003; Jensen & Akers, 2003; Wang & Jensen, 2003), the content of definitions, influential peers, and reinforcement mechanisms may differ across contexts. Few studies examine ASLT in organizational settings (Ruiz-Palomino & Martinez-Cañas, 2011; Zey-Ferrell & Ferrell, 1982), and no behavioral InfoSec studies empirically examine ASLT in organizational settings. Given the lack of rich data concerning ASLT in organizational settings, we qualitatively explored definitions, influential peers, and social reinforcement mechanisms in relation to information security in organizations. We also explored the possibility that other constructs beyond the four mentioned in ASLT influence information security attitudes and behaviors. Further, we seek to explore the relevance of ASLT with regard to compliant behavior. Traditionally, ASLT has been used as a theory of deviance. However, it assumes that deviant and compliant behavior are both learned phenomena.

An interpretive study was conducted using semi-structured interviews to explore employees' beliefs and behaviors related to rules and information security. This is a first step toward determining the applicability of ASLT to behavioral InfoSec research. To

ensure that we were open to other possible explanations of information security beliefs and behavior, we examined other theories besides ASLT. Exploring multiple theories before conducting a qualitative study and coding data helps to sensitize researchers to a variety of perspectives (Glasser, 1978). This sensitization process helps to minimize potential bias and one-sided perspectives during data collection and analysis, and provides a greater number of codes to consider while analyzing the qualitative data (Glasser, 1978, 1992). We examined a number of other theories, including: general deterrence theory, protection motivation theory, fear appeals theory, habit theories, rational choice theory, and Bandura's social learning theory. We also considered the dimensions in Lange's (Lange, 2008) typology of corruption controls. The sensitization process provided us with new codes other than those provided by ASLT. Additionally, some codes emerged from the transcripts that were unrelated to any of the aforementioned theories. Thus, we were open to new concepts derived from the respondents' perceptions as well.

Before collecting large amounts of data through interviews, we pre-tested the interview questions with a panel of three information systems professors and one sociology professor. The pre-test was used to ensure the questions were understandable and likely to elicit relevant information. Based on the review by the panel, some changes were made to the initial set of questions. The primary list of questions are presented in Table B-1 in Appendix B.

After pre-testing the survey questions, we conducted three pilot interviews to ensure that the questions elicited pertinent information. After conducting the three pilot

interviews, we added some new questions pertaining to topics we had not considered. Respondents directed our attention to different explanations of their beliefs and behaviors. To allow each respondent to direct the conversation toward new topics, we started and ended each interview with a broad question asking the respondents how they believed their information security beliefs and behaviors developed. Because we used a semi-structured interview, we were able to explore some of the novel perceptions the interviewees mentioned, while still maintaining consistency in the topics that were discussed.

### ***Participants***

We interviewed 20 individuals (Creswell, 2007) who work in organizations to identify different information security beliefs and behaviors. The participants were selected to highlight a diverse set of perspectives. To explore the extremes of pro-security beliefs and behaviors, we interviewed employees who work for the information technology (IT) function of the organization. To explore less extreme pro-security beliefs and behaviors, we interviewed employees who use IT, but who are not strongly tied to the IT function. Security concerns are directly related to the job responsibilities of many IT employees. However, security concerns are relatively less important to non-IT employees. Thus, we expected IT employees to provide more extreme pro-security perspectives and non-IT employees to provide relatively less extreme viewpoints. Table 1 presents the number of IT and non-IT employees that were interviewed.

**Table 1. Number of Interview Participants Based on Employee Type**

Type of Employee	Number of employees
IT employee	10
Non-IT employee	10

*Data Collection and Analysis*

Data was collected through interviews with organizational employees. Employees were selected from a broad set of industries, but due to the sample size, we did not use stratified sampling or other advanced sampling techniques. These methods are more appropriate for quantitative survey research and not for qualitative studies. We used theoretical sampling to identify respondents. For example, we sought to interview employees in IT and non-IT industries. Theoretical sampling seeks to identify respondents that should differ on key attributes or perspectives based on some condition. Theoretically speaking, one would expect employees in an IT industry to have a greater knowledge of and closer ties to information security than employees in a non-IT industry. In some instances, our selection of individuals was purposeful to identify a diverse set of beliefs and behaviors. We employed several recruitment methods to identify participants. First, we recruited personal contacts who were known to hold different rule-related beliefs and behaviors. We also asked respondents for the names of others with unique perspectives on rules and policies. In addition to these recruitment methods, we also posted recruitment messages on LinkedIn. Finally, we recruited some interviewees using Amazon Mechanical Turk. Respondents recruited through Amazon Mechanical Turk were paid ten dollars for the interview. While Amazon Mechanical Turk is a new recruitment method, it is found to provide a diverse population of respondents

(Buhrmester, Kwang, & Gosling, 2011; Mason & Suri, 2012; Paolacci, Chandler, & Ipeirotis, 2010).

Interviews lasted between 30 to 75 minutes. Only two interviews were shorter than 45 minutes, and most of the interviews were 55-60 minutes. Interviews were conducted in-person, by phone, and via Skype. The interviews were transcribed using the Express Scribe transcription software. Table B-1 in Appendix B presents the semi-structured interview questions asked to participants, along with some common follow-up questions that were asked.

## **CHAPTER VI**

### **RESULTS OF THE QUALITATIVE STUDY**

Open coding (Corbin & Strauss, 1990) was used to determine the emergent, low-level codes in the interview transcripts. Axial coding (Corbin & Strauss, 1990) was then used to determine how the low-level codes related to form higher-level themes. Axial coding was also used to determine how the different themes relate to one another. NVivo 10 was used to code the interview transcripts and combine the low-level codes into larger themes.

#### **Qualitative Themes and Codes**

Through open coding, 50 different codes were identified. Through axial coding, the 50 codes were grouped into nine high level themes. The nine themes include: individuals' security-related values, individuals' beliefs and behaviors regarding rules in general, individuals' beliefs and behaviors regarding information security policies, individuals' beliefs about authority, behavioral influencers, the workplace environment, and major events. Each of the nine major themes is described briefly and the frequency with which they occurred across interviews is provided in the following sections. Following the description of each theme, the manner in which the themes relate to one another is considered later. Table 2 presents the major qualitative themes.

<b>Table 2. Major Qualitative Themes</b>
Major Themes
Security-related values
General rule-related beliefs
General rule-related behaviors
Information security policy beliefs
Information security policy behaviors
Authority-related beliefs
Behavioral influencers
Workplace environment
Major life events

### ***Security-Related Values***

Throughout the interviews, respondents brought up values related to information security. Most of the values directly supported individuals' efforts to follow policies and protect confidential information. However, three of the espoused values may be related to insecure behaviors. For example, respondents noted that they valued utility and personal convenience over security. These respondents felt that security interfered with their ability to perform their work responsibilities. They valued their other work responsibilities over their security responsibilities. Respondents also noted that they valued trust among their coworkers. These respondents felt that their coworkers would not abuse their systems, and therefore, they were less cautious with their computer systems, such as allowing coworkers to use their computers unsupervised. They were also less critical of their coworkers' negligent or rule-breaking security behaviors, because they felt that their coworkers would not do anything to harm the organization.

The most frequently cited value was that of protecting others. Eight respondents noted that their security behaviors were guided by a desire to protect others. Discussion

of protection was most prominent from respondents who worked with potentially at-risk clients, such as elementary students, clients of nonprofits, healthcare patients, and clients of financial firms. Other frequently cited values that support strong security behaviors are: a concern about information privacy, respect for others and for authority, and a desire to do no harm to others. Table 3 presents the codes related to security-related values.

<b>Table 3. Codes for Security-Related Values</b>	
<b>Code</b>	<b>Quote</b>
Do no harm	Generally, if I broke some kind of rule that was important, I would find out that it was important by the repercussion of it. If it was just sort of a punitive response, I didn't really see it as a big deal. If it seemed to hurt someone or someone's feelings, that was a big deal. And that always would impact me in a meaningful way.
Honesty/obedience	I signed the acceptable use policy like everyone else did. I should also have to follow the rules, even if it is just on the honor system.
Privacy	It is personal information and I believe that personal information should be kept safe. I would want someone who had my personal information to keep it safe.
Protection of self and others	I feel like security is important, because it... in a lot of circumstances it keeps a lot of people safe, particularly in the situation where you deal with unaccompanied minors. Sometimes there are custody issues with children and someone's name is not on the list of people we are allowed to release the child to.
Respect for others/authority	When I was growing up we were taught respect for our elders.
Responsibility	Being employed at the one web development company gave me a sense of ownership over my systems. That probably gives some strength to the security side. Yeah, a sense of responsibility. That's why I do frequent backups so that if anything blows up I can get us back to at least the day before.
Safety/Caution	I felt uncomfortable. I don't think it is really safe to use that when there are other things you could use.

*Trust of others	Like trusting. I was raised... I grew up in a really small town and you knew everybody and you trusted everybody. And you can't do that on the Internet, because people are not trustworthy. And that is hard for me, because I want to give people the benefit of the doubt and think they are good.
*Utility/Convenience	Some policies are being changed now which make it more difficult to do my job. And of course that is the eternal tradeoff between security and utility. I work for a group on in the organization that is interested in utility, and only cares about security as a risk factor. So, that is the attitude that I take. I figure I want to minimize the risk to my group and let us get as much done as we can up against these policies that are intended to protect the organization, clients, and employees.

\* Refers to a value that may support insecure behavior

### ***Beliefs and Behaviors Regarding Rules, Policies, and Authority***

Respondents spoke frequently about security beliefs and security behaviors. Beliefs were coded into the beliefs of the respondent and the beliefs of those close to the respondent. Beliefs were broken down further by whether they favored compliance or noncompliance with rules. Finally, beliefs were coded as relating to rules in general or to security policies in specific. Similarly, Behaviors were coded into the behaviors of the respondent and the behaviors of those close to the respondent. Behaviors were further coded as compliant, noncompliant, or ignorant (i.e., the person was unaware of the rule violation). Finally, behaviors were coded as related to rules in general or to security in specific. Respondents spoke readily about the beliefs and behaviors of others. They also spoke openly about their own beliefs and behaviors. Table 4 presents the codes related to the beliefs and behaviors of the respondents.

**Table 4. Codes for Beliefs and Behaviors**

Code	Quote
General rule beliefs	
Others' beliefs	
In favor of compliance	I guess I would have to say that, in general, they demonstrated and taught me that rules are in place for a reason.
In favor of noncompliance	I think for him, it was a lack of respect for people and a feeling that he wanted to do... he wanted that feeling of freedom. He didn't want to have any limitations.
Personal beliefs	
In favor of compliance	You follow them. I was a rule follower. I followed after my parents. I followed what my parents said very good for several reasons. First, it was just pounded into me when I was a kid. You know... over and over and over and over. I think that sticks with you. But nonetheless, I still thought about things and thought about, "is this a legitimate rule that I want to follow." And if I didn't want to follow it I just did what my dad said, I said "okay well, I don't think this rule applies to me or it shouldn't; it should be changed." And then I would just talk to people and try to get in changed. And a lot of times you would be surprised that there is a lot of flexibility in there.
In favor of noncompliance	I don't like a lot of laws. I think we over legislate. A great deal of our laws... when I was growing up, seatbelts weren't required and we lived. It has been legislated to the point of ridiculousness. You know, kids are living at home now until they're 26 years old, which in my opinion is part of legislation. We don't allow kids to drink until they are 21 now, but we will throw them into prison when they are

	14. I think the laws and authority have their issues right now. We can't figure out whether a child is a child or an adult. And we need to fix that a great deal. I also can't stand driving laws. I get pulled over for 100 different things that are all because someone has sued someone else.
Security policy beliefs	
Others' beliefs	
In favor of compliance	I think a lot of that had to do with the nature of the business. When you deal with these things, if you identified a security loop hole, you wanted to make sure it was covered, so everyone took it very seriously. It was our job to make sure that the stuff in there was safe. And if there was anything that you could think of, you would bring it up and everyone brought it up.
In favor of noncompliance	They are so bad. They totally sign [the security policy]. They don't read it. And even after you explain it, they totally don't do it. The other week they were sharing account information for running credit cards. I was like, "really... tell me why you are doing that. Don't do that. This is a temp, the person is going to leave the company." So they think it is a bunch of fluff. They don't understand. They aren't thinking about how somebody might use the information maliciously. They are just thinking, "oh, I've got to get my job done. I want it to be easy. So, when I'm gone I'm going to make sure that Sally down the hall has my password so she can log in as me so they don't have to contact us."
Personal beliefs	
In favor of compliance	I think it is important. Sometimes it makes me mad when I can't get a picture of a national park, but I can't get

	it because it is blocked. Or if I need a picture of an animal that's kind of irritating. But I understand why it is there.
In favor of noncompliance	We've been dealing with Sarbanes-Oxley for years. And just the paper trail and all of those changing of records based on Sarbanes-Oxley they have in place. It has been a nightmare to implement policies for things that happened in the past. If I can fit them in, I do, but if I am pressed for you... you know, legislative policies do fall by the wayside to get things out the door.
General rule behaviors	
Others' behaviors	
Compliant behavior	It was pretty straight cut about being a child and knowing what the rules were and stuff. And I think for them as citizens it was the same. They were pretty honest. So they just followed the rules.
Noncompliant behavior	He was always just pushing his boundaries, always pushing the limits. Talking back, not just to my parents, but to his teachers. He was a really bad trouble maker in school. He had multiple run-ins with the police. Not just when he was younger, but when he was a bit older as well.
Ignorant/unaware behaviors	N/A
Personal behaviors	
Compliant behavior	I've always been a bit of a rule follower in certain aspects of my life.
Noncompliant behavior	There is a threshold to things that I can do that I know I'm not necessarily going to get in a lot of trouble for. So let's say if I'm late for an appointment and I have to drive ten miles over the speed limit to get there, that sort of stuff I'm okay with, but that's about where I draw the line. Things that I know that I'm in control of, but aren't necessarily

	going to be endangering anybody or anything like that.
Ignorant/unaware behaviors	N/A
Security behavior	
Others' behaviors	
Compliant behavior	The sales people couldn't care less. They are completely indifferent. They don't live on a computer a lot like the rest of us do. Any rules that they enforce, they go right along with because they're really indifferent. As far as management goes, they'll do whatever we tell them to do as well. So if we notice any trends or any issues that they should be made aware of they'll follow them pretty closely.
Noncompliant behavior	Frustrating, very frustrating. Really frustrating. Some of the stuff is pretty major, like sharing the credit card information to run the credit card. Things like that are insecure. That's hard. Some of it is minor. But it can also be damaging. Streaming music... it is written in the policy that you are not supposed to stream audio or video. We have that written in there because we scale the Internet connections for a certain speed based on the number of people that are there and the data usage we expect. If we have ten people who are streaming, it is going to take the network down.
Ignorant/unaware behaviors	But I think a lot of it to was done out of ignorance. I think a lot of the people in the department didn't realize or understand the need for security or maybe the critical nature of it. You know if they do something, what are the ramifications if I don't follow this protocol.
Personal behaviors	
Compliant behavior	

	Well I followed the rules 100% and I tried to educate others about not just the rules, but about why the rules are there. Because you can tell someone not to do something all day long, but unless they know why they shouldn't do it, they are not going to listen to you. And so I played more of the role of, "this rule is here for this reason and here is why."
Noncompliant behavior	Basically, going from the large company with these very strict rules very much kept me on the straight and narrow. I had two computers up at all times. Now, I don't have two computers anymore. Now I just have two monitors running from one computer. It is company equipment. I am a remote employee still. I flew out there and got the computer and that is what I work on. They have very relaxed rules, so I do what I want. And I probably do things that I shouldn't do, like Amazon Turk. I'll see something out there interesting and I'll take a half-an-hour break and do that. And I do that on my company's equipment because it is not monitored.
Ignorant/unaware behaviors	I think that anytime that I was doing something that maybe wasn't appropriate from a security standpoint was out of ignorance about the issue as opposed to blatant disregard to rules around security.
Beliefs about authority	
Obey/respect authority	Respectful. You should always respect a person in a place of authority. And maybe not just authority, but all people. They taught me to be respectful of all people. And specifically an authority figure. You don't go in when you are upset with someone and go in there yelling and screaming and carrying on about something. You walk in calmly

	and talk to people. You talk to them the way you would like to be treated.
Challenge authority	Honestly, authority is the last gang in town. I don't have any respect for authority whatsoever except for its ability to influence my life. I don't think that because something is authoritative or has authority that it deserves any respect. I think that respect is earned in whatever relationship that I have with my government or my boss or whatever.

### ***Behavioral Influencers***

Respondents discussed many factors that influenced their own beliefs and behaviors regarding information security. The major themes that arose from the interviews included: respondents' observations and experiences with punishments and rewards; respondents' observations and experiences with security breaches; the social influence of family, friends, coworkers, and managers; and mass media and books. As discussed later, each influencer influenced individuals differently. Although all respondents discussed punishment, not all respondents were strongly influenced by punishment. Thus, the strength of an influencer was dependent on the individual's values and beliefs. This is described more in later sections. Table 5 presents the codes related to behavioral influencers.

<b>Table 5. Codes for Behavioral Influencers</b>	
<b>Code</b>	<b>Quote</b>
Consequences (rewards and punishments)	The reward is that you get to keep the job. The punishment would be suspension or temporary reprimand and if you did it twice violating any of the

	policies you were eligible for possible termination.
Experiences with security breach	
Others' experiences	Growing up I had friends of the family that had their identity stolen. When the friends of the family got hit by some scammers, a lot of things, a lot of activities got locked down when I was little.
Personal experiences	As much as we could tell, someone had stolen a lot of credit card numbers from the bank that I bank with and they do the card numbers sequentially. So they just took a bunch of numbers and signed up some people on there. That way when the bank issued you a new card, the number was still on there. It was pretty sneaky. I never thought that I would be the victim of something like that, because I am paranoid.
People	
Family	My parents have just been very straight arrowed. Good credit, follow the rules, do what you are supposed to.
Friends	My parents had purchased me one. I stayed up that night and learned how to program. I was one of the 3 or 4 geeky kids in middle school and high school who actually had a modem. I was that kid that would sit around and do printouts of girls breasts based on a character only printing. So it was in the 7th grade that they gave me a computer. So me and some of my friends did that. A buddy of mine in 8th grade actually wrote a book. You know, I hung out with them. That was my circle of friends.
Coworkers	She has a lot to do with how I... she has taught me about how to use computers. As soon as she hears something new she comes and tells me. I am one of the first to know about stuff.

Managers	He wrote [the security policy]. He is extremely technical. He is also the typical computer tech. He is the type to sit in a dark room and they would prefer never to talk to anybody. That is kind of him. And he is great at it. He is fantastic at it. But part of the problem is that the policy was written by him and the users don't always understand it because it was written in geek-speak, and they don't know what SSH is and they shouldn't, they are users. You know, they don't use it as a tool. They don't need to remote into a server. The policy is very thorough because he spent a lot of time on it.
Media	
Books	One of the books that most influenced my thinking along these lines is <i>The Moon is a Harsh Mistress</i> by Robert Heinlein, which I read several times a year in middle school and about once a year since.
News	And the news. You know the circumstances you hear through the news. That probably is a big part of the perception of security or reason to stay security.

### ***The Organizational Environment***

Another major theme that arose from the interviews was the workplace environment and individuals' roles within that environment. Some work environments were configured to support strong security behaviors, while other environments were not structured to support strong security behaviors. Strong security behaviors were supported by the existence of formal and informal policies to guide security behavior, the regular dissemination of security policies, security training, and normative and top management

support. Other factors that influenced the perceived importance of security included: the industry, organization size, external threats to security, and the sensitivity of the information an organization maintained. The job responsibilities of the respondent was another contextual theme that influenced the respondent's beliefs and behaviors pertaining to information security. Table 6 presents the codes related to organizational environment.

<b>Table 6. Codes for Organizational Environment</b>	
<b>Code</b>	<b>Quote</b>
Job roles/responsibilities	A number of job roles and responsibilities are represented in the interviews. Each interviewee discussed all of their jobs. Examples of job roles include: media specialist, regional manager, vice president of customer service, helpdesk, computer repair technician, data entry, network administrator, and zoologist.
Industry	A number of industries are represented in the interviews. Examples of industries include: manufacturing, primary education, higher education, information technology, and retail.
Organization size	A number of organizational sizes are represented in the interviews. These range from small, family owned companies to large firms with several locations.
<b>Policy</b>	
Formal	Well, the code of ethics comes from the school district. Each school is site based, so the principal gets to decide what they want to do. They have to follow the general rules of the district, but there are certain things that they make the decisions about at their school. So like, with our new principle, kids who have medical issues... they are telling not just the teacher that has that student but anyone who associates with that child. They started giving information about that child. So you know if they are diabetic and start having sugar issues then we're able to help them.

Informal	We kind of know that there are things that as far as from a security standpoint if we're going to play around with a machine that has like let's say for an example this is a recent example, dealing with machines that have the cryptal locker infection that target network drives using something like that we have the knowledge that machines like that have to be isolated. They have to be disconnected from the internet at all time. We have policies that aren't necessarily by the book or from a business perspective, but it's things that we've shared just through common knowledge that we've enforced amongst our group.
Dissemination of	I think that security was just one of those standardly worded policies, "read this, sign it, understand it, follow it." It's just one of those, "here's what you do when you sign on" and you probably never see it again.
Security threats	Over time as you see more and more issues, incidents, you learn more about the way technology works. I found that my perceptions of security have changed a lot. Because you realize the extent to which damage can be done to your network or to yourself, such as identity theft and stuff like that. So yeah, I think there is something true about the statement ignorance is bliss. If they don't know it is a risk, they go through their life and don't think about it. I wasn't in IT to begin with. I was a scientist. I got into IT about 10 or 11 years ago now. Once I started learning about it and seeing just how much people can do... Just simple website browsing, for example, people can see so much about what you are looking at. It is amazing to me. Over time, I think I have gotten a little more secure and quite frankly a bit more paranoid because I have seen what people can see.
Sensitivity of information	It has peoples' social security numbers, and their names and addresses, and other sorts of information... credit cards. Lots of personal information.
Top management support	What are peoples' perceptions of those. They think they are a bunch of fluff. Part of that is coming from upper management because upper

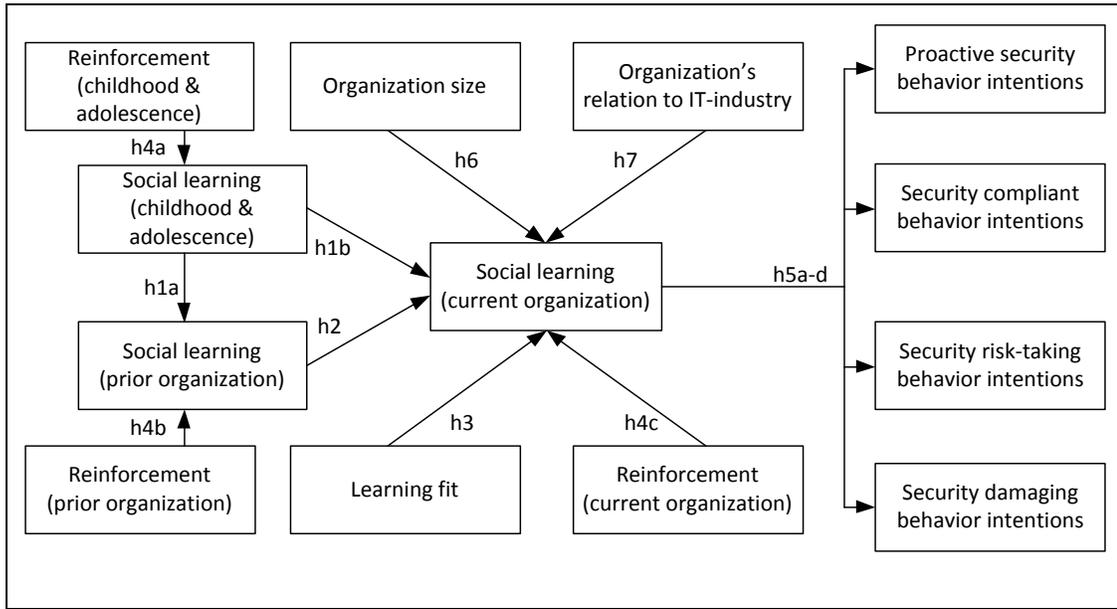
	<p>management doesn't care either. The vice president will send a 30 meg video over to his buddy next door in the office and they are like "oh, there shouldn't be any policies at all." Or we tried filtering and having proxy filters to filter out some of the sites that were being gone to. We got huge pushback from management. They said, "no, we don't want that. We don't want to block YouTube because I want to go to YouTube." On the one hand, they are telling us that they want us to be secure and protect the company, but on the other hand, whenever we try to set a new policy in place, we get a lot of pushback from management.</p>
<p>Training</p>	<p>We had like a meeting with the owner of the company and just kind of read over the rules that we should be abiding by. And we signed an agreement to follow the HIPAA laws. It was pretty short. Maybe an hour or less. And that was to go over every rule in the company. So maybe five minutes to ten minutes on HIPAA laws and stuff like that.</p>

***Major Life Events***

Major life events also emerged as an important theme in the interviews. The transition between different jobs was a major life event that influenced employees' security beliefs and behaviors. Respondents mentioned that they had made transitions to new jobs with different security policies and enforcement mechanisms. In certain circumstances, the transition from one work environment to another prompted changes in respondents' beliefs and behaviors. This is discussed further in later sections. Other major life events included moving away from family, and extraordinary successes related to information security. Major security breaches also had an important effect on individuals' beliefs and behaviors.

### *Summary of Themes*

The previous sub-sections briefly describe the major themes that arose during the coding process. Many of the themes are consistent with ASLT. ASLT studies focus primarily on deviant behaviors (Ronald L. Akers, 2009). Although we find that the social learning process proposed in ASLT fits violations of information security policy in organizations, we also find that ASLT is a useful model for studying proactive and compliant security behaviors. ASLT suggests that individuals learn values through differential associations that favor compliance or noncompliance. We see this across the interviews. This is described more fully in later sections. We also find evidence of positive and negative reinforcement for positive and negative security behaviors, further confirming the usefulness of ASLT for the study of compliant and noncompliant behavior. This is also described further below. Finally, we show in later sections that mimicry works in similar ways for compliant and noncompliant behaviors. These findings provide support for the use of ASLT in models of compliant and noncompliant security behaviors. We now examine how all the themes relate to one another. The following sections describe how the nine major themes converge into a larger model of information security beliefs and behavior. Figure 6 presents the model that emerged from the interviews.



**Figure 6. Emergent Conceptual Model**

### **Early Rule-Related Beliefs as the Foundation for Current Security Beliefs and Behaviors**

ASLT suggests that the general beliefs individuals adopt early in life about compliance and noncompliance are relatively stable and may guide individuals' rule-related behaviors through much of their lives (Ronald L. Akers, 2009). Further, the beliefs developed early in life may guide individuals to choose associations later in life with individuals who share the same value system, thereby reinforcing their early value and beliefs (R L Akers, 1990; Ronald L. Akers, 2009). By drawing from the rule-related narratives of the respondents, we find evidence that supports the general stability of rule-related beliefs. In every interview, respondents discussed their current beliefs in relation to the beliefs of their parents or adolescent friends. For example, one respondent noted:

My parents' perceptions of rules and laws were that you abide by the rules and laws. Your job is just to adhere to them. It's okay to question them. My dad specifically raised me to think about things before I did them. What if a law is immoral, for example? For example, segregation used to be a big issue during the civil rights movement. What do you do when the law is actually immoral? There are ways that you can go about changing that, but it doesn't mean that even if you disagree with a law that you can just ignore it or pretend like it is not there. If I disagreed with the rules my parents had, I could argue with them on it or bring information to them saying "hey this rule is incorrect, and here is why," but they had the authority over me to say "you have to follow that or you don't." So I learned that it was my job as a child to follow the rules of them and of other authority figures, like police officers and school officials. You follow the rules until they are changed. And if you disagree with them, you need to find a way to change them instead of just ignoring them.

Throughout the interview, this same respondent referred back to these same basic beliefs about compliance (i.e., rules should be followed, but they can be challenged through legitimized avenues). Later in the interview, the respondent noted:

You follow rules and laws. I was a rule follower. I followed after my parents. I followed what my parents said very good for several reasons. First, it was just pounded into me when I was a kid. You know, over and over and over and over. I think that sticks with you. But nonetheless, I still thought about things and thought, "is this a legitimate rule that I want to follow." And if I didn't want to follow it I just did what my dad said, I said, "well, I don't think this rule applies to me or it shouldn't; it should be changed." And then I would just talk to people and try to get it changed. You have to be willing to ask.

This example is not singular. Unless a major life event caused an individual to alter their general rule-related beliefs, the early influence of parents and adolescent peers continued to influence the respondents' rule-related behaviors later in life. As another example, another respondent noted:

There's not really any one conforming norm that I can think of that is outlandish for me to follow. You know, most people know what their boundaries are in a social aspect or in a political aspect. They know their place and that's kind of how I feel. I'm not really too into rocking the boat either. Kind of like my dad growing up. So I've got a lot of that from him. As far as authority and respecting people in their positions goes, I follow all of the same characteristics as my parents.

Individuals who associated with family members and peers that favored noncompliance early in life also held to these early beliefs. For example, one respondent labeled himself a latchkey kid. Both of his parents worked and he spent many hours alone and with friends. Many of his rule-related beliefs were influenced by the friends he associated with while his parents were working. He and his friends were part of the punk culture in a small town. He said the following about the early beliefs that he developed with his friends:

It was like, "make whatever rules you like and I'm going to do what I'm going to do." So we didn't steal from people. We did make mix tapes. That was part of the culture, but it wasn't like we were bootlegging or whatever. It was all more than a statute of limitations ago. And certainly, I wasn't doing any of that [sarcastically with laughter]. But then at the same time, the Sheriff's department would show up a lot of the times at the shows if it was inside city limits. And I would perfectly happily chat with the Sheriffs in front of the punk show. So while we were kind of dismissive about it, it's not like we were actively hostile. We sort of said, "well that's for you. These rules aren't for us. They don't help us. They don't make us safer. They don't make us better."

This same attitude toward rules and policies can be seen in his later descriptions of his attitudes toward security policies in college and at work. At one point, he noted:

We didn't think about [the security policies] at all. I mean seriously. We did whatever we wanted on the network. You know, there were others

with different perspectives, but my crew... our attitude was “don’t be a dick, and have fun playing around.” And that was kind of all of it.

Regarding the stability of his early beliefs, the respondent also noted how he felt no need to justify his nonconforming beliefs and behaviors. In fact, the respondent stated that he felt that he had to justify his conforming behaviors. The respondent said:

I feel like I have to rationalize my mainstream behaviors. So the fact that I work for a business says to me that I am part of the problem. I am churning out a bunch of capitalist types who are for the most part making the world a worse place by espousing a value system that I don’t hold. I look at the American dream of capitalism as a promise of eternal and constant growth... and the only model I have for that is cancer. I have to justify my mainstream activities and not my counterculture activities.

These and other examples can be seen throughout the interviews. Individual’s general beliefs about rules and about compliance and noncompliance are formed early and remain fairly constant. Similar to ASLT, the interviews provide evidence that beliefs learned early in life tend to be quite stable over time. We propose that early rule-related learning influences behavior and learning later in life such that general rule-related social learning early in life acts as a foundation for future behavior and learning regarding specific rules, laws, and policies. Based on this proposition, the following hypotheses will be examined further in the quantitative study:

*Hypothesis 1a & 1b: general, rule-related social learning encountered during childhood and adolescence influences security-specific social learning in organizational settings (prior organizations and current organization).*

## **Social Learning across Time**

Based on the responses from respondents, social learning was not completely stable across time. Beliefs and behaviors develop and change as events cause individuals to reassess their beliefs. In the interviews, two primary types of events emerged—major life events and continuous experiences. Major life events caused dramatic shifts in security beliefs and even general rule-related beliefs. Continuous experiences, however, caused subtle shifts in beliefs and behavior over time. The influence of major life events and continuous experience are discussed in the following sub-sections. We also explore one particular event because it was discussed frequently in the interviews—transitions to new employers.

### ***The Influence of Major Events***

Major security-related events emerged as an important theme in the interviews. ASLT does not specifically discuss the importance of major events. Rather, ASLT draws attention to the continuous reinforcement that individuals encounter over time. Major events, however, are sensational occurrences that are rare, but leave a lasting impression on the perspectives of the individuals who experience the events. Respondents discussed several major security-related events including: breaches of personal information (i.e., identity theft or theft of a credit card); large data breaches or security-related events at work; moving far from family into unfamiliar normative environments; and the introduction of new and extremely close social relationships.

Personal data breaches were mentioned frequently in the interviews. Personal data breaches included breaches of one's own information or breaches of a close family

member (i.e., parents or spouse). For example, one respondent had experienced a breach of personal health information. The respondent had served a proselyting mission for a Christian church. While serving on the mission, the respondent was struck by a car driven by another missionary from the same mission. One of the leaders of the mission took the respondent to a clinic. The leader insisted on being present in the examination room during the visit. The leader also invited the missionary who had hit the respondent into the examination room without receiving permission to do so. Additionally, the leader of the mission spoke with the doctor in private. The respondent said, “I don’t even know what they were talking about, but come on, that is private information. If she had influenced [the doctor] in any way, that is just not appropriate and it breaks HIPAA laws.” This event influenced the way the respondent viewed HIPAA rules. The respondent worked for a medical billing company and was very adamant about protecting her client’s healthcare information. She would not even describe the general types of information she had access to for her job. She stated that she protected the data so fiercely because of her own experience with a breach of medical information.

Experience with large data breaches and other security-related events at work may also cause dramatic changes in security beliefs and behaviors. Given that large data breaches are relatively rare, we only encountered one such event in our interviews. However, the example provides evidence that major data breaches at work can exert a strong influence on security beliefs and behaviors, particularly for those intimately involved in the event. One respondent worked for an organization in New York. The

organization was affected by the attacks on the World Trade Center on September 11, 2001. The respondent stated the following about the event:

I worked for a company well before 9-11. I was a computer operator at the time, but I was trying to work my way into programming. So, I developed a backup system which took all of their data, they were a securities firm, out of their in-house servers into what we called the mountain so that data would be secure. That company would not have been up and running the next day had those measures not been in place. So holding the data secure in that fashion and having a way to recover from an attack, either viral or external. That was very eventful.

The respondent later noted that the event altered his perceptions about how to protect computerized information. After the event, he was less concerned with preventing security breaches and more concerned with being able to recover from breaches. When asked toward the end of the interview what had been most influential on the development of his beliefs about security, he stated:

Like I said at the very beginning, 9-11 and developing that backup system. And you could see in my answers in talking about which way do I go, backup and recovery or prevention. It was definitely a massive influence on my life. I go with recovery.

Separating oneself from family or being introduced to family may also act as sensational events that trigger new perspectives on compliance and noncompliance. For example, one respondent was raised on military compounds as a child. He had been raised to follow rules strictly. While living with his family, he said, "I was on the straight and narrow path." Later in life, he moved away from his family to a large city more than

500 miles away. He moved to what he called a “hardcore neighborhood.” He said the following of the new area:

I lived in [city name], and I saw a great deal. I may have been the straight white-bred kid from the South where the kid across the street wouldn't even sell me pot because they thought I was a cop, but I lived in that environment. It was a hardcore neighborhood. It was hard to get by.

He stated that his experiences in the neighborhood and the behaviors and attitudes he observed from others in that neighborhood altered the way he perceived rules. Because of his experiences in that neighborhood, he changed his core perceptions of rules and laws. After living in the neighborhood he adopted a perspective very different from his early perceptions.

Similarly, introductions to estranged family members with different values may also exert a strong influence on core rule-related beliefs. One respondent grew up with her father who opposed rules, and associated with friends who rarely followed rules. The respondent adopted many of the perspectives of her father and friends. She had confrontations with police for breaking laws. However, later in life, she was reintroduced to her mother. She said the following of her mother:

She is 100% a law follower. I even looked up her record because I couldn't believe that anyone could be 100%. But she does not break any laws. It doesn't matter if she agrees with it or not, she is going to follow it. She won't associate with anyone that doesn't have the same beliefs as her.

The respondent later stated that her mother's influence in the latter part of her adolescence influenced her perceptions of rules and policies as she began working.

Reflecting on her mother's influence, the respondent said, "I had been so much into not really caring and breaking the law that I kind of wanted to take a new approach and do what my mom does as far as listening." The introduction of her mother who held vastly different beliefs than her father and friends, had a strong influence on the respondent's own beliefs and behaviors.

Based on the content of the interviews we propose that major security-related events and personal exposure to privacy and security breaches will influence social learning in favor of information policy compliance.

### ***The Influence of Time and Continuous Experience***

Although major events may exert a dramatic effect on individuals' beliefs and behaviors, time and repeated experiences with computers and continuous exposure to security beliefs also influences individuals' beliefs and behaviors. An individual's first experiences with security policies, particularly when the policies are strong and well-supported, have a positive influence of pro-security behavior. One respondent described her first experience working as an IT employee. She said that the position was very difficult because there was much to learn. She noted:

It was difficult at first, because it was a completely different mindset than I was used to. I hadn't thought about computers as being anything that anyone would ever try to get into. Why, why would someone try to get into someone's computers? I had never thought about it that way. You know I was kind of innocent and trusting.

Another respondent who worked as a customer service manager commented on her transition from the paper manufacturing industry to the IT services industry. The

respondent noted that the IT services company had many security policies and procedures that she was required to learn and follow. In a follow up interview, she said that she had not learned all of the security policies and procedures until six months into her tenure at the organization. The complexity of the policies and additions to the policies required a long socialization process. Thus, tenure at an organization can influence the adoption of norms. If norms require the completion of complex procedures, time is needed for the socialization process to have an effect on individual's beliefs and behaviors.

Although the first strong exposure to information security influences respondent's security beliefs and behaviors, prolonged exposure to security threats also influences beliefs and behaviors. The influence of prolonged exposure to security threats was particularly influential for IT personnel. One respondent who worked in IT noted:

Over time as you see more and more issues and incidents, you learn more about the way technology works. I found that my perceptions of security have changed a lot, because you realize the extent to which damage can be done to your network or to yourself, such as identity theft and stuff like that. I wasn't in IT to begin with. I was a scientist. I got into IT about 10 or 11 years ago now. Once I started learning about it and seeing just how much people can do... just simple website browsing for example. People can see so much about what you are looking at. It is amazing to me. Over time, I think I have gotten a little more secure and quite frankly a bit more paranoid because I have seen what people can see.

Another IT employee noted:

I say it's based mainly on my real world experience. The kind of line of work that I'm in I see a lot of people that suffer from things like not having sufficient protection, not practicing good habits, being susceptible to things like identity theft and privacy issues. So I've seen the whole gambit of different issues. So as time has gone on, what wasn't necessarily of importance to me has definitely grown to be, especially in the past few

years as phishing has really picked up and identify theft and things like that. So I'd definitely say that my work, and you know what I've seen and learned from others, has definitely influenced that quite a bit.

Based on the content of the interviews, we propose that individuals with continued exposure to computers over time, particularly the strong exposure experienced by IT workers, will be more likely to comply with security policy than those with less exposure.

### ***Job Transitions and Security Beliefs***

Job transitions were mentioned by all of the respondents. Job transitions included: transitions to new organizations and departments within the same organization, and major changes in practices and processes at one's current employer. Employees may not fully adopt the beliefs they encounter in these new contexts. Although organizational context influences the adoption of security-specific beliefs and behaviors as discussed in section 7.3, the beliefs and behaviors developed while working in previous jobs or working environments also influence respondents' current security beliefs and behaviors. That is, individuals carry some beliefs and behaviors learned in previous jobs or work environments to their current jobs or working environments.

For example, one respondent worked as a nurse for two different hospitals. The first hospital had strict internal policies and had strong norms that supported adherence to HIPAA rules. However, when she transitioned to the second hospital, the organizational norms and policies were less strict. When asked if the loose policies and norms affected her own beliefs and behaviors, she stated:

No. I think I kind of stuck with how I was trained. I did my schooling at [the first organization]. So that was just kind of the way I did things. I just kind of stuck to what I knew and what I felt was the best practice for the patient.

Later the respondent noted that she did not experience any negative consequences for maintaining her previously adopted values. Thus, her comfort with the prior socialization and the lack of consequences for not adopting the new norms created an environment where the respondent could select the beliefs and behaviors most comfortable to her.

Another respondent had previously worked for an organization with strong security policies and procedures. The respondent then transitioned to several organizations with weak security norms and policies. The respondent noted his frustration with the employees and managers he encountered at the latter organizations. Despite the lack of support from co-workers and management, the respondent continued to practice the secure behaviors he had previously learned. These examples show that social learning from previous organizations can influence the adoption of social learning beliefs and behaviors prevalent in one's current organization. Based on findings from the interviews, we propose the following hypothesis:

*Hypothesis 2: security-specific social learning encountered in prior organizations influences the adoption of security-specific social learning in an employee's current organization.*

These responses also demonstrate that individuals are more or less likely to adopt the beliefs and behaviors in their current organization depending on how well the

learning environment in the current organization fits their stable beliefs and behaviors.

*Learning fit* is the extent to which an individual's preferred beliefs and behaviors learned in previous life stages align with the beliefs and behaviors expected within a particular setting. Based on the responses, we propose the following hypothesis:

*Hypothesis 3: learning fit increases the adoption of social learning in organizational contexts.*

### **Explaining Differences between Early Rule-Related Beliefs and Current Security-Specific Beliefs**

Although rule-related beliefs learned early in life influence the development of individuals' policy-specific beliefs, policy-specific beliefs may also differ substantially from general rule-related beliefs due to context and circumstance (Ronald L. Akers, 2009). This was present in several interviews. In some contexts, individuals favored compliance, but in other contexts, individuals favored noncompliance. For example, one respondent learned early in life that rule violations were acceptable. During adolescence, the respondent had confrontations with police officers for her behavior. When speaking of security beliefs and behaviors, the respondent mentioned that she hacked software to see if she could accomplish the hack and to gain access to the software for personal use. When she was asked whether she tried to hack software at work as well, she responded:

No. I definitely don't try to do that inside of work, because there are people that will snitch on you and I am not one of the one's to tell my boss what I did. So, that is more of a... I'll give an example. Take [software name]. There is a tool kit that will crack your software and turn it into the full version of the software. And so, I did it. I know how to do it. I have the software, but I don't do it to other people's computers. Even though I

know it is still wrong; I know it is stealing. And yes, I still use the software. That is another thing that I can't explain. People follow certain things, but then they don't follow other things... But as far as out of work friends, I will be like, "hey guess what I just did. I turned this into a full software. Or guess what, I just got [software name] for two years because I did this."

Throughout the interviews this respondent described herself as being highly compliant with rules at work because of sanctions and her desire to be promoted. She even admitted to using the company's anonymous whistleblowing hotline to report the noncompliant behavior of her coworkers. Clearly, her security behaviors at home differ greatly from her security behaviors at work. Other examples of inconsistent and context-specific beliefs and behaviors can be seen in many of the interviews.

We now seek to identify some of the conditions that prompt the adoption of beliefs and behaviors that are inconsistent with individuals' rule-related beliefs learned early in life. To begin, the contextual nature of the core tenets of ASLT is explored. The following sub-sections describe how differential association, reinforcement, and imitation are influenced by context. Next, two aspects of context that arose from the interviews are discussed, namely organizational size and industry type. Finally, we describe how organizational size, and industry type influence security-specific learning.

### ***Social Learning: The Contextual Nature of Differential Association***

ASLT acknowledges that differential association is contextual in nature. That is, individuals come into contact with different beliefs about compliance and noncompliance in different contexts and with regard to different rules, which influences their rule-related behaviors according to the context. Although ASLT acknowledges the contextual nature

of beliefs, many ASLT studies only examine beliefs related to one rule and in one context (Pratt et al., 2010). Thus, the conditions that explain why differential association is contextual are not well addressed in the literature. Similar compartmentalization can be seen in InfoSec research. Most InfoSec studies are cross-sectional in nature (Crossler et al., 2013). The studies primarily seek to understand the behavioral influence of security controls in the respondents' current work setting, or to understand security beliefs and behaviors in that current setting. There is little consideration for how security beliefs develop outside of the current work setting. One exception is the study of habit in InfoSec research (Vance et al., 2012). However, even habit is examined broadly and does not try to account for where an individual's security habits were formed. Based on the interviews, we identify some of the conditions that create differences between general rule beliefs and security-specific beliefs. We also highlight those events that cause changes in security beliefs and behaviors.

Several respondents noted that the attitudes of their coworkers differed from organization to organization or even from department to department within the same organization. For example, one respondent discussed a transition he made from an organization with strict security policies to an organization with loose policies. He noted:

Basically, going from the large company with these very strict rules kept me on the straight and narrow. I had two computers up at all times. Now, I don't have two computers anymore. Now I just have two monitors running from one computer. It is company equipment. I am a remote employee still. I flew out there and got the computer and that is what I work on. They have very relaxed rules, so I do what I want. And I probably do things that I shouldn't do, like Amazon Turk. I'll see something out there

interesting and I'll take a half-an-hour break and do that. Their security practices are very relaxed.

Another respondent commented on his transition from one department to another within the same organization. He worked for the airline industry. He noted that the organization had policies that prohibited the use of the Internet for personal purposes while at work, such as browsing Facebook. The respondent stated:

Yeah, I've seen people access Facebook. That is a big one we've been asked not to access and I've seen people access it. I don't see the group of people that use to do it. I'm closest to the customer service group [now], but I used to have a job working outside on the ramp working with rampers. Working with them, they were always the ones going the backdoor ways in, using K-proxy or other web addresses to get into Facebook and email accounts. The one's I'm closest with [now], I don't see them violate the policies.

Another respondent transitioned to a different organization and a different department. She started in a non-IT position in a zoological research lab as a research scientist. However, she returned to school to study IT. She transitioned from the research lab to a data center. She said the following of the transition and the new beliefs she encountered:

It was difficult, because you have to think about things in a different way. There is no longer a walking away from the computer. There are repercussions for that. To go back into the datacenter, you had to know what the rules were and you had to know why the rules were in place. They went through all of that. It was difficult at first, because it was a completely different mindset than I was used to. I hadn't thought about computers as being anything that anyone would ever try to get into. Why, why would someone try to get into someone's computers? I had never thought about it that way. You know I was kind of innocent and trusting, and here I was like, well geez, you can do some real damage here.

These and other quotes show that individuals come in contact with different values and belief systems as they transition to new organizations and departments, and interface with others in the different social environments. Changes in organizational practices and processes may also engulf employees in different belief systems that may prompt adoption of new beliefs and behaviors. For example, a nurse respondent described the changes in rule-related beliefs and behaviors of her coworkers when her hospital transitioned from a paper-based patient charting system to a computer-based patient charting system. She stated that the transition brought their access of patient records under scrutiny, because access to the medical records became heavily monitored. The extra monitoring caused changes in the behaviors of the employees at the hospital. When asked about the transition from paper to computerized charting, the respondent noted:

I think that it was a learning curve for everyone. Because you are used to being able to pull out patient charts and look at this or look at that, and really know nobody is checking on you. It is not that they were doing anything wrong, but you know that information now is out there. Now, with the computerized charting and everything, every time somebody logs into that patient chart there is a record of that. Whereas, back in the day when we were just using paper charts it wasn't quite as obvious. But now anytime anyone logs into a patient chart there is a record of it. If nothing, it has gotten more secure than before.

### ***Social Learning: The Contextual Nature of Reinforcement***

ASLT, general deterrence theory, and rational choice theory all suggest that positive or negative reinforcement exert influence on individuals' beliefs and behaviors. Consistent with these theories, we find that reinforcement through punishment, shaming,

praise, and rewards influences individuals to change their beliefs and behaviors based on the contextualized reinforcement they receive.

For example, one respondent noted that he received drastically different levels of reinforcement while working for different organizations. At one organization, the respondent encountered heavy monitoring and sanctions. He said, “every keystroke that I ever took during my 17 years at that company are sitting on a computer someplace.” He spoke of the company as “big brother” and frequently stated, “big brother is watching you.” When asked about policies at the organization he transitioned to after working for the strict company, the respondent stated, “I have to have Skype. That is basically the policy. They’ve been in business for a bunch of years, but they really don’t have laid out policies.” Regarding the difference in reinforcement he received at the two organizations, the respondent stated:

Rule breaking and what not are more prominent in my current life, which is probably the real question that should be asked here. Now that I’ve moved on from that heavy duty, tight security to another small company with very relaxed security policies, what was that transition like? That is a more interesting answer.

Later the respondent suggested that his security behaviors became very relaxed at the less strict organization. He knew he would not be punished and that he was not monitored at the latter organization. He was willing to do things that he didn’t do at the previous organization.

Similarly, another respondent stated that she was comfortable violating a rule in one setting, but would not violate the same rule under different circumstances. In

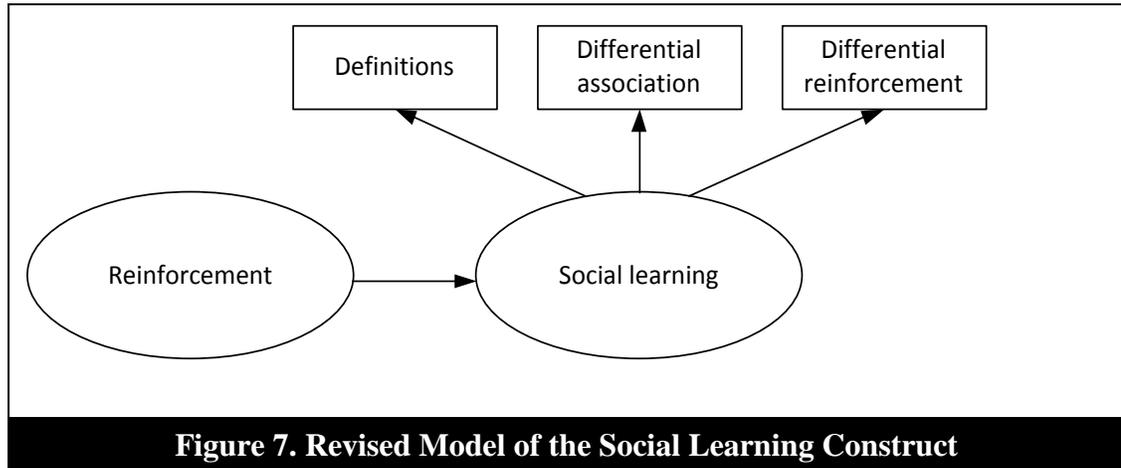
particularly, she was willing to hack software at home, but not at work. She suggested that her decision to hack the software at home was based on the lack of negative reinforcement. She noted:

Well the whole not stealing thing. I wouldn't go into the store and steal. I wouldn't go to my friend's house or parent's house to steal, but then when it comes to the whole breaking of the software for my own computer, yeah that is still stealing. Even though you know you are stealing from the company and maybe they are losing revenue and somebody is getting laid off, no one is in front of you. So you don't see who you are doing it to. It is kind of like out of sight out of mind.

Because the respondent didn't see the consequences of her hacking behaviors, she received no negative reinforcement for hacking the software.

Although differential association is somewhat contextual, differential reinforcement seems to be much more contextual. Organizations have very different reinforcement structures as do parents and friends. As shown in the quotes above, individuals experience different levels of reinforcement at any given time based on the context in which they are placed. Thus, individuals may behave differently at home and work because reinforcement is drastically different. Based on the highly contextual nature of reinforcement, we do not see it as part of the larger social learning system. However, differential reinforcement is highly influential on the adoption of social beliefs and behaviors as depicted in the quotes above. Thus, rather than modeling social learning as a process consisting of definitions, differential association, differential reinforcement, and imitation, we propose an alternative perspective that places differential reinforcement as

an external force that influences the social learning process. Figure 7 depicts the revised modeling of the larger social learning process.



Based on our findings regarding differential reinforcement, we propose the following hypotheses:

*Hypothesis 4a: differential reinforcement during childhood and adolescence influences social learning in childhood and adolescence.*

*Hypothesis 4b & 4c: differential reinforcement during employment at an organization influences social learning in the organization (prior and current organization).*

### ***Social Learning: The Contextual Nature of Mimicry and Modeling***

ASLT and Bandura's social learning theory both suggest that individuals learn by observing others behaviors and mimicking and modeling those behaviors (R L Akers, 1985; Bandura, 1977b). ASLT suggests that the importance of mimicry and modeling diminishes over time as individuals learn how to perform the actions they mimic (Ronald

L. Akers, 2009). However, mimicry and modeling can be extremely important when an individual is learning new behaviors. For example, one respondent reflected on her first IT position. She stated:

I was absolutely fascinated. They had people whose jobs it was to break into peoples' stuff. I was fascinated by that. They would do things like dress up like a worker out having a smoke break and try to break into peoples' offices. They would leave thumb drives that were infected with viruses out in the parking lot to see who would pick them up. People would pick them up and put them in their computers. The stuff they did it was astounding. I was completely fascinated by that and freaked out a little bit. They would call and try to get peoples' passwords. And if you left your computer unlocked, people would send a note out that you were buying drinks afterward. The amount of knowledge they had, it was just astounding. I was fascinated by computers. I knew I didn't know much about them. I had taken a few night classes, but here were all of these brilliant minds trying to find ways to break into systems or secure systems. And they were fighting back and forth. It was just these epic battles and it was awesome.

Speaking further, this respondent described the importance of her training with her coworkers:

When you started, you would get training from a manager, but then most of the training was done by your coworkers, because they were the real experts. Management was kind of the overseer, but they didn't know things quite the same. Sometimes you think that the manager is the expert, but it wasn't really like that there. The people doing it every day were the experts. So you would get initial training from them, but coworkers were the main ones who would help you understand the right mindset.

Many non-IT employees lacked the formal and informal training necessary to facilitate behavioral modeling. These employees' focused their conversation on password security and the requirements of acceptable use policies. In one extreme case, a

respondent mentioned passwords 20 times during the interview. Similarly, 60 percent of the non-IT respondents mentioned acceptable use agreements and limitations on visiting sites like Facebook. Only 30 percent of IT respondents mentioned the use of such sites. In many cases, training for non-IT employees was either nonexistent or consisted of reading and signing policies at the time the individual was hired.

While many non-IT employees didn't encounter strong formal training, some encountered strong informal training. For example, one respondent had learned about security behaviors through a colleague from the IT department. Formal training was weak. The respondent was required to read and sign an acceptable use agreement once per year, and she received occasional emails from the IT department about potential phishing threats. However, no formal training was in place to assist her learn other security responsibilities. Although she didn't encounter strong formal training, she received strong informal training through regular contact with the organization's only IT employee. The office of the IT employee was next to the office of the respondent. The respondent and the IT employee developed a good personal and working relationship. The respondent said the following of the IT employee, "She has a lot to do with how I... she has taught me about how to use computers. As soon as she hears something new, she comes and tells me. I am one of the first to know about stuff." The respondent stated that the IT employee had the greatest influence on her security beliefs and behaviors.

While many non-IT employees lacked sufficient training, a few employees received excellent training. One respondent worked in the IT services industry providing customer support for clients. The respondent's organization handled sensitive data for

several large businesses, such as Verizon and Walmart, through a software as a service architecture. Because of the sensitive information the organization handled, security was heavily stressed. The respondent went through an all-day training when she was hired and received follow up training on several occasions. Quality training and a strong culture that supports pro-security behaviors provides an ideal learning environment for individuals. By mimicking the behaviors of others and those behaviors taught in trainings, employees were able to perform their security behaviors well.

In the following sub-sections the core tenets of ASLT are presented based on insight from the interviews. Based on the discussion in the previous sections, we propose the following hypotheses for further testing:

*Hypothesis 5a: the likelihood that an individual will develop intentions to engage in proactive security behavior increases to the extent that the individual has been socialized to engage in positive security behavior in the individual's current organization.*

*Hypothesis 5b: the likelihood that an individual will develop intentions to engage in security compliant behavior increases to the extent that the individual has been socialized to engage in positive security behavior at the individual's current organization.*

*Hypothesis 5c: the likelihood that an individual will develop intentions to engage in security risk-taking behavior increases to the extent that the individual has been socialized to engage in security misbehavior at the individual's current organization.*

*Hypothesis 5d: the likelihood that an individual will develop intentions to engage in security damaging behavior increases to the extent that the individual has been socialized to engage in security misbehavior at the individual's current organization.*

### ***Contextual Influencers: Organizational Size and Industry Type***

The contextual nature of differential association and differential reinforcement is somewhat dependent on organizational size and industry type. Small organizations tended to have less strict security policies and enforcement mechanism than large, highly bureaucratic organizations. Similarly, organizations in IT-related industries tended to have stricter security policies and more enforcement mechanisms than organizations in nonIT-related industries. Some of these differences were quite marked. For example, one respondent worked for a small engineering firm with less than ten employees. According to the respondent, the organization's only information security policy was, "don't leak information." Even many small IT organizations had weak security controls. When asked about the policies at a small website design company, one respondent stated:

It was basically, get your job done and do it as best as you can. I wrote all of our code for a long time and then I kind of technically managed the folks who were writing code. I mean active code, not just HTML. And the attitude was, keep it as secure as you know how to keep it. We did not have a large number of policies. I think at our peak we got to maybe five people. The intention was to keep it a small close-knit group. Yeah, we were not policy oriented. We operated under the principle that 99 percent of your managing gets done when you decide who to hire. And that is the single best management technique I've learned. There are different constraints that you operate under in a big agency. But yeah, we just hired people that we knew weren't going to rip us off and that we could trust.

Similarly, another respondent who worked for a small computer repair shop said that he was surprised to learn of the weak security controls at the organization. When asked whether the policies at the organization were strict, the respondent stated:

No. Alarmingly, [the policies are] not strict. Every computer as it came into the shop was immediately connected to a network that had no security whatsoever. On top of that, they had a wireless network that had wireless access to that network that had no encryption at all. So, the second the computer got there, it was completely exposed to anyone who wanted to get to it. Plus it had total exposure to every other computer on the network; that includes the computers they used for their servers and other work computers. They seemed to understand that it was important to have some sort of antivirus. That was as far as they went.

Larger, bureaucratic organizations tended to have stricter policies, particularly organizations in IT-related industries. Speaking of her experiences across companies, one respondent noted:

I think it was mostly about the types of companies that I worked for. The two largest companies I worked for were the consulting company and the energy company. The energy company had exceptionally strict rules. They had all kinds of security issues because they are considered critical infrastructure in the United States. They had very stringent security policies, as stringent as the other place that I worked, the [IT] consulting firm. So, the larger companies have been very strict. The smaller companies haven't been. That is also probably related to the type of companies they are; a school district and a manufacturing company. My current boss is very smart, but from the company as a whole, we get a lot of pushback within the smaller organization. At the larger organizations, there is more at stake, and I think they choose specific people with the capacity to do that or to learn that.

Another respondent worked for a mid-sized, secure data center. She stated that policies were strict and that employees sought to make the policies even stricter. The respondent said the following about the support of security policies in that organization:

They would think about it, and if they didn't think that it was strict enough, they would find ways to improve it. I think a lot of that had to do with the nature of the business. When you deal with these things, if you identified a security loop hole, you wanted to make sure it was covered.

So, everyone took it very seriously. It was our job to make sure that the stuff in there was safe. And if there was anything that you could think of, you would bring it up, and everyone brought it up. Everyone took it real seriously. Everyone was interested in making it better.

Based on the interviews, we propose that employees in large organizations and organizations related to the information technology (IT) industry will be socialized to obey information security policies more than employees in small organizations and organizations unrelated to the IT industry. Thus we quantitatively test the following hypotheses:

*Hypothesis 6: the likelihood that an individual will learn deviant security behaviors decreases to the extent that the individual works for a large organization.*

*Hypothesis 7: the likelihood that an individual will learn deviant security behaviors decreases to the extent that the individual works for an organization in the IT industry.*

### **Trust among Coworkers**

Another important theme that emerged from the interviews was employees' trust in their coworkers. With regard to information security behavior, trust is a relatively understudied topic (Posey, Bennett, Roberts, & Lowry, 2011). Trust research in organizational contexts focuses on how employees' trust in their organizations influences the employees' behaviors. Trust among coworkers has not been studied as an antecedent to information security behaviors. In the interviews, we identified several instances in which trust in one's coworkers seemed to decrease adherence to information security policies. For example, one respondent related her experiences with information security

at a large paper manufacturing company. The respondent stated that security beliefs were relaxed and policies were ignored by many employees. While explaining why the environment was relaxed with regard to information security policies, she stated:

There were people who had been [with the company] for more than 24 years. A lot of people were there long term. I think that familiarity also breeds a little bit of... I'm not sure the word I'm looking for. Because we knew one another and worked together so long, you tend to become more relaxed because you trust people that they won't do anything that would jeopardize anyone's job; they wouldn't do anything to jeopardize the company knowingly. Once you understand that person, you trust that they will do what is in the best interest of the company without disturbing anything that shouldn't be disturbed, at least intentionally. I don't think they would intentionally disclose information without realizing the ramifications of that. So I think a lot of it has to do with the fact that we had worked together so long that over time we became accustomed to. I trust that they will do nothing to jeopardize the company or their job.

Because the respondent trusted her coworkers, she was not concerned with their relaxed security behaviors. Another respondent who worked in an elementary school shared a similar story. The respondent was employed as a media specialist and managed the school's library. The school had a policy that employees must log out of their computers upon leaving their workstations. They also had a policy that employees should not use another employee's computer account for any purpose. Although the respondent was careful to lock her computer when students' parents were at the school, she often left her computer unlocked to allow faculty members to check out books for their students. This action violated both of the aforementioned policies. The respondent said, "I really trust the people I work with." She further stated, "A lot of time I just trust that nobody's going to mess with my stuff."

In another instance, the hiring model of a company was based on trust. Formal policy was of lesser importance to the organization and its operations. The respondent who worked for the company stated:

Yeah, we were not policy oriented. We operated under the principle that 99 percent of your managing gets done when you decide who to hire, and that is the single best management technique I've learned. There are different constraints that you operate under in a big agency. But yeah, we just hired people that we knew weren't going to rip us off and that we could trust.

Based on the discussions of respondents, trust among coworkers seems to create a vulnerability in information security. Trust seems to focus the attention of employees on social norms rather than formal policy. Trust also seems to create a feeling of comfort and security, which may provide a false sense of security. Thus, trust among coworkers may lead to the development of weak security norms. Trust is not examined in this study due to the current complexity of the model. It also lies outside of the scope of the current study. However, it may be studied in future research to further confirm the findings in this study.

### **Managing Security Behavior**

Based on the interviews, a one-size-fits-all management approach may not be an appropriate solution to manage internal security risks. Employees' security beliefs can be categorized into two major groups. Employees expressed pro-policy beliefs and anti-policy beliefs. Pro-policy beliefs include beliefs that favor compliance with security policies, and in some cases, beliefs that favor engagement in extra-policy behaviors designed to protect the organization and its clients. Anti-policy beliefs include beliefs that

favor noncompliance with policy or strong negative perceptions of policy. In this study, anti-policy beliefs do not include malicious actions intended to cause harm to the organization. Although malicious behaviors have been identified as an important type of security behavior (Willison & Warkentin, 2013), we did not encounter malicious beliefs and behaviors in the interviews.

### ***Managing Employees with Pro-policy Beliefs***

Employees with pro-policy beliefs believe that following policies is important and that policies are “in place for a reason.” These employees also tend to believe in the importance of rules and laws in general. Respondents with pro-policy beliefs commonly labeled themselves as rule followers. As long as they understood the security policies, these respondents were eager to follow the security policies. Some respondents even stated that they felt uncomfortable in environments that did not support adherence to security policies.

Based on the respondents’ statements, employees with pro-policy beliefs required two forms of support to follow through on their pro-policy beliefs: training oriented toward awareness and skill development, and normative support. In the context of this study, *normative support* refers to the extent to which the organizational culture and social norms within an organization support positive security behaviors.

Security training was an important tool to strengthen pro-security beliefs and improve security behavior. Respondents who expressed pro-policy beliefs often blamed their security-related indiscretions on their lack of awareness. For example, one respondent noted:

I'm always more cautious anyway because I've had some experiences and I understand that... there are people out there that have intentions that are not necessarily good intentions. If they want to hack into your system they are going to hack into your system, but I don't want to participate by taking a relaxed approach to my security and making it any easier for them than it already is. I think that to the degree that I understand it and understand what to do to prevent it, I do that.

Unfortunately, as previously discussed, many of the respondents had not encountered strong training. For many respondents, particularly non-IT respondents, their knowledge of security was limited to the use of passwords and to acceptable use agreements. Based on the interviews, it seems that training can have a very strong influence on individuals with pro-policy beliefs.

Normative support was also extremely important to respondents with pro-policy beliefs. Employees with pro-policy beliefs felt most comfortable in environments where workplace norms favor compliance with policies. When the normative environment does not support policy following behaviors, employees with pro-policy beliefs find it more difficult to follow policy. This may be in-part because the norms become the policies that they follow. One respondent, a customer service manager, who labeled herself as a rule-follower explained the discomfort she felt in a work environment that did not support information security policies. While discussing the information security norms at a previous organization, she noted:

When you are in an environment and working with the same people long enough, they influence you in certain ways. I do believe that with the prevailing attitude [at my previous employer], I was a little more relaxed than... the truth of the matter was that because everyone was relaxed, and that was the prevailing attitude, there was really no way for me to enforce the policy when no one else was enforcing the policy. So I kind of ended

up going with the flow. As much as it sometimes bothered me, I felt like I couldn't really buck the system because there were people... if I were the only manager enforcing the policy then what does it matter? It would have made me the manager who was really coming down on people and being difficult, when in fact, if everyone were enforcing it, it would have been an easier thing.

IT employees in charge of information security shared similar sentiments. When IT employees are not supported by top management and the workplace norms do not favor compliance with information security policies, IT employees face major frustrations and difficulties. For example, one IT employee had moved from an organization which was highly supportive of information security to an organization that cared little about information security. When asked about the transition, the respondent noted:

[It is] frustrating, very frustrating. Really frustrating. Some of the stuff [they do] is pretty major, like sharing the credit card information to run the credit card. Things like that are insecure. That's hard. Some of it is minor, but it can also be damaging. Streaming music... it is written in the policy that you are not supposed to stream audio or video. We have that written in there because we scale the Internet connections for a certain speed based on the number of people that are there and the data usage we expect. If we have ten people who are streaming, it is going to take the network down. So sometimes it is fighting that battle. It is pretty frustrating and I feel like we fight the same battles over and over again, because people don't listen.

Respondents with pro-policy beliefs were particularly interested in following information security policies when they felt as though they were protecting a vulnerable client. For example, one respondent worked with small children. She believed that

following information security policies is extremely important. When asked if she thought that information security policies are important, she stated:

Yes I do, especially when you are working with young children. Especially working at an elementary school... you don't want teachers looking on child porn. That doesn't make it safe for the children. Yes I think security is an important part, especially where I'm working right now in an elementary school.

Two respondents working in the healthcare industry both noted that they felt it was their responsibility to protect patient privacy. They both claimed that they are careful to follow information security policies. Another respondent who worked for a non-profit organization that sought to protect women from spousal abuse felt strongly that following security policies was important, because it protected the organization's clients. Similarly, IT employees, particularly those who are in charge of security, also felt an increased need to follow policies. They felt it was their responsibility to protect the organization from internal and external threats.

### ***Managing Employees with Anti-policy Beliefs***

Multiple respondents noted that they did not believe that some information security policies were important or necessary. Although these employees expressed anti-policy beliefs, they did not always violate the policies. Their anti-policy beliefs did not always result in insecure behavior because the respondents were influenced by organization controls. For example, one respondent stated the following about information security policies:

I believe some of them are unnecessary or violate your rights in other ways. So I still don't agree with most of them... well I wouldn't say most of them, because I understand why they are there. There are still 10 to 20 percent that I don't agree with. I follow them until they tell me not to.

Earlier in the respondent's life, her anti-policy opinions of security policies were even stronger. Other respondents shared similar sentiments. When asked about his perceptions of security policies, another respondent noted:

I think they are good. I think that most of them do solve issues, but once again, I see a bunch of policies come into place because of over legislation. We've been dealing with Sarbanes-Oxley for years, and just the paper trail and all of those changing of records based on Sarbanes-Oxley they have in place. It has been a nightmare to implement policies for things that happened in the past. If I can fit them in, I do, but if I am pressed for, you know... Legislative policies do fall by the wayside to get things out the door.

Respondents with anti-policy beliefs were those individuals who were influenced early in life to believe that rules were unnecessary or who were influenced later in their lives to see rules as negative because of major events. Employees with anti-policy beliefs stated that they followed policies to avoid negative consequences. In most cases, values of protecting others were less important to these respondents. These respondents were primarily concerned with their own well-being. These respondents spoke regularly of monitoring and sanctions. For example, one respondent spoke about sanctions and monitoring on several occasions. In one instance, he stated:

They monitored our usage and stuff and then if you were caught you would lose your computer privileges. If you misuse your computer they will fire you. Like for pornography or for religious purposes. There is

zero-tolerance on that. They send a monthly Internet usage... sites we've visited.... what we're looking at.

Another respondent admitted to violating several information security policies while he worked for an organization with weak policies and enforcement. However, he stated that he was highly compliant with policies while working for an organization with monitoring and severe sanctions. Similarly, yet another respondent admitted to avoiding rules because he could avoid consequences. The respondent worked as an IT employee in an organization with a federated IT governance structure. The respondent worked for a department of the organization that "is interested in utility, and only cares about security as a risk factor." He avoided working with the personnel in the centralized IT department who were more process and rule oriented. Regarding the centralized IT department, he said:

The central IT group is very much process driven. At least from the outside, it seems to be a very process driven organization. And they need to follow [policies] to get it to work the way they want it to work. That is not to say that there are people there who might have different attitudes, but they have to live there. They have to follow the policy and the rules or whatnot. I do as much as possible by myself rather than relying on the central IT group or another unit. My reaction to their process driven and more reasoned way of doing things is, "well I'll just do it. Get it done." So yeah, disengaging, that is my way of dealing with it. If their system won't do it, I'll just find another way that will work.

The respondent also noted that the enforcement of policy was weak at the organization. The respondent shared several stories in which employees made large security-related mistakes, including major data leaks, but were not terminated or

reprimanded. In fact, the respondent suggested that one of the employees was promoted to remedy the error that he had created.

Based on the interviews, employees with anti-policy beliefs were best controlled by highlighting the consequences of insecure behavior. When strong, negative consequences were not in place, employees with anti-policy beliefs were far more likely to engage in insecure and policy violating behaviors. Again, hypotheses could be generated based on these findings. However, they go beyond the scope of the current paper and should be considered in future research.

## **CHAPTER VII**

### **THE QUANTITATIVE STUDY**

To further validate the findings from the qualitative study, a quantitative study was conducted. An online survey with Qualtrics survey software was administered to determine how generalizable the qualitative findings are. The online survey was distributed through Amazon Mechanical Turk. Amazon Mechanical Turk is increasingly used in academic research to reach a diverse population at a reasonable cost (Buhrmester et al., 2011; Mason & Suri, 2012; Paolacci et al., 2010). The demographics of Amazon Mechanical Turk respondents is similar to those found in other types of studies (Buhrmester et al., 2011; Mason & Suri, 2012). Panels, such as Amazon Mechanical Turk users, may also provide a greater diversity in respondents than convenience sampling methods, such as surveying the employees in a single organization (Posey, Bennett, Roberts, et al., 2011). Recruitment on Amazon Mechanical Turk was limited to respondents from the US and India. Before distributing the survey to the Amazon Mechanical Turk panel, the survey instrument was pre-tested and pilot tested. The instrument was pre-tested with three information systems professors, one sociology professor, and three information systems Ph.D. students. After making some adjustments to the questions based on the pre-tests, the survey was pilot tested on a group of undergraduate students in a business school in the Eastern United States. Based on more than 100 responses, the pilot test showed that the instrument exhibited high reliability and

strong validity. After pilot testing the instrument, the survey was administered to the Amazon Mechanical Turk panel.

The survey included three items to ensure that the respondent was reading carefully. For example, one item stated: Please select “Strongly Agree” for this question. These questions were used to identify respondents whose answers were haphazardly provided. If respondents failed these attention traps, they were removed from the sample. Similarly, we filtered for respondents who had worked in at least two jobs and who used computers at work multiple times per week. The US sample consisted of 384 responses. However, 137 responses were dropped because of incomplete surveys (9 percent), failing the filters (42 percent), or failing the attention traps (51 percent). The India sample consisted of 452 responses. However, 277 responses were dropped because of incomplete surveys (13 percent), failing the filters (35 percent), or failing the attention traps (52 percent). In the US sample, 64 percent of the responses were retained. In the India sample, 39 percent of the responses were retained (25 percent difference across samples). The difference in the number of responses dropped may be due to differences in comfort with Amazon Mechanical Turk. Participants in the India sample may have been less familiar with the platform, and therefore, more likely to fill out the survey when they were unqualified. By consistently applying our filtering methods across samples, the equivalence of the samples was strengthened.

### **Exploring Social Learning Internationally**

The overall social learning process is consistent across national boundaries (Hwang & Akers, 2003). However, because certain nations exhibit different value

systems (e.g., individualism vs. collectivism) (Hofstede, Hofstede, & Minkov, 2010), aspects of the learning process, such as how influential social learning is on behavior, may be more pronounced in different nations. It is also possible that political and regulatory differences across countries may influence social learning, particularly in relation to information security. Security is highly publicized in the US and many laws and standards have been developed. In other parts of the world, there are fewer security regulations. The lack of national concern and regulation may translate to lower security concern from the citizens of that nation. Additionally, IT infrastructure is different throughout the world. Some nations' IT infrastructure is relatively new. The citizens of these nations have had less time to learn security behaviors, simply because they have had less access to reliable computing devices and services. These differences are explored in this study at a high level by comparing the social learning process in the US and India.

India was selected for several reasons. First, the US and India differ culturally. Hoit is known to differ from the US culturally. According to Hofstede, the US and India differ in national culture along several cultural dimensions (Hofstede et al., 2010). For example, the US culture tends to be more individualistic, while the Indian culture tends to be more collectivist. Similarly, the US culture tends to exhibit lower levels of power distance than the Indian culture. Finally, the US culture tends to be more indulgent than the Indian culture. The indulgent, individualistic nature of the US culture and the low power distance may increase the likelihood of security behaviors that are contrary to policy as compared to India. Thus, the social learning environment in the US may be less

amenable to compliant behavior than the learning environment in India. However, India is also a developing country and IT infrastructure is still being developed (Palvia, Palvia, & Whitworth, 2002). The US, on the other hand, is an advanced country with a strong and stable IT infrastructure (Palvia et al., 2002). A developing infrastructure may result in lower levels of knowledge pertaining to information security, as citizens have less access to computing devices and services. Thus, social learning in favor of secure behavior may be increased in the US, simply because it is a more relevant social issue. The exploration of cultural differences offered later attempts to understand the larger social learning trends in the US and India.

### **Conceptual Model**

Figure 6 depicts the model that emerged from the qualitative data. The model is consistent with the premise of ASLT. Due to an error in the online survey, the industry of the organization was not collected. Thus, we were unable to test hypothesis 7. Hypothesis 7 was dropped from the model.

In addition to the relationships found in the qualitative study, we included other important constructs found across behavioral InfoSec literature. First, we included items to measure formal security training to understand how security training influences social learning. One of the purposes of this study is to understand how the formal administrative environment influences social learning. Although training was important in some of the interviews, training was weak in many of the organizations. Thus, we could not conclusively determine from the interviews whether training was a strong influence on

social learning. To determine the extent to which formal training influences social learning we propose the following hypothesis:

*Hypothesis 7: formal security training influences security-specific social learning.*

Second, we included self-efficacy, which is an alternate explanation of the effect social influence exerts on behavior intentions and behavior (Ronald L. Akers, 2009), stemming from Bandura's social learning theory (Bandura, 1977a, 1977b). Bandura's social learning theory has already been tested in InfoSec research (Warkentin et al., 2011). Thus, understanding whether self-efficacy provides a better explanation of behavioral intentions than Akers' social learning construct may assist researchers in selecting the most appropriate social learning theory for InfoSec research. Self-efficacy is also important in protection motivation theory (Johnston & Warkentin, 2010). Protection motivation theory also posits that response efficacy is an important influencer of behavioral intentions and behavior (Johnston & Warkentin, 2010). In the interviews, protecting others was a major value and rationale for engaging in secure behavior. Thus, social learning should influence perceptions of response efficacy.

Self-efficacy and response efficacy were added to the model as mediators. Social learning is the process by which values, attitudes, perceptions, and behaviors are shared and adopted. Response efficacy are perceptions that individuals may adopt. Given that social learning can influence values and perceptions of the environment, it stands to reason that social learning should influence how individuals perceive perceptions such as response efficacy. Further, social learning is a persuasive process by which individuals

are persuaded by social actors to adopt certain beliefs, attitudes, and behaviors.

According to Bandura's social learning theory, persuasion can influence perceptions of self-efficacy (Bandura, 1977b). Thus, we would also expect social learning to influence self-efficacy. The question remains, however, whether social learning has a stronger influence on behavioral intentions and behavior than self-efficacy. Thus, we seek to determine if a partial mediation relationships exists between social learning and self-efficacy with regard to behavioral intentions.

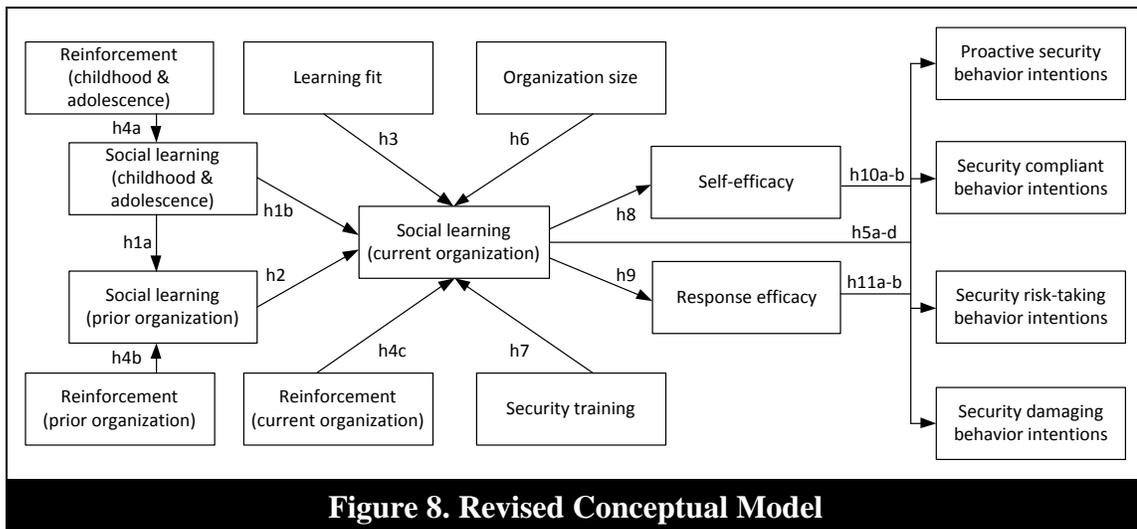
To minimize the number of measures in the survey, self-efficacy was conceptualized as self-efficacy to comply with security policy and response efficacy was conceptualized as perceptions of security policy and its ability to protect the organization. Thus, self-efficacy and response efficacy were included as an explanations for proactive security behavior and security compliant behavior. They were not included in the models for security risk-taking behavior and security damaging behavior. Protection motivation theory, which rely on self-efficacy and response efficacy, is used to explain positive security behavior (Johnston & Warkentin, 2010). Thus, they are not included in the models for negative behavior. Table 8 presents the revised conceptual model. Based on this information, we propose the following hypotheses in addition to those previously described in the qualitative section:

*Hypothesis 8: security-specific social learning influences self-efficacy to comply with security policies.*

*Hypothesis 9: security-specific social learning influences perceptions of response efficacy related to security policies.*

*Hypothesis: 10a-b: self-efficacy to comply with security policies influences individuals' proactive security behavior intentions and security compliant behavior intentions.*

*Hypothesis: 11a-b: response efficacy influences individuals' proactive security behavior intentions and security compliant behavior intentions.*



## Measures

The survey consisted of social learning measures derived from previous studies and adapted to the security context using insights from the qualitative study. The survey questions are provided in Appendix C. The questions captured the four major elements of the social learning process: definitions, differential association, differential reinforcement, and mimicry. These questions were asked three times with slight variations to measure social learning in childhood and adolescence, social learning at the respondent's previous job, and social learning at the respondent's current job. Randomization was used within question sets and question sets were also presented in a

random order to prevent bias due to ordering effects. The instrument also included several common security constructs, including: self-efficacy, response efficacy, the certainty of sanctions, and the severity of sanctions. The survey included four dependent variables to represent security behaviors, including: proactive security behavior, security compliant behavior, security risk-taking behavior, and security damaging behavior. Again, questions were randomly ordered and question sets representing each dependent variable were randomly order to prevent biases due to ordering effects. All questions were asked on a 7-point Likert scale. Finally, the survey contained demographic questions pertaining to age, job tenure, work experience, job position (i.e., are they a manager or an IT employee), and organizational size. Gender, and whether the employee was an IT employee and manager were coded with a dummy variable. Gender was represented as 0 for female and 1 for male. IT employees were coded as 1 and non-IT employees were coded as 0. Managers were also coded as 1 and non-managers as 0.

Social learning was measured as a higher order construct (Ronald L. Akers, 2009). The four dimensions of social learning include: definitions, differential association, differential reinforcement, and mimicry. However, based on the interviews, we found that reinforcement is highly contextual, while the other three constructs are more stable over time and across contexts. Thus, we proposed a revised higher order construct which consists of definitions, differential association, and mimicry. Differential reinforcement is viewed as an external, contextual factor that influences the social learning process. Figure 7 presents the revised higher order construct and the relationship between reinforcement and social learning. The definitions dimension was measured

reflectively with three items. The differential association and mimicry dimensions were measured as reflective-formative constructs. Differential association and mimicry were measured by two dimensions each: family and friends for social learning in childhood and adolescence, and managers and coworkers for social learning in the workplace. The differential reinforcement dimension was measured with four formative measures representing positive social reinforcement, positive administrative reinforcement, negative social reinforcement, and negative administrative reinforcement.

Learning fit was also measured on a 7-point Likert scale. However, it was then converted to a 4 point scale. The center of the original 7-point scale represented the point at which individuals and the organization shared common beliefs about the importance of information security as depicted in Appendix C. Thus, we needed to make 4 represent the highest score, demonstrating the highest fit. To remedy this, we first calculated the absolute value of the distance of the original score from 4. For example, a score of 7 would be a distance of 3 from 4. Second, the absolute distance was subtracted from 4. So, a score of 7 was represented by a 1 ( $4-3 = 1$ ), showing low fit. A score of 1 on the original scale was also represented by a 1, showing low fit. The score of 4 represented good fit between the organization and individual. The constructs are presented in Table 7.

<b>Table 7. List of Key Constructs with Acronyms</b>
Construct
Social learning (adolescence & childhood) (SLEA)
Definitions of compliance (DFCA)
Differential association (DAEA)
Family (DAPA)
Friends (DAFA)

Imitation (IMEA)
Family (IMPA)
Friends (IMFA)
Differential reinforcement (adolescence & childhood) (DREA)
Social learning (previous organization) (SLPO)
Definitions of compliance (DFCP)
Differential association (DAPO)
Manager (DAMP)
Coworker (DACP)
Imitation (IMPO)
Manager (IMMP)
Coworker (IMCP)
Differential reinforcement (previous organization) (DREP)
Social learning (current organization) (SLCO)
Definitions of compliance (DFCC)
Differential association (DACO)
Manager (DAMC)
Coworker (DACC)
Imitation (IMCO)
Manager (IMMC)
Coworker (IMCC)
Differential reinforcement (current organization) (DREC)
Learning fit (LFIT)
Response efficacy (REFF)
Self-efficacy (SEFF)
Certainty of sanctions (CERT)
Severity of sanctions (SEVR)
Security training (TRAN)

## Participants

The US sample consisted primarily of individuals between the ages of 25-44. Most had earned a Bachelor's degree or higher. Nearly an equal number of men and women responded to the survey. Most of the respondents had a household income less than \$70,000. Most of the respondents held a job that was not part of the IT function and most employees were not in management. Most of the respondents worked for

organizations with 1-500 employees, although organizations of all sizes were included in the sample. Most employees had worked for their organization for 1-6 years and had varying levels of work experience. Overall, the sample was diverse. Table 8 presents the demographic details of the US sample.

<b>Table 8. Demographic Factors for US Sample</b>			
<b>Demographic Item</b>	<b>Level</b>	<b>Number</b>	<b>Percent</b>
Age	18-24	34	14
	25-34	101	41
	35-44	61	25
	45-54	27	11
	55-64	22	9
	65+	1	0
Education	Less than high school	0	0
	High school or equivalent	9	4
	Some college	48	19
	Two-year degree	29	12
	Bachelor's degree	112	45
	Master's degree	40	16
	Doctorate degree	9	4
Gender	Male	114	46
	Female	133	54
Income	Less than \$30,000	34	14
	\$30,000-\$39,000	43	17
	\$40,000-\$49,000	27	11
	\$50,000-\$59,000	34	14
	\$60,000-\$69,000	22	9
	\$70,000-\$79,000	24	10
	\$80,000-\$89,000	12	5
	\$90,000-\$99,000	19	8
	\$100,000+	31	13
IT Staff	Yes	55	22
	No	192	78
Manager	Yes	63	26
	No	184	74
Organizational size	1-99	84	34
	100-499	59	24
	500-999	28	11

	1000-4999	32	13
	5000+	44	18
Tenure (current organization)	Less than 1 year	49	20
	1-3 years	93	38
	4-6 years	48	20
	7-9 years	26	11
	10+ years	29	12
Work experience	Less than 1 year	1	0
	1-5 years	36	15
	6-10 years	64	26
	11-15 years	45	18
	16-20	33	13
	21+	66	27

Similar to the US sample, the India sample consisted primarily of individuals between the ages of 25-44. Like the US sample, most had earned a Bachelor's Degree or higher. Unlike the US sample, the India sample had far more male respondents than female respondents; 71 percent were male. Most of the respondents had a household income less than \$60,000. A little more than half of the respondents held a job in IT and a little more than half of the employees were not in management. Like the US sample, most of the respondents worked for organizations with 1-500 employees, although organizations of all sizes were included in the sample. Most employees had worked for their organization for 1-6 years and had 1-15 years of total work experience. Overall, the sample was diverse. Other than the level of male and female respondents, both samples were reasonably similar. Table 9 presents the demographic details of the India sample.

**Table 9. Demographic Factors for India Sample**

Demographic Item	Level	Number	Percent
Age	18-24	12	7
	25-34	112	64
	35-44	42	24
	45-54	8	5
	55-64	0	0
	65+	0	0
Education	Less than high school	0	0
	High school or equivalent	0	0
	Some college	5	3
	Two-year degree	6	3
	Bachelor's degree	95	55
	Master's degree	66	38
	Doctorate degree	2	1
Gender	Male	125	71
	Female	50	29
Income	Less than \$30,000	41	23
	\$30,000-\$39,000	24	14
	\$40,000-\$49,000	20	11
	\$50,000-\$59,000	13	7
	\$60,000-\$69,000	10	6
	\$70,000-\$79,000	7	4
	\$80,000-\$89,000	8	5
	\$90,000-\$99,000	11	6
	\$100,000+	41	23
IT Staff	Yes	102	58
	No	73	42
Manager	Yes	74	42
	No	101	58
Organizational size	1-99	44	25
	100-499	51	29
	500-999	33	19
	1000-4999	23	13
	5000+	24	14
Tenure (current organization)	Less than 1 year	8	5
	1-3 years	82	47
	4-6 years	52	30
	7-9 years	19	11
	10+ years	14	8
Work experience	Less than 1 year	0	0

	1-5 years	50	29
	6-10 years	71	41
	11-15 years	36	21
	16-20	11	6
	21+	7	4

## **CHAPTER VIII**

### **RESULTS OF THE QUANTIATIVE STUDY**

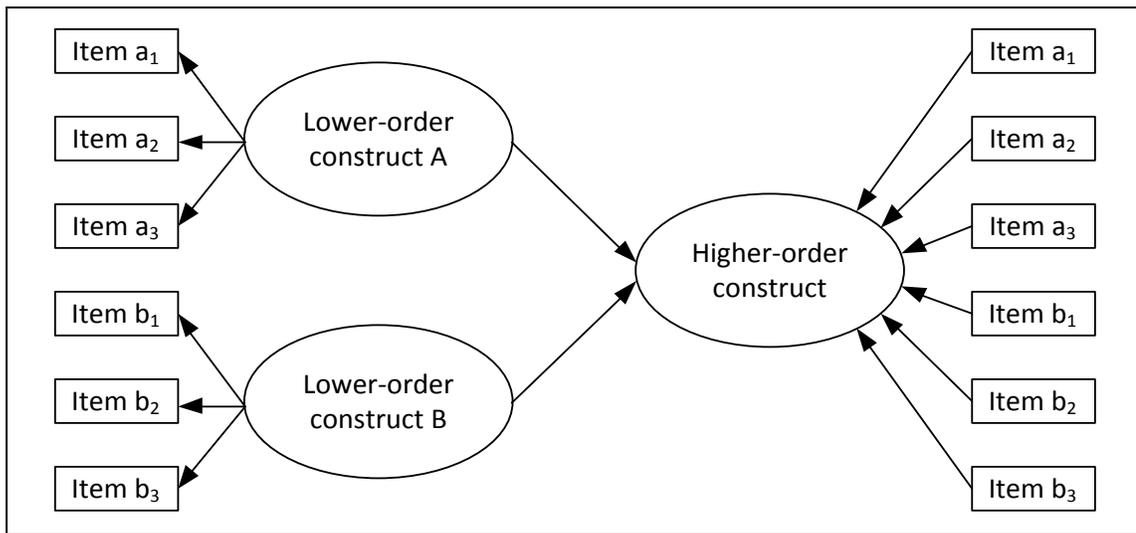
Partial least squares structural equation modeling (PLS-SEM) was used to analyze the data. SmartPLS (version 2.0M3) (Ringle, Wende, & Will, 2005) was used to assess the measurement and structural model. Because we had four dependent variables, we ran four models, each with one of the four dependent variables. A MANOVA was not employed because mediation and other complex path relationships were explored which are not supported by a MANOVA analysis. Four separate models were also run because information security research focuses primarily on single dependent variables. We also ran separate models for the US and India samples to compare path coefficients, statistical significance, and  $R^2$  values (Hovav & D'Arcy, 2012). To ensure that differences between the US and India models are caused by differences in nationality and not by other factors, measurement invariance can be assessed. At its core, measurement invariance seeks to identify whether the measurement models of different groups are similar. To assess this, we compared factor loadings across the US and India models. The factor loadings were similar across the US and India samples, providing evidence that the US and India models are measuring the same constructs and are comparable. In total, eight models were analyzed.

## **Two Stage Analysis Approach**

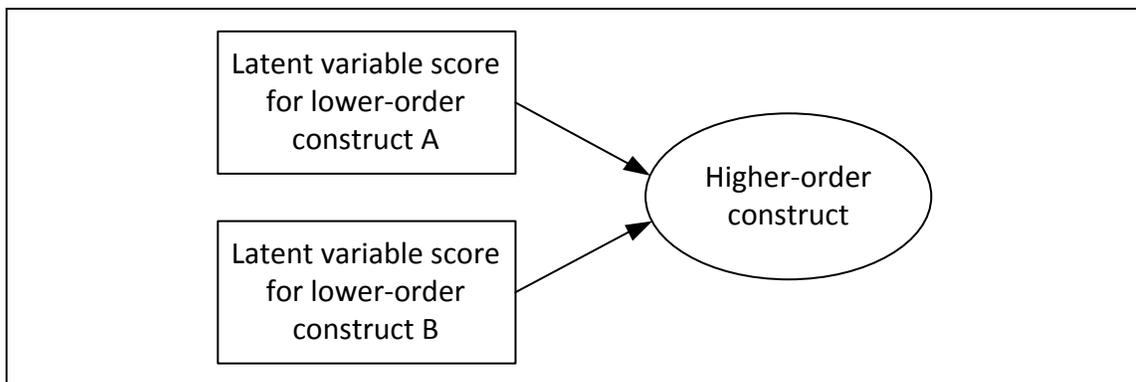
Because the differential association and mimicry dimensions of social learning are reflective-formative measurement, a two-stage analysis method was employed (Becker, Klein, & Wetzels, 2012; Wetzels, Odekerken-Schöder, & Oppen, 2009). The two-stage method is necessary because the formative relationship between the lower and higher order construct fully explains the variance in the higher order construct. Thus, other paths leading to the higher order construct will have coefficients of 0.0 because all of the variance in the higher order construct is explained by the lower order constructs. To remedy this, a model is constructed in the first stage of the process with the higher and lower order constructs and all of the associated items. The items are repeated from lower order constructs to the higher order constructs (Becker et al., 2012; Wetzels et al., 2009). Figure 9 presents a reflective formative model as it would be used in the first stage of analysis. Note that the measures for the lower order constructs are combined and repeated as measures for the higher order construct.

After running the first model, the latent variable scores are extracted for each lower order dimension (i.e., definitions, differential association, and mimicry) of the higher order construct (i.e., social learning). The latent variable scores are then included in the dataset and used as items to represent the higher order construct in a second model (Becker et al., 2012). Thus, definitions, differential association, and mimicry are not used as constructs in the second stage model. Their latent variable scores, however, are used as items of social learning. Figure 10 presents the second stage model after calculating the latent variables scores for the lower order constructs following the example in Figure 9.

In the second stage, the second model consists of solely first order constructs. The higher order constructs are represented by the latent variable scores of the lower order constructs calculated in the first model, and each other construct is represented by its original items (Becker et al., 2012).



**Figure 9. First Stage Model of the Reflective Formative Construct**



**Figure 10. Second Stage Model of the Reflective Formative Construct**

## **Assessing the Psychometric Properties of the Higher Order Constructs**

The two-stage analysis approach reduces the lower order constructs of a higher order construct to single indicators using latent variables scores as indicators. In doing so, information about the lower order constructs of the higher order construct is lost. However, some of this information is available in the model in the first stage of the two-stage analysis approach.

We examined eight separate models. To ensure consistency between all of the models, we examined the measurement properties for each model. By analyzing the psychometric properties of the first stage model, we found that some of the items of the first-order constructs of the higher order constructs did not perform equally well across the US and India samples. To maintain consistency, we dropped items from the models that did not perform well across both samples and across all eight models. Performance issues were caused by low loadings (less than 0.7) and high cross loadings (less than 0.1 difference between loadings and cross loadings). Issues arose for at least one of the six items on at least one of the first order differential association constructs. These first order constructs include differential association (parents), differential association (friends), differential association (co-workers from previous job), differential association (managers from previous job), differential association (co-workers from current job), and differential association (managers from previous job). In reflective-formative measurement, it is advised to maintain the same number of items for each first order construct that forms the second order construct (W. W. Chin, Marcolin, & Newsted, 2003). For example, if a measure was dropped from differential association (parents), a

measure was also dropped from the associated differential association (friends) construct. After making these adjustments, each of the first-order constructs for all of the second-order differential association construct were represented with two items.

One of the measures for the certainty of sanctions construct was also removed due to low loadings in the India sample. All other constructs are represented with at least three items. The remaining items for the first-order constructs loaded highly (above 0.70), exhibited strong reliability (above 0.80), and demonstrated average variance extracted (AVE) values above 0.5. These values suggest that the first-order constructs of the higher order constructs demonstrate satisfactory psychometric properties.

Because the two dimensions of differential association and mimicry were reduced to latent variable scores, the validity of the formative measurement was assessed through the first stage model as well. To assess the validity of the formative measures, we assessed whether the weights leading from the lower order constructs to the higher order constructs were statistically significant (Becker et al., 2012). In all cases, the weights were statistically significant ( $p < 0.01$ ). This provides evidence of validity for the reflective-formative measurement. The remainder of the measurement is examined in the sections that follow.

### **Assessing the Psychometric Properties of the Formative Constructs**

Each model contained three constructs representing differential reinforcement during the respondents' childhood/adolescence, previous job, and current job. The three differential reinforcement constructs were measured formatively. The validity of formative measurement is assessed differently than for reflective measurement. To assess

formative measurement, the statistical significance of the weights of each formative measure are examined and the variance inflation factor (VIF) of each measure is examined to determine whether each measure contributes uniquely to the variance in the construct (W W Chin, 1998). VIF values should be below 3.3 for all items (Petter et al., 2007). VIF was calculated in SAS (version 9.4) with PROC REG. Ideally, t-values should be above 1.96. However, items with insignificant t-values may be retained to maintain the content validity of the construct (Diamantopoulos & Winklhofer, 2001; Jarvis, MacKenzie, & Podsakoff, 2003). For the US sample, VIF was below the cutoff value, suggesting that multicollinearity was not an issue. Some t-values were below the cutoff. However, we retained the items to maintain the theoretical meaning of the construct. The items capture non-social punishment and reward for rule following and rule breaking behavior, and social shame and praise for rule following and rule breaking behavior. Removing any of these items would eliminate conceptual information about reinforcement. Thus, the items were retained in the analysis. Table 10 presents the t-values and VIF values for the US sample.

<b>Table 10. t-values and VIFs for Formative Constructs for US sample</b>			
Construct	Item	t-value	VIF
Differential reinforcement (childhood/adolescence)	DREA1	1.9080	1.6122
	DREA2	2.0355	1.5368
	DREA3	0.0391	1.6394
	DREA4	5.6550	1.6219
Differential reinforcement (previous job)	DREP1	1.2523	1.8260
	DREP2	3.1269	2.5659
	DREP3	1.1098	1.9690
	DREP4	1.9182	2.5556
Differential reinforcement	DREC1	2.1091	1.3566

(current job)	DREC2	1.8197	1.8969
	DREC3	1.4104	1.3767
	DREC4	3.4208	1.8815

For the India sample, VIF was also below the cutoff value, suggesting that multicollinearity was not an issue. Again, some t-values were below the cutoff. However, we retained the items to maintain the theoretical meaning of the construct. Table 11 presents the t-values and VIF values for the India sample.

<b>Table 11. t-values and VIFs for Formative Constructs for IN sample</b>			
Construct	Item	t-value	VIF
Differential reinforcement (childhood/adolescence)	DREA1	1.8726	1.5029
	DREA2	5.6350	1.4498
	DREA3	0.1482	1.4973
	DREA4	3.2389	1.4326
Differential reinforcement (previous job)	DREP1	1.5728	1.3193
	DREP2	7.2666	1.7824
	DREP3	0.2387	1.2949
	DREP4	2.0491	1.8175
Differential reinforcement (current job)	DREC1	3.0047	1.2907
	DREC2	3.7628	1.5389
	DREC3	0.6405	1.3024
	DREC4	4.4678	1.5267

A post-hoc analysis shows that removing the formative items whose weights were not statistically significant has no major effect on the relationships between differential reinforcement and social learning. Both the path and t-values were nearly identical after removing the insignificant items. Thus, to maintain the theoretical meaning of the differential reinforcement construct, they remained in the analysis.

## Models 1 and 2: Security Assurance Behavior in the US and India

Models 1 and 2 represent security assurance behavior in the US and India, respectively. The measurement model and structural model are examined below.

### *Measurement Model*

In the models, the quality of the reflective scales was assessed by examining reliability, convergent validity, and discriminant validity. The US sample exhibited high composite reliabilities for all reflective scales. Composite reliabilities should exceed 0.70 (Fornell & Larcker, 1981). The composite reliabilities for the US model exceeded 0.90 as depicted in Table 12, suggesting that the measures are reliable.

<b>Table 12. Model 1: AVE and Composite Reliability for US Sample</b>		
	AVE	Composite Reliability
LFIT	0.8380	0.9539
PINT	0.7867	0.9171
REFF	0.7951	0.9208
SEFF	0.8165	0.9302
SLCO	0.8249	0.9339
SLEA	0.7738	0.9112
SLPO	0.8828	0.9576
TRAN	0.9050	0.9662

The India sample also exhibited high composite reliabilities for all reflective scales. All composite reliability scores exceeded 0.85 as depicted in Table 13. Although composite reliabilities were slightly lower for the India sample, they still exceeded the recommended cutoff of 0.70, suggesting reliable measures.

**Table 13. Model 2: AVE and Composite Reliability for India Sample**

	AVE	Composite Reliability
LFIT	0.8320	0.9519
PINT	0.7441	0.8971
REFF	0.6587	0.8519
SEFF	0.6755	0.8617
SLCO	0.8795	0.9563
SLEA	0.8377	0.9393
SLPO	0.8679	0.9517
TRAN	0.8504	0.9446

Convergent validity was assessed by ensuring that all factor loadings exceeded 0.70 and that the average variance extracted (AVE) exceeded 0.5 (Fornell & Larcker, 1981; Gefen & Straub, 2005). The US sample exhibited high factor loadings as depicted in Table 14. AVE was also above 0.5 for all constructs as depicted in Table 12. The values suggest that the US sample exhibits convergent validity.

**Table 14. Model 1: Loadings and Cross Loadings for US Sample**

	LFIT	PINT	REFF	SEFF	SLCO	SLEA	SLPO	TRAN
LFIT 1	<b>0.9301</b>	0.0172	0.1780	0.2182	0.2249	0.0953	0.1065	0.0747
LFIT 2	<b>0.9267</b>	0.0551	0.1221	0.2129	0.2021	0.0847	0.0965	0.0462
LFIT 3	<b>0.8899</b>	-0.0187	0.0846	0.1247	0.1153	0.0520	0.0290	0.0431
LFIT 4	<b>0.9145</b>	0.0246	0.1161	0.1830	0.1140	0.0626	0.0648	0.0401
PINT 1	0.0389	<b>0.8864</b>	0.1108	0.1696	0.1784	0.1682	0.0481	0.2076
PINT 2	-0.0082	<b>0.8680</b>	0.1594	0.2288	0.2032	0.1721	0.1550	0.2451
PINT 3	0.0446	<b>0.9060</b>	0.1415	0.1716	0.1923	0.1367	0.0678	0.2234
REFF 1	0.1353	0.1152	<b>0.8900</b>	0.6108	0.5374	0.2638	0.3716	0.3337

REFF 2	0.0982	0.1444	<b>0.9212</b>	0.5458	0.6089	0.3710	0.3413	0.3739
REFF 3	0.1565	0.1569	<b>0.8629</b>	0.5910	0.5915	0.3129	0.3611	0.3884
SEFF 1	0.1977	0.2180	0.6279	<b>0.9384</b>	0.5547	0.4032	0.4110	0.2797
SEFF 2	0.1712	0.1964	0.5558	<b>0.8656</b>	0.4391	0.2813	0.3625	0.2672
SEFF 3	0.2014	0.1748	0.5801	<b>0.9053</b>	0.5288	0.3736	0.4296	0.2842
SLC O1	0.1699	0.2126	0.6686	0.5532	<b>0.8782</b>	0.4004	0.3942	0.4392
SLC O2	0.1732	0.2071	0.5681	0.5146	<b>0.9487</b>	0.4716	0.4435	0.4298
SLC O3	0.1892	0.1683	0.5294	0.4656	<b>0.8964</b>	0.4494	0.4544	0.3996
SLE A1	0.0973	0.2132	0.3624	0.3164	0.4605	<b>0.8566</b>	0.3262	0.2125
SLE A2	0.1048	0.0971	0.3065	0.3950	0.4391	<b>0.8978</b>	0.3307	0.1716
SLE A3	0.0214	0.1643	0.2694	0.3291	0.3756	<b>0.8841</b>	0.3782	0.1855
SLPO 1	0.1177	0.1524	0.4220	0.4280	0.4573	0.3800	<b>0.9341</b>	0.1723
SLPO 2	0.0623	0.0710	0.3645	0.4415	0.4875	0.3897	<b>0.9515</b>	0.1674
SLPO 3	0.0725	0.0752	0.3385	0.3781	0.3775	0.3277	<b>0.9331</b>	0.1390
TRA N1	0.0704	0.2240	0.4156	0.3041	0.4631	0.2146	0.1857	<b>0.9491</b>
TRA N2	0.0610	0.2520	0.3796	0.2667	0.4450	0.2247	0.1438	<b>0.9483</b>
TRA N3	0.0357	0.2556	0.3759	0.3039	0.4221	0.1757	0.1576	<b>0.9565</b>

Though slightly different from the US sample, the India sample also exhibited high factor loadings as depicted in Table 15. AVE was also above 0.5 for all constructs as depicted in Table 13. The values suggest that the India sample also exhibits convergent validity.

**Table 15. Model 2: Loadings and Cross Loadings for India Sample**

	LFIT	PINT	REFF	SEFF	SLCO	SLEA	SLPO	TRAN
LFIT 1	<b>0.9206</b>	-0.2381	-0.4241	-0.4039	-0.4272	-0.3794	-0.3321	-0.3561
LFIT 2	<b>0.9342</b>	-0.2630	-0.4240	-0.3834	-0.4479	-0.3936	-0.3164	-0.3833
LFIT 3	<b>0.8961</b>	-0.2341	-0.4353	-0.3752	-0.4234	-0.3659	-0.3061	-0.3918
LFIT 4	<b>0.8970</b>	-0.2090	-0.4108	-0.3561	-0.3901	-0.3549	-0.2845	-0.3846
PINT 1	-0.1505	<b>0.8622</b>	0.2947	0.2870	0.3446	0.2639	0.4333	0.2534
PINT 2	-0.3108	<b>0.8581</b>	0.4074	0.3644	0.4204	0.4002	0.4242	0.3236
PINT 3	-0.1881	<b>0.8674</b>	0.2803	0.3192	0.3570	0.3533	0.4181	0.2974
REFF 1	-0.2325	0.2342	<b>0.7139</b>	0.4933	0.4221	0.2949	0.3920	0.4941
REFF 2	-0.4300	0.3676	<b>0.8542</b>	0.6599	0.6047	0.4695	0.5343	0.5546
REFF 3	-0.4312	0.3241	<b>0.8585</b>	0.7173	0.6708	0.4763	0.5867	0.5677
SEFF 1	-0.3508	0.3684	0.6380	<b>0.8392</b>	0.6497	0.5064	0.5636	0.5317
SEFF 2	-0.4211	0.3247	0.7319	<b>0.8591</b>	0.6984	0.4924	0.5943	0.5374
SEFF 3	-0.2276	0.2221	0.5322	<b>0.7643</b>	0.4989	0.3343	0.4041	0.4658
SLC O1	-0.4350	0.4235	0.7226	0.7622	<b>0.9184</b>	0.5443	0.6993	0.6435
SLC O2	-0.4307	0.3878	0.6337	0.6964	<b>0.9458</b>	0.5610	0.7567	0.6662
SLC O3	-0.4382	0.4196	0.6437	0.6749	<b>0.9490</b>	0.6026	0.7419	0.6414
SLE A1	-0.3765	0.3329	0.4480	0.4810	0.4753	<b>0.8896</b>	0.4546	0.3514
SLE A2	-0.3620	0.3557	0.4952	0.5131	0.5955	<b>0.9359</b>	0.5785	0.3546
SLE A3	-0.3893	0.4025	0.4866	0.5168	0.5817	<b>0.9197</b>	0.5922	0.3877
SLPO 1	-0.2724	0.4790	0.5958	0.5848	0.6848	0.5340	<b>0.9046</b>	0.6222

SLPO 2	-0.3352	0.4345	0.6124	0.6315	0.7460	0.5717	<b>0.9454</b>	0.6214
SLPO 3	-0.3402	0.4665	0.5601	0.5847	0.7496	0.5645	<b>0.9443</b>	0.6314
TRA N1	-0.3441	0.2981	0.5968	0.5370	0.6101	0.3759	0.6100	<b>0.9324</b>
TRA N2	-0.3898	0.3252	0.6268	0.6115	0.6677	0.3829	0.6279	<b>0.9231</b>
TRA N3	-0.4123	0.3189	0.6101	0.5758	0.6383	0.3435	0.6163	<b>0.9109</b>

Discriminant validity was assessed by ensuring that the square root of AVE for each construct was greater than the corresponding latent variable correlations for construct (W W Chin, 1998), and that factor loadings were greater than cross loadings by at least 0.1 (W W Chin, 2010; D'Arcy, Herath, & Shoss, 2014). For the US sample, the square root of AVE for each construct was greater than the corresponding latent variable correlations. Table 16 presents latent variable correlations for the US sample with the square root of AVE along the diagonal. As depicted in Table 14, the factor loadings for each item exceeded cross loadings by at least 0.1 in every instance. These tests suggest that the US sample exhibits discriminant validity.

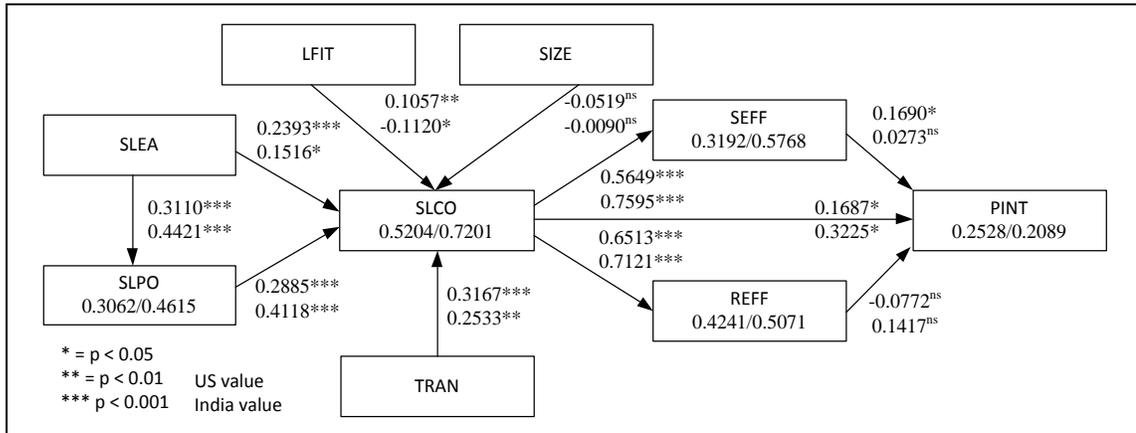
<b>Table 16. Model 1: Latent Variable Correlations for US Sample</b>								
	LFIT	PINT	REFF	SEFF	SLCO	SLEA	SLPO	TRAN
LFIT	<b>0.9154</b>							
PINT	0.0259	<b>0.8870</b>						
REFF	0.1454	0.1567	<b>0.8917</b>					
SEFF	0.2111	0.2174	0.6519	<b>0.9036</b>				
SLCO	0.1951	0.2169	0.6515	0.5651	<b>0.9082</b>			
SLEA	0.0857	0.1803	0.3568	0.3944	0.4844	<b>0.8797</b>		
SLPO	0.0898	0.1067	0.4008	0.4450	0.4734	0.3918	<b>0.9396</b>	
TRAN	0.0591	0.2559	0.4110	0.3065	0.4668	0.2162	0.1711	<b>0.9513</b>

For the India sample, the square root of AVE for each construct was also greater than the corresponding latent variable correlations. Table 17 presents latent variable correlations for the India sample with the square root of AVE along the diagonal. As depicted in Table 15, the factor loadings for each item exceeded cross loadings by at least 0.1 in every instance. These tests suggest that the India sample exhibits discriminant validity.

<b>Table 17. Model 2: Latent Variable Correlations for India Sample</b>								
	LFIT	PINT	REFF	SEFF	SLCO	SLEA	SLPO	TRAN
LFIT	<b>0.9121</b>							
PINT	-0.2596	<b>0.8626</b>						
REFF	-0.4644	0.3869	<b>0.8116</b>					
SEFF	-0.4166	0.3790	0.7802	<b>0.8219</b>				
SLCO	-0.4637	0.4379	0.7122	0.7596	<b>0.9378</b>			
SLEA	-0.4099	0.3991	0.5221	0.5511	0.6069	<b>0.9153</b>		
SLPO	-0.3401	0.4930	0.6322	0.6445	0.7809	0.5979	<b>0.9316</b>	
TRAN	-0.4151	0.3411	0.6634	0.6246	0.6937	0.3986	0.6706	<b>0.9222</b>

### ***Structural Model***

The structural model was assessed in SmartPLS using the second stage model which included the latent variable scores of the lower order constructs as items for the higher order constructs (Becker et al., 2012). Figure 11 presents the results of the models 1 and 2. Scores for the US sample are above or to the left of the scores for the India sample. Only the relationships that differ in models 3-8 from models 1 and 2 are presented in the figures for models 3-8, because the relationships that are consistent between the models have the same scores as presented in models 1 and 2.



The data suggests that perceptions of social learning that favor compliant behavior encountered during childhood and adolescence increases perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job ( $\beta = 0.3110$ ; p-value < 0.001). Similarly, perceptions of social learning that favor compliant behavior encountered during childhood and adolescence increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.2393$ ; p-value < 0.001). The data provides support for hypotheses 1a and 1b. The data also suggests that perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.2885$ ; p-value < 0.001). The data provides support for hypothesis 2.

The data provides evidence that perceptions of learning fit increase perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.1057$ ; p-value < 0.01). The data provides support for hypothesis 3.

The data suggests that differential reinforcement increases perceptions of social learning in favor of compliance. The data provides evidence that perceptions of differential reinforcement from childhood and adolescence increase perceptions of social learning that favor compliant behavior encountered during childhood and adolescence ( $\beta = 0.4394$ ;  $p\text{-value} < 0.001$ ). The data also provides evidence that perceptions of differential reinforcement from one's previous job increase perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job ( $\beta = 0.3990$ ;  $p\text{-value} < 0.001$ ). Similarly, the data provides evidence that perceptions of differential reinforcement from one's current job increase perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.2479$ ;  $p\text{-value} < 0.001$ ). The data provides support for hypotheses h4a, h4b, and h4c.

The data provide evidence that perceptions of social learning that favor compliant behavior encountered during tenure at one's current job increase intentions to engage in proactive security behavior ( $\beta = 0.1687$ ;  $p\text{-value} < 0.05$ ). The data provides support for hypothesis 5.

Statistical evidence does not exist to suggest that organizational size influences social learning at one's current organization ( $\beta = -0.0519$ ;  $p\text{-value} > 0.05$ ). The data do not provide support for hypothesis 6. However, the data provide evidence that security training increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.3167$ ;  $p\text{-value} < 0.001$ ). Thus, the data provide support for hypothesis 7.

The data also provide evidence that perceptions of social learning that favor compliant behavior encountered during tenure at one's current job increase self-efficacy to comply with ISP ( $\beta = 0.5649$ ;  $p$ -value  $< 0.001$ ). Similarly, the data provide evidence that perceptions of social learning that favor compliant behavior encountered during tenure at one's current job increase response efficacy perceptions ( $\beta = 0.6513$ ;  $p$ -value  $< 0.001$ ). The data provides support for hypotheses 8 and 9. Finally, the data provide evidence that self-efficacy to comply with ISP increases intentions to engage in proactive security behavior ( $\beta = 0.1690$ ;  $p$ -value  $< 0.05$ ). Statistical evidence does not exist to suggest that response efficacy increases intentions to engage in proactive security behavior ( $\beta = -0.0772$ ;  $p$ -value  $> 0.05$ ). Thus, the data provide support for hypothesis 10, but not for hypothesis 11. Table 18 presents each hypothesis with its coefficient, t-value, p-value, and whether the hypothesis was supported by the data.

<b>Table 18. Model 1: Statistical Support for Hypotheses for US Sample</b>				
Relationship	Coefficient	t-value	p-value	Supported
h1a: SLEA → SLPO	0.3110	5.4063	$p < 0.001$	Yes
h1b: SLEA → SLCO	0.2393	4.3356	$p < 0.001$	Yes
h2: SLPO → SLCO	0.2885	4.6171	$p < 0.001$	Yes
h3: LFIT → SLCO	0.1057	2.5985	$p < 0.01$	Yes
h4a: DREA → SLEA	0.4394	8.6530	$p < 0.001$	Yes
h4b: DREP → SLPO	0.3990	7.8661	$p < 0.001$	Yes
h4c: DREC → SLCO	0.2479	4.3431	$p < 0.001$	Yes
h5: SLCO → PINT	0.1687	1.9813	$p < 0.05$	Yes
h6: SIZE → SLCO	-0.0519	0.8238	$p > 0.05$	No
h7: TRAN → SLCO	0.3167	4.5550	$p < 0.001$	Yes
h8: SLCO → SEFF	0.5649	9.3063	$p < 0.001$	Yes
h9: SLCO → REFF	0.6513	13.8742	$p < 0.001$	Yes
h10: SEFF → PINT	0.1690	2.2115	$p < 0.05$	Yes
h11: REFF → PINT	-0.0772	0.9561	$p > 0.05$	No

The Sobel mediation test (Sobel, 1982) was conducted to assess whether self-efficacy is a mediating variable. The Sobel test provides evidence that self-efficacy is a mediating variable (test statistic = 2.1521, p-value < 0.05). Because response efficacy was not significantly related to intentions to engage in proactive security behavior, the Sobel test was not used for response efficacy. Significance between the mediating variable and the dependent variable is a requirement for mediation (MacKinnon, Lockwood, & Hoffman, 2002).

Age, education, gender, income, job position, organizational size, tenure, work experience were used as control variables. The data provide evidence that education decreases intentions to engage in proactive security behavior ( $\beta = -0.1131$ ; p-value < 0.05). Educated individuals may feel that they possess sufficient knowledge and do not need further information about security, which may explain the decrease in proactive behaviors that often require extra research. This finding should be explored further in future research. The data also provide evidence that being an IT employee increases intentions to engage in proactive security behavior ( $\beta = 0.3568$ ; p-value < 0.001). All other control variables were statistically insignificant. Table 19 presents the coefficient, t-value, p-value, and whether the relationship was supported for each control variable.

<b>Table 19. Model 1: Statistical Support for Control Variables for US Sample</b>				
Control Variable	Coefficient	t-value	p-value	Supported
Age	-0.0882	1.1484	p > 0.05	No
Education	-0.1131	2.1399	p < 0.05	Yes
Gender	0.0726	1.2390	p > 0.05	No
Income	-0.0596	1.0298	p > 0.05	No
IT employee	0.3568	6.7493	p < 0.001	Yes

Manager	0.0332	0.4824	p > 0.05	No
Organizational size	-0.0519	0.8936	p > 0.05	No
Tenure	0.0518	0.7408	p > 0.05	No
Work experience	0.1288	1.7144	p > 0.05	No

The model explained 25.28 percent of the variance in intentions to engage in proactive security behavior, 42.41 percent of the variance in response efficacy, 31.92 percent of the variance in self-efficacy, 52.04 percent of the variance in social learning (current organization), 30.62 percent of the variance in social learning (previous organization), and 19.30 percent of the variance in social learning (adolescence and childhood). Table 20 presents the R<sup>2</sup> values for each endogenous construct.

<b>Table 20. Model 1: R<sup>2</sup> Values for Endogenous Constructs for US Sample</b>	
Construct	R <sup>2</sup> Value
PINT	0.2528
REFF	0.4241
SEFF	0.3192
SLCO	0.5204
SLEA	0.1930
SLPO	0.3062

For the India sample, the data suggest that perceptions of social learning that favor compliant behavior encountered during childhood and adolescence increases perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job ( $\beta = 0.4421$ ; p-value < 0.001). Similarly, perceptions of social learning that favor compliant behavior encountered during childhood and adolescence increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.1516$ ; p-value < 0.05). The data provides support for hypotheses

1a and 1b. The data also suggests that perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.4118$ ;  $p\text{-value} < 0.001$ ). The data provides support for hypothesis 2.

The data provides evidence that perceptions of learning fit decrease perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = -0.1120$ ;  $p\text{-value} < 0.05$ ). The data provides support for hypothesis 3.

The data suggests that differential reinforcement increases perceptions of social learning in favor of compliance. The data provides evidence that perceptions of differential reinforcement from childhood and adolescence increase perceptions of social learning that favor compliant behavior encountered during childhood and adolescence ( $\beta = 0.6143$ ;  $p\text{-value} < 0.001$ ). The data also provides evidence that perceptions of differential reinforcement from one's previous job increase perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job ( $\beta = 0.3593$ ;  $p\text{-value} < 0.001$ ). Similarly, the data provides evidence that perceptions of differential reinforcement from one's current job increase perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.1449$ ;  $p\text{-value} < 0.01$ ). The data provides support for hypotheses h4a, h4b, and h4c.

The data provide evidence that perceptions of social learning that favor compliant behavior encountered during tenure at one's current job increase intentions to engage in proactive security behavior ( $\beta = 0.3225$ ;  $p\text{-value} < 0.05$ ). The data provides support for hypothesis 5.

Statistical evidence does not exist to suggest that organizational size influences social learning at one's current organization ( $\beta = -0.0090$ ;  $p\text{-value} > 0.05$ ). The data do not provide support for hypothesis 6. However, the data provide evidence that security training increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.2533$ ;  $p\text{-value} < 0.01$ ). Thus, the data provide support for hypothesis 7.

The data also provide evidence that perceptions of social learning that favor compliant behavior encountered during tenure at one's current job increase self-efficacy to comply with ISP ( $\beta = 0.7595$ ;  $p\text{-value} < 0.001$ ). Similarly, the data provide evidence that perceptions of social learning that favor compliant behavior encountered during tenure at one's current job increase response efficacy perceptions ( $\beta = 0.7121$ ;  $p\text{-value} < 0.001$ ). The data provides support for hypotheses 8 and 9. Finally, the data do not provide evidence that self-efficacy to comply with ISP increases intentions to engage in proactive security behavior ( $\beta = 0.0273$ ;  $p\text{-value} > 0.05$ ). Statistical evidence does not exist to suggest that response efficacy increases intentions to engage in proactive security behavior ( $\beta = 0.1417$ ;  $p\text{-value} > 0.05$ ). Thus, the data do not provide support for hypotheses 10 and 11. Table 21 presents each hypothesis with its coefficient, t-value, p-value, and whether the hypothesis was supported by the data.

**Table 21. Model 2: Statistical Support for Hypotheses for India Sample**

Relationship	Coefficient	t-value	p-value	Supported
h1a: SLEA → SLPO	0.4421	6.3016	$p < 0.001$	Yes
h1b: SLEA → SLCO	0.1516	2.3218	$p < 0.05$	Yes
h2: SLPO → SLCO	0.4118	4.0214	$p < 0.001$	Yes
h3: LFIT → SLCO	-0.1120	2.2132	$p < 0.05$	Yes

h4a: DREA → SLEA	0.6143	12.6724	p < 0.001	Yes
h4b: DREP → SLPO	0.3593	5.7639	p < 0.001	Yes
h4c: DREC → SLCO	0.1449	3.0660	p < 0.01	Yes
h5: SLCO → PINT	0.3225	2.2694	p < 0.05	Yes
h6: SIZE → SLCO	-0.0090	0.2573	p > 0.05	No
h7: TRAN → SLCO	0.2533	3.0199	p < 0.01	Yes
h8: SLCO → SEFF	0.7595	19.2013	p < 0.001	Yes
h9: SLCO → REFF	0.7121	16.8485	p < 0.001	Yes
h10: SEFF → PINT	0.0273	0.2137	p > 0.05	No
h11: REFF → PINT	0.1417	1.1013	p > 0.05	No

The Sobel mediation test (Sobel, 1982) was not conducted on the India sample because the paths leading from self-efficacy and response efficacy to intentions to engage in proactive security behavior were statistically insignificant. Thus, they are not mediators (MacKinnon et al., 2002).

Age, education, gender, income, job position, organizational size, tenure, work experience were used as control variables. All control variables were statistically insignificant in the India sample. Table 22 presents the coefficient, t-value, p-value, and whether the relationship was supported for each control variable.

<b>Table 22. Model 2: Statistical Support for Control Variables for India Sample</b>				
Control Variable	Coefficient	t-value	p-value	Supported
Age	0.0369	0.3580	p > 0.05	No
Education	0.0266	0.3030	p > 0.05	No
Gender	0.0030	0.0395	p > 0.05	No
Income	-0.0529	0.6916	p > 0.05	No
IT employee	-0.0260	0.3275	p > 0.05	No
Manager	0.0293	0.3565	p > 0.05	No
Organizational size	-0.0004	0.0053	p > 0.05	No
Tenure	0.0386	0.3434	p > 0.05	No
Work experience	-0.0869	0.6381	p > 0.05	No

The model explained 20.89 percent of the variance in intentions to engage in proactive security behavior, 50.71 percent of the variance in response efficacy, 57.68 percent of the variance in self-efficacy, 72.01 percent of the variance in social learning (current organization), 37.74 percent of the variance in social learning (previous organization), and 46.15 percent of the variance in social learning (adolescence and childhood). Table 23 presents the R<sup>2</sup> values for each endogenous construct.

<b>Table 23. Model 2: R<sup>2</sup> Values for Endogenous Constructs for India Sample</b>	
Construct	R <sup>2</sup> Value
PINT	0.2089
REFF	0.5071
SEFF	0.5768
SLCO	0.7201
SLEA	0.3774
SLPO	0.4615

Comparing the US and India samples shows that the India sample exhibited higher coefficients for several relationships. The higher differences were most prominent in the relationships between social learning (childhood and adolescence) and social learning (previous organization), between social learning (previous organization) and social learning (current organization), between differential reinforcement and social learning (childhood and adolescence), between social learning (current organization) and intentions to engage in proactive security behavior, between social learning (current organization) and self-efficacy, and between response efficacy and intentions to engage in proactive security behavior. The US sample exhibited higher coefficients in the relationships between learning fit and social learning (current organization), between

differential association and social learning (current organization), and between self-efficacy and intentions to engage in proactive security behavior. The samples also differed in the statistical significance of the path leading from self-efficacy to intentions to engage in proactive security behavior. The US sample exhibited a statistically significant path, but the path in the India sample was statistically insignificant. Table 24 presents the primary differences between the US and India samples.

<b>Table 24. Comparison of Path Coefficients for US and India Samples</b>		
Relationship	Coefficient (US – India)	Supported (US/India)
h1a: SLEA → SLPO	-0.1311	Yes/Yes
h1b: SLEA → SLCO	0.0877	Yes/Yes
h2: SLPO → SLCO	-0.1233	Yes/Yes
h3: LFIT → SLCO	0.2177	Yes/Yes
h4a: DREA → SLEA	-0.1749	Yes/Yes
h4b: DREP → SLPO	0.0397	Yes/Yes
h4c: DREC → SLCO	0.1030	Yes/Yes
h5: SLCO → PINT	-0.1538	Yes/Yes
h6: SIZE → SLCO	-0.0429	No/No
h7: TRAN → SLCO	0.0634	Yes/Yes
h8: SLCO → SEFF	-0.1946	Yes/Yes
h9: SLCO → REFF	-0.0608	Yes/Yes
h10: SEFF → PINT	0.1417	Yes/No
h11: REFF → PINT	-0.2189	No/No

The India sample also exhibited higher  $R^2$  values for more endogenous constructs than the US sample. The most substantial differences were in the  $R^2$  values for: self-efficacy, social learning (childhood and adolescence), social learning (previous organization), and social learning (previous organization). Table 25 presents differences between  $R^2$  values for the US and India samples.

**Table 25. Comparison of R<sup>2</sup> Values for US and India Samples**

Construct	R <sup>2</sup> Values (US – India)
PINT	0.0439
REFF	-0.0830
SEFF	-0.2576
SLCO	-0.1997
SLEA	-0.1844
SLPO	-0.1553

**Models 3 and 4: Security Compliant Behavior in the US and India**

Models 3 and 4 represent security compliant behavior in the US and India, respectively. The measurement model and structural model are examined below.

***Measurement Model***

In the models, the quality of the reflective scales was assessed by examining reliability, convergent validity, and discriminant validity. The US sample exhibited high composite reliabilities for all reflective scales. Composite reliabilities should exceed 0.70 (Fornell & Larcker, 1981). The composite reliabilities for the US model exceeded 0.90 as depicted in Table 26, suggesting that the measures are reliable.

**Table 26. Model 3: AVE and Composite Reliability for US Sample**

	AVE	Composite Reliability
CINT	0.8263	0.9345
LFIT	0.8380	0.9539
REFF	0.7951	0.9208
SEFF	0.8162	0.9301
SLCO	0.8247	0.9338
SLEA	0.7738	0.9112
SLPO	0.8828	0.9576
TRAN	0.9050	0.9662

The India sample also exhibited high composite reliabilities for all reflective scales. All composite reliability scores exceeded 0.85 as depicted in Table 27. Although composite reliabilities were slightly lower for the India sample, they still exceeded the recommended cutoff of 0.70, suggesting reliable measures.

<b>Table 27. Model 4: AVE and Composite Reliability for India Sample</b>		
	AVE	Composite Reliability
CINT	0.8088	0.9269
LFIT	0.8320	0.9519
REFF	0.6599	0.8528
SEFF	0.6763	0.8622
SLCO	0.8795	0.9563
SLEA	0.8377	0.9393
SLPO	0.8679	0.9517
TRAN	0.8504	0.9446

The US sample exhibited high factor loadings as depicted in Table 28. AVE was also above 0.5 for all constructs as depicted in Table 26. The values suggest that the US sample exhibits convergent validity.

<b>Table 28. Model 3: Loadings and Cross Loadings for US Sample</b>								
	CINT	LFIT	REFF	SEFF	SLCO	SLEA	SLPO	TRAN
CINT 1	<b>0.9211</b>	0.1599	0.3720	0.4187	0.4859	0.3295	0.2487	0.3034
CINT 2	<b>0.8816</b>	0.1511	0.3121	0.4143	0.4135	0.2709	0.2263	0.2118
CINT 3	<b>0.9237</b>	0.2133	0.3722	0.4128	0.4476	0.2782	0.2757	0.2495
LFIT 1	0.1726	<b>0.9301</b>	0.1781	0.2183	0.2248	0.0953	0.1065	0.0747
LFIT 2	0.1798	<b>0.9268</b>	0.1222	0.2127	0.2021	0.0847	0.0965	0.0462

LFIT 3	0.1758	<b>0.8899</b>	0.0848	0.1253	0.1151	0.0520	0.0291	0.0431
LFIT 4	0.1801	<b>0.9144</b>	0.1164	0.1839	0.1139	0.0627	0.0648	0.0401
REFF 1	0.3189	0.1353	<b>0.8902</b>	0.6102	0.5382	0.2638	0.3716	0.3337
REFF 2	0.3499	0.0982	<b>0.9204</b>	0.5458	0.6098	0.3710	0.3413	0.3739
REFF 3	0.3666	0.1565	<b>0.8635</b>	0.5911	0.5924	0.3129	0.3611	0.3884
SEFF 1	0.4393	0.1977	0.6282	<b>0.9379</b>	0.5554	0.4033	0.4110	0.2797
SEFF 2	0.3415	0.1713	0.5561	<b>0.8611</b>	0.4393	0.2813	0.3625	0.2672
SEFF 3	0.4459	0.2014	0.5804	<b>0.9095</b>	0.5295	0.3736	0.4296	0.2842
SLC O1	0.5200	0.1699	0.6685	0.5543	<b>0.8807</b>	0.4005	0.3942	0.4392
SLC O2	0.4387	0.1732	0.5681	0.5151	<b>0.9480</b>	0.4717	0.4435	0.4298
SLC O3	0.3785	0.1893	0.5293	0.4659	<b>0.8943</b>	0.4494	0.4544	0.3996
SLE A1	0.2749	0.0973	0.3622	0.3173	0.4608	<b>0.8567</b>	0.3262	0.2125
SLE A2	0.2998	0.1048	0.3063	0.3958	0.4388	<b>0.8978</b>	0.3308	0.1716
SLE A3	0.2776	0.0214	0.2692	0.3294	0.3748	<b>0.8840</b>	0.3782	0.1855
SLPO 1	0.2974	0.1177	0.4221	0.4286	0.4575	0.3800	<b>0.9341</b>	0.1723
SLPO 2	0.2672	0.0623	0.3647	0.4422	0.4871	0.3897	<b>0.9514</b>	0.1674
SLPO 3	0.2029	0.0725	0.3386	0.3786	0.3768	0.3277	<b>0.9330</b>	0.1390
TRA N1	0.2825	0.0704	0.4156	0.3044	0.4634	0.2146	0.1857	<b>0.9491</b>
TRA N2	0.2733	0.0610	0.3796	0.2665	0.4454	0.2247	0.1438	<b>0.9483</b>
TRA N3	0.2472	0.0357	0.3760	0.3040	0.4222	0.1757	0.1576	<b>0.9565</b>

Though slightly different from the US sample, the India sample also exhibited high factor loadings as depicted in Table 29. AVE was also above 0.5 for all constructs as depicted in Table 27. The values suggest that the India sample also exhibits convergent validity.

<b>Table 29. Model 4: Loadings and Cross Loadings for India Sample</b>								
	CINT	LFIT	REFF	SEFF	SLCO	SLEA	SLPO	TRAN
CINT 1	<b>0.9000</b>	-0.3128	0.5020	0.4473	0.4579	0.4128	0.3710	0.3992
CINT 2	<b>0.9246</b>	-0.2993	0.5588	0.4950	0.4844	0.4506	0.4118	0.4896
CINT 3	<b>0.8726</b>	-0.2778	0.4102	0.4492	0.4606	0.4023	0.3909	0.3817
LFIT 1	-0.3152	<b>0.9206</b>	-0.4207	-0.4016	-0.4272	-0.3794	-0.3321	-0.3561
LFIT 2	-0.3212	<b>0.9341</b>	-0.4210	-0.3813	-0.4478	-0.3936	-0.3164	-0.3833
LFIT 3	-0.3180	<b>0.8961</b>	-0.4344	-0.3731	-0.4233	-0.3659	-0.3061	-0.3918
LFIT 4	-0.2449	<b>0.8971</b>	-0.4077	-0.3546	-0.3902	-0.3549	-0.2845	-0.3846
REFF 1	0.3927	-0.2325	<b>0.7274</b>	0.4935	0.4220	0.2949	0.3920	0.4941
REFF 2	0.5429	-0.4300	<b>0.8593</b>	0.6578	0.6046	0.4695	0.5343	0.5546
REFF 3	0.3946	-0.4312	<b>0.8439</b>	0.7157	0.6707	0.4763	0.5867	0.5677
SEFF 1	0.4603	-0.3508	0.6370	<b>0.8356</b>	0.6496	0.5064	0.5636	0.5317
SEFF 2	0.4311	-0.4211	0.7267	<b>0.8556</b>	0.6983	0.4924	0.5943	0.5374
SEFF 3	0.3775	-0.2276	0.5307	<b>0.7739</b>	0.4987	0.3343	0.4041	0.4658
SLC O1	0.4848	-0.4350	0.7190	0.7614	<b>0.9180</b>	0.5443	0.6993	0.6435
SLC O2	0.4719	-0.4307	0.6295	0.6939	<b>0.9460</b>	0.5610	0.7567	0.6662

SLC O3	0.5059	-0.4382	0.6401	0.6725	<b>0.9492</b>	0.6026	0.7419	0.6414
SLE A1	0.4425	-0.3765	0.4457	0.4806	0.4752	<b>0.8896</b>	0.4546	0.3514
SLE A2	0.4064	-0.3620	0.4924	0.5104	0.5956	<b>0.9359</b>	0.5785	0.3546
SLE A3	0.4466	-0.3893	0.4850	0.5145	0.5818	<b>0.9197</b>	0.5922	0.3877
SLPO 1	0.3936	-0.2724	0.5934	0.5838	0.6847	0.5340	<b>0.9045</b>	0.6222
SLPO 2	0.4096	-0.3352	0.6094	0.6290	0.7461	0.5717	<b>0.9454</b>	0.6214
SLPO 3	0.4126	-0.3402	0.5573	0.5823	0.7497	0.5645	<b>0.9443</b>	0.6314
TRA N1	0.4367	-0.3441	0.5970	0.5371	0.6101	0.3759	0.6100	<b>0.9324</b>
TRA N2	0.4175	-0.3898	0.6241	0.6101	0.6677	0.3829	0.6279	<b>0.9231</b>
TRA N3	0.4575	-0.4123	0.6130	0.5762	0.6382	0.3435	0.6163	<b>0.9109</b>

For the US sample, the square root of AVE for each construct was greater than the corresponding latent variable correlations. Table 30 presents latent variable correlations for the US sample with the square root of AVE along the diagonal. As depicted in Table 28, the factor loadings for each item exceeded cross loadings by at least 0.1 in every instance. These tests suggest that the US sample exhibits discriminant validity.

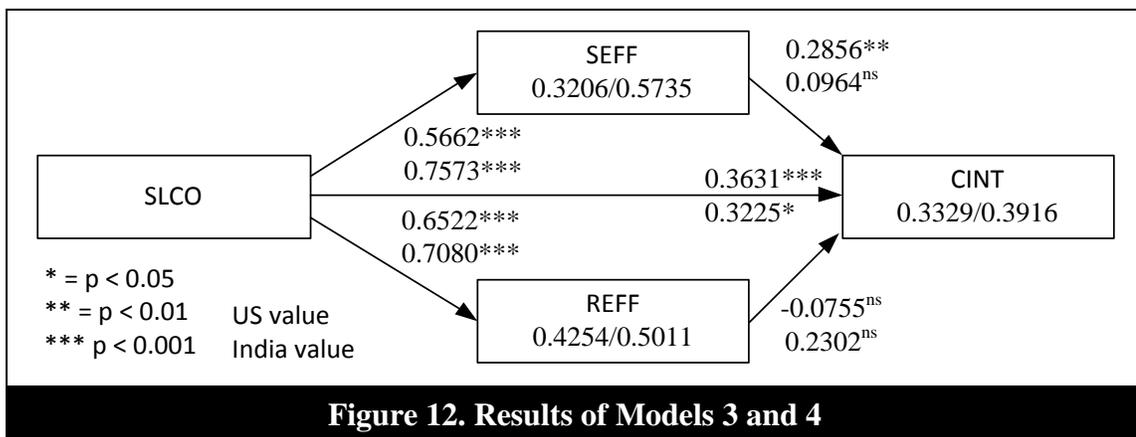
<b>Table 30. Model 3: Latent Variable Correlations for US Sample</b>								
	CINT	LFIT	REFF	SEFF	SLCO	SLEA	SLPO	TRAN
CINT	<b>0.9090</b>							
LFIT	0.1922	<b>0.9154</b>						
REFF	0.3882	0.1455	<b>0.8917</b>					
SEFF	0.4567	0.2113	0.6520	<b>0.9034</b>				
SLCO	0.4950	0.1951	0.6525	0.5664	<b>0.9081</b>			
SLEA	0.3231	0.0857	0.3566	0.3952	0.4842	<b>0.8797</b>		
SLPO	0.2755	0.0898	0.4010	0.4457	0.4731	0.3918	<b>0.9396</b>	
TRAN	0.2819	0.0591	0.4111	0.3066	0.4671	0.2162	0.1711	<b>0.9513</b>

For the India sample, the square root of AVE for each construct was also greater than the corresponding latent variable correlations. Table 31 presents latent variable correlations for the India sample with the square root of AVE along the diagonal. As depicted in Table 29, the factor loadings for each item exceeded cross loadings by at least 0.1 in every instance. These tests suggest that the India sample exhibits discriminant validity.

<b>Table 31. Model 4: Latent Variable Correlations for India Sample</b>								
	CINT	LFIT	REFF	SEFF	SLCO	SLEA	SLPO	TRAN
CINT	<b>0.8993</b>							
LFIT	-0.3301	<b>0.9121</b>						
REFF	0.5495	-0.4615	<b>0.8123</b>					
SEFF	0.5166	-0.4144	0.7753	<b>0.8224</b>				
SLCO	0.5201	-0.4637	0.7080	0.7574	<b>0.9378</b>			
SLEA	0.4701	-0.4099	0.5196	0.5490	0.6069	<b>0.9153</b>		
SLPO	0.4351	-0.3401	0.6293	0.6424	0.7810	0.5979	<b>0.9316</b>	
TRAN	0.4739	-0.4151	0.6635	0.6242	0.6937	0.3986	0.6706	<b>0.9222</b>

**Structural Model**

The structural model was assessed in SmartPLS using the second stage model which included the latent variable scores of the lower order constructs as items for the higher order constructs (Becker et al., 2012). Figure 12 presents the results of models 3 and 4, excluding the relationships that were identical in models 1 and 2. The identical relationships result in the same scores.



The data suggests that perceptions of social learning that favor compliant behavior encountered during childhood and adolescence increases perceptions of social learning that favor compliant behavior encountered during tenure at one’s previous job ( $\beta = 0.3110$ ; p-value < 0.001). Similarly, perceptions of social learning that favor compliant behavior encountered during childhood and adolescence increases perceptions of social learning that favor compliant behavior encountered during tenure at one’s current job ( $\beta = 0.2390$ ; p-value < 0.001). The data provides support for hypotheses 1a and 1b. The data also suggests that perceptions of social learning that favor compliant behavior

encountered during tenure at one's previous job increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.2882$ ;  $p\text{-value} < 0.001$ ). The data provides support for hypothesis 2.

The data provides evidence that perceptions of learning fit increase perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.1057$ ;  $p\text{-value} < 0.05$ ). The data provides support for hypothesis 3.

The data suggests that differential reinforcement increases perceptions of social learning in favor of compliance. The data provides evidence that perceptions of differential reinforcement from childhood and adolescence increase perceptions of social learning that favor compliant behavior encountered during childhood and adolescence ( $\beta = 0.4394$ ;  $p\text{-value} < 0.001$ ). The data also provides evidence that perceptions of differential reinforcement from one's previous job increase perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job ( $\beta = 0.3990$ ;  $p\text{-value} < 0.001$ ). Similarly, the data provides evidence that perceptions of differential reinforcement from one's current job increase perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.2478$ ;  $p\text{-value} < 0.001$ ). The data provides support for hypotheses h4a, h4b, and h4c.

The data provide evidence that perceptions of social learning that favor compliant behavior encountered during tenure at one's current job increase intentions to engage in security compliant behavior ( $\beta = 0.3631$ ;  $p\text{-value} < 0.001$ ). The data provides support for hypothesis 5.

Statistical evidence does not exist to suggest that organizational size influences social learning at one's current organization ( $\beta = -0.0751$ ;  $p\text{-value} > 0.05$ ). The data do not provide support for hypothesis 6. However, the data provide evidence that security training increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.3173$ ;  $p\text{-value} < 0.001$ ). Thus, the data provide support for hypothesis 7.

The data also provide evidence that perceptions of social learning that favor compliant behavior encountered during tenure at one's current job increase self-efficacy to comply with ISP ( $\beta = 0.5662$ ;  $p\text{-value} < 0.001$ ). Similarly, the data provide evidence that perceptions of social learning that favor compliant behavior encountered during tenure at one's current job increase response efficacy perceptions ( $\beta = 0.6522$ ;  $p\text{-value} < 0.001$ ). The data provides support for hypotheses 8 and 9. Finally, the data provide evidence that self-efficacy to comply with ISP increases intentions to engage in security compliant behavior ( $\beta = 0.2856$ ;  $p\text{-value} < 0.01$ ). Statistical evidence does not exist to suggest that response efficacy increases intentions to engage in security compliant behavior ( $\beta = -0.0755$ ;  $p\text{-value} > 0.05$ ). Thus, the data provide support for hypothesis 10, but not for hypothesis 11. Table 32 presents each hypothesis with its coefficient, t-value, p-value, and whether the hypothesis was supported by the data.

<b>Table 32. Model 3: Statistical Support for Hypotheses for US Sample</b>				
Relationship	Coefficient	t-value	p-value	Supported
h1a: SLEA → SLPO	0.3110	5.7391	$p < 0.001$	Yes
h1b: SLEA → SLCO	0.2390	3.8713	$p < 0.001$	Yes
h2: SLPO → SLCO	0.2882	4.6384	$p < 0.001$	Yes
h3: LFIT → SLCO	0.1057	2.0772	$p < 0.05$	Yes

h4a: DREA → SLEA	0.4394	7.5845	p < 0.001	Yes
h4b: DREP → SLPO	0.3990	7.0485	p < 0.001	Yes
h4c: DREC → SLCO	0.2478	4.0487	p < 0.001	Yes
h5: SLCO → CINT	0.3631	4.2522	p < 0.001	Yes
h6: SIZE → SLCO	-0.0751	0.7114	p > 0.05	No
h7: TRAN → SLCO	0.3173	4.8601	p < 0.001	Yes
h8: SLCO → SEFF	0.5662	9.0881	p < 0.001	Yes
h9: SLCO → REFF	0.6522	13.0911	p < 0.001	Yes
h10: SEFF → CINT	0.2856	2.6412	p < 0.01	Yes
h11: REFF → CINT	-0.0755	0.6219	p > 0.05	No

The Sobel mediation test (Sobel, 1982) was conducted to assess whether self-efficacy is a mediating variable. The Sobel test provides evidence that self-efficacy is a mediating variable (test statistic = 2.5348, p-value < 0.05). Because response efficacy was not significantly related to intentions to engage in proactive security behavior, the Sobel test was not used for response efficacy. Significance between the mediating variable and the dependent variable is a requirement for mediation (MacKinnon et al., 2002).

Age, education, gender, income, job position, organizational size, tenure, work experience were used as control variables. The data provide evidence that work experience increases intentions to engage in proactive security behavior ( $\beta = 0.2142$ ; p-value < 0.01). All other control variables were statistically insignificant. Table 33 presents the coefficient, t-value, p-value, and whether the relationship was supported for each control variable.

**Table 33. Model 3: Statistical Support for Control Variables for US Sample**

Control Variable	Coefficient	t-value	p-value	Supported
Age	-0.0533	0.6726	p > 0.05	No
Education	-0.0020	0.0316	p > 0.05	No
Gender	-0.0368	0.6433	p > 0.05	No
Income	-0.0486	0.8281	p > 0.05	No
IT employee	0.0093	0.1578	p > 0.05	No
Manager	-0.0925	1.3533	p > 0.05	No
Organizational size	-0.0751	1.2565	p > 0.05	No
Tenure	0.0254	0.4002	p > 0.05	No
Work experience	0.2142	2.6184	p < 0.01	Yes

The model explained 33.29 percent of the variance in intentions to engage in security compliant behavior, 42.54 percent of the variance in response efficacy, 32.06 percent of the variance in self-efficacy, 52.03 percent of the variance in social learning (current organization), 30.62 percent of the variance in social learning (previous organization), and 19.31 percent of the variance in social learning (adolescence and childhood). Table 34 presents the R<sup>2</sup> values for each endogenous construct.

**Table 34. Model 3: R<sup>2</sup> Values for Endogenous Constructs for US Sample**

Construct	R <sup>2</sup> Value
CINT	0.3329
REFF	0.4254
SEFF	0.3206
SLCO	0.5203
SLEA	0.1931
SLPO	0.3062

For the India sample, the data suggest that perceptions of social learning that favor compliant behavior encountered during childhood and adolescence increases perceptions of social learning that favor compliant behavior encountered during tenure at

one's previous job ( $\beta = 0.4421$ ;  $p\text{-value} < 0.001$ ). Similarly, perceptions of social learning that favor compliant behavior encountered during childhood and adolescence increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.1516$ ;  $p\text{-value} < 0.05$ ). The data provides support for hypotheses 1a and 1b. The data also suggests that perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.4118$ ;  $p\text{-value} < 0.001$ ). The data provides support for hypothesis 2.

The data provides evidence that perceptions of learning fit decrease perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = -0.1120$ ;  $p\text{-value} < 0.05$ ). The data provides support for hypothesis 3.

The data suggests that differential reinforcement increases perceptions of social learning in favor of compliance. The data provides evidence that perceptions of differential reinforcement from childhood and adolescence increase perceptions of social learning that favor compliant behavior encountered during childhood and adolescence ( $\beta = 0.6143$ ;  $p\text{-value} < 0.001$ ). The data also provides evidence that perceptions of differential reinforcement from one's previous job increase perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job ( $\beta = 0.3593$ ;  $p\text{-value} < 0.001$ ). Similarly, the data provides evidence that perceptions of differential reinforcement from one's current job increase perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.1449$ ;  $p\text{-value} < 0.01$ ). The data provides support for hypotheses h4a, h4b, and h4c.

The data provide evidence that perceptions of social learning that favor compliant behavior encountered during tenure at one's current job increase intentions to engage in security compliant behavior ( $\beta = 0.3225$ ;  $p\text{-value} < 0.05$ ). The data provides support for hypothesis 5.

Statistical evidence does not exist to suggest that organizational size influences social learning at one's current organization ( $\beta = -0.0090$ ;  $p\text{-value} > 0.05$ ). The data do not provide support for hypothesis 6. However, the data provide evidence that security training increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.2533$ ;  $p\text{-value} < 0.01$ ). Thus, the data provide support for hypothesis 7.

The data also provide evidence that perceptions of social learning that favor compliant behavior encountered during tenure at one's current job increase self-efficacy to comply with ISP ( $\beta = 0.7595$ ;  $p\text{-value} < 0.001$ ). Similarly, the data provide evidence that perceptions of social learning that favor compliant behavior encountered during tenure at one's current job increase response efficacy perceptions ( $\beta = 0.7121$ ;  $p\text{-value} < 0.001$ ). The data provides support for hypotheses 8 and 9. Finally, the data provide evidence that self-efficacy to comply with ISP increases intentions to engage in security compliant behavior ( $\beta = 0.0273$ ;  $p\text{-value} > 0.05$ ). Statistical evidence does not exist to suggest that response efficacy increases intentions to engage in security compliant behavior ( $\beta = 0.1417$ ;  $p\text{-value} > 0.05$ ). Thus, the data do not provide support for hypotheses 10 and 11. Table 35 presents each hypothesis with its coefficient, t-value, p-value, and whether the hypothesis was supported by the data.

**Table 35. Model 4: Statistical Support for Hypotheses for India Sample**

Relationship	Coefficient	t-value	p-value	Supported
h1a: SLEA → SLPO	0.4421	6.5756	p < 0.001	Yes
h1b: SLEA → SLCO	0.1517	2.3415	p < 0.05	Yes
h2: SLPO → SLCO	0.4118	4.1536	p < 0.001	Yes
h3: LFIT → SLCO	-0.1119	2.2860	p < 0.05	Yes
h4a: DREA → SLEA	0.6143	13.2120	p < 0.001	Yes
h4b: DREP → SLPO	0.3593	5.5215	p < 0.001	Yes
h4c: DREC → SLCO	0.1450	2.9604	p < 0.01	Yes
h5: SLCO → CINT	0.2945	2.4825	p < 0.05	Yes
h6: SIZE → SLCO	-0.0091	0.2610	p > 0.05	No
h7: TRAN → SLCO	0.2532	3.0286	p < 0.01	Yes
h8: SLCO → SEFF	0.7573	18.0734	p < 0.001	Yes
h9: SLCO → REFF	0.7080	16.4388	p < 0.001	Yes
h10: SEFF → CINT	0.0964	0.5890	p > 0.05	No
h11: REFF → CINT	0.2302	1.7772	p > 0.05	No

The Sobel mediation test (Sobel, 1982) was not conducted on the India sample because the paths leading from self-efficacy and response efficacy to intentions to engage in proactive security behavior were statistically insignificant. Thus, they are not mediators (MacKinnon et al., 2002).

Age, education, gender, income, job position, organizational size, tenure, work experience were used as control variables. The data provide evidence that education decreases intentions to engage in security compliant behavior ( $\beta = -0.1446$ ; p-value < 0.05). The data also provide evidence that being an IT employee decreases intentions to engage in security compliant behavior ( $\beta = -0.1684$ ; p-value < 0.05). All other control variables were statistically insignificant in the India sample. Table 36 presents the coefficient, t-value, p-value, and whether the relationship was supported for each control variable.

**Table 36. Model 4: Statistical Support for Control Variables for India Sample**

Control Variable	Coefficient	t-value	p-value	Supported
Age	0.0018	0.0229	p > 0.05	No
Education	-0.1446	2.5048	p < 0.05	Yes
Gender	0.0243	0.3632	p > 0.05	No
Income	-0.0030	0.0433	p > 0.05	No
IT employee	-0.1684	2.5314	p < 0.05	Yes
Manager	0.0908	1.3273	p > 0.05	No
Organizational size	0.0800	1.0967	p > 0.05	No
Tenure	-0.0265	0.3550	p > 0.05	No
Work experience	0.0269	0.2791	p > 0.05	No

The model explained 39.16 percent of the variance in intentions to engage in security compliant behavior, 50.11 percent of the variance in response efficacy, 57.35 percent of the variance in self-efficacy, 72.02 percent of the variance in social learning (current organization), 37.74 percent of the variance in social learning (previous organization), and 46.15 percent of the variance in social learning (adolescence and childhood). Table 37 presents the R<sup>2</sup> values for each endogenous construct.

**Table 37. Model 4: R<sup>2</sup> Values for Endogenous Constructs for India Sample**

Construct	R <sup>2</sup> Value
CINT	0.3916
REFF	0.5011
SEFF	0.5735
SLCO	0.7202
SLEA	0.3774
SLPO	0.4615

Comparing the US and India samples shows that the India sample exhibited higher coefficients for several relationships. The higher differences were most prominent in the relationships between social learning (childhood and adolescence) and social

learning (previous organization), between social learning (previous organization) and social learning (current organization), between differential reinforcement and social learning (childhood and adolescence), between social learning (current organization) and self-efficacy, and between response efficacy and intentions to engage in security compliant behavior. The US sample exhibited higher coefficients in the relationships between learning fit and social learning (current organization), between differential association and social learning (current organization), and between self-efficacy and intentions to engage in security compliant behavior. The samples also differed in the statistical significance of the path leading from self-efficacy to intentions to engage in security compliant behavior. The US sample exhibited a statistically significant path, but the path in the India sample was statistically insignificant. Table 38 presents the primary differences between the US and India samples.

<b>Table 38. Comparison of Path Coefficients for US and India Samples</b>		
Relationship	Coefficient (US – India)	Supported (US/India)
h1a: SLEA → SLPO	-0.1311	Yes/Yes
h1b: SLEA → SLCO	0.0873	Yes/Yes
h2: SLPO → SLCO	-0.1236	Yes/Yes
h3: LFIT → SLCO	0.2176	Yes/Yes
h4a: DREA → SLEA	-0.1749	Yes/Yes
h4b: DREP → SLPO	0.0397	Yes/Yes
h4c: DREC → SLCO	0.1028	Yes/Yes
h5: SLCO → CINT	0.0686	Yes/Yes
h6: SIZE → SLCO	-0.0660	No/No
h7: TRAN → SLCO	0.0641	Yes/Yes
h8: SLCO → SEFF	-0.1911	Yes/Yes
h9: SLCO → REFF	-0.0558	Yes/Yes
h10: SEFF → CINT	0.1892	Yes/No
h11: REFF → CINT	-0.3057	No/No

The India sample also exhibited higher  $R^2$  values for all of the endogenous constructs. The most substantial differences were in the  $R^2$  values for: self-efficacy, social learning (childhood and adolescence), social learning (previous organization), and social learning (previous organization). Table 39 presents differences between  $R^2$  values for the US and India samples.

<b>Table 39. Comparison of <math>R^2</math> Values for US and India Samples</b>	
Construct	$R^2$ Values (US – India)
CINT	-0.0587
REFF	-0.0757
SEFF	-0.2529
SLCO	-0.1999
SLEA	-0.1843
SLPO	-0.1553

### **Models 5 and 6: Security Risk-taking Behavior in the US and India**

Models 5 and 6 represent security risk-taking behavior in the US and India, respectively. The measurement model and structural model are examined below.

#### ***Measurement Model***

The US sample exhibited high composite reliabilities for all reflective scales. Composite reliabilities should exceed 0.70. The composite reliabilities for the US model exceeded 0.90 as depicted in Table 40, suggesting that the measures are reliable.

**Table 40. Model 5: AVE and Composite Reliability for US Sample**

	AVE	Composite Reliability
LFIT	0.8381	0.9539
SLCO	0.8254	0.9341
SLEA	0.7738	0.9112
SLPO	0.8828	0.9576
SRBI	0.9362	0.9778
TRAN	0.9050	0.9662

The India sample also exhibited high composite reliabilities for all reflective scales. All composite reliability scores exceeded 0.90 as depicted in Table 41. The composite reliability scores exceeded the recommended cutoff of 0.70, suggesting reliable measures.

**Table 41. Model 6: AVE and Composite Reliability for India Sample**

	AVE	Composite Reliability
LFIT	0.8320	0.9519
SLCO	0.8797	0.9564
SLEA	0.8377	0.9393
SLPO	0.8679	0.9517
SRBI	0.9314	0.9760
TRAN	0.8504	0.9446

The US sample exhibited high factor loadings as depicted in Table 42. AVE was also above 0.5 for all constructs as depicted in Table 40. The values suggest that the US sample exhibits convergent validity.

**Table 42. Model 5: Loadings and Cross Loadings for US Sample**

	LFIT	SLCO	SLEA	SLPO	SRBI	TRAN
LFIT1	<b>0.9301</b>	0.2252	0.0952	0.1064	-0.1378	0.0747
LFIT2	<b>0.9266</b>	0.2019	0.0847	0.0964	-0.1803	0.0462
LFIT3	<b>0.8901</b>	0.1158	0.0519	0.0290	-0.1633	0.0431
LFIT4	<b>0.9145</b>	0.1140	0.0626	0.0647	-0.1229	0.0401
SLCO1	0.1698	<b>0.8686</b>	0.4002	0.3941	-0.2775	0.4392
SLCO2	0.1731	<b>0.9512</b>	0.4715	0.4435	-0.2285	0.4298
SLCO3	0.1892	<b>0.9039</b>	0.4495	0.4544	-0.2085	0.3996
SLEA1	0.0973	0.4593	<b>0.8561</b>	0.3261	-0.1530	0.2125
SLEA2	0.1048	0.4401	<b>0.8979</b>	0.3307	-0.1530	0.1715
SLEA3	0.0214	0.3782	<b>0.8845</b>	0.3781	-0.1962	0.1855
SLPO1	0.1176	0.4563	0.3800	<b>0.9339</b>	-0.2181	0.1723
SLPO2	0.0622	0.4888	0.3898	<b>0.9515</b>	-0.2041	0.1674
SLPO3	0.0724	0.3800	0.3278	<b>0.9332</b>	-0.1980	0.1390
SRBI1	-0.1256	-0.2329	-0.1804	-0.1947	<b>0.9593</b>	-0.1332
SRBI2	-0.1815	-0.2521	-0.1775	-0.2277	<b>0.9686</b>	-0.1417
SRBI3	-0.1720	-0.2727	-0.1926	-0.2159	<b>0.9748</b>	-0.1689
TRAN1	0.0705	0.4618	0.2146	0.1857	-0.1525	<b>0.9491</b>
TRAN2	0.0610	0.4433	0.2246	0.1437	-0.1814	<b>0.9483</b>
TRAN3	0.0357	0.4214	0.1757	0.1575	-0.1025	<b>0.9565</b>

Though slightly different from the US sample, the India sample also exhibited high factor loadings as depicted in Table 43. AVE was also above 0.5 for all constructs as depicted in Table 41. The values suggest that the India sample also exhibits convergent validity.

**Table 43. Model 6: Loadings and Cross Loadings for India Sample**

	LFIT	SLCO	SLEA	SLPO	SRBI	TRAN
LFIT1	<b>0.9206</b>	-0.4271	-0.3794	-0.3321	0.1605	-0.3561
LFIT2	<b>0.9341</b>	-0.4471	-0.3936	-0.3164	0.1211	-0.3832
LFIT3	<b>0.8961</b>	-0.4228	-0.3659	-0.3062	0.0858	-0.3918
LFIT4	<b>0.8971</b>	-0.3903	-0.3549	-0.2845	0.1092	-0.3846
SLCO1	-0.4350	<b>0.9126</b>	0.5443	0.6992	-0.3773	0.6435

SLCO2	-0.4307	<b>0.9487</b>	0.5611	0.7567	-0.3852	0.6662
SLCO3	-0.4382	<b>0.9519</b>	0.6027	0.7419	-0.4123	0.6414
SLEA1	-0.3765	0.4747	<b>0.8896</b>	0.4546	-0.3075	0.3514
SLEA2	-0.3620	0.5966	<b>0.9359</b>	0.5785	-0.4022	0.3546
SLEA3	-0.3893	0.5823	<b>0.9197</b>	0.5922	-0.3301	0.3877
SLPO1	-0.2724	0.6833	0.5340	<b>0.9044</b>	-0.3445	0.6222
SLPO2	-0.3352	0.7470	0.5717	<b>0.9455</b>	-0.3514	0.6214
SLPO3	-0.3401	0.7516	0.5646	<b>0.9444</b>	-0.3010	0.6314
SRBI1	0.1483	-0.4436	-0.3722	-0.3714	<b>0.9719</b>	-0.3239
SRBI2	0.1001	-0.3856	-0.3703	-0.3482	<b>0.9618</b>	-0.3115
SRBI3	0.1275	-0.3737	-0.3607	-0.3068	<b>0.9615</b>	-0.2960
TRAN1	-0.3441	0.6100	0.3759	0.6100	-0.2759	<b>0.9325</b>
TRAN2	-0.3898	0.6676	0.3829	0.6278	-0.3367	<b>0.9232</b>
TRAN3	-0.4123	0.6376	0.3435	0.6163	-0.2764	<b>0.9108</b>

For the US sample, the square root of AVE for each construct was greater than the corresponding latent variable correlations. Table 44 presents latent variable correlations for the US sample with the square root of AVE along the diagonal. As depicted in Table 42, the factor loadings for each item exceeded cross loadings by at least 0.1 in every instance. These tests suggest that the US sample exhibits discriminant validity.

	LFIT	SLCO	SLEA	SLPO	SRBI	TRAN
LFIT	<b>0.9155</b>					
SLCO	0.1952	<b>0.9085</b>				
SLEA	0.0856	0.4853	<b>0.8797</b>			
SLPO	0.0897	0.4743	0.3918	<b>0.9396</b>		
SRBI	-0.1662	-0.2620	-0.1899	-0.2204	<b>0.9676</b>	
TRAN	0.0591	0.4655	0.2161	0.1711	-0.1538	<b>0.9513</b>

For the India sample, the square root of AVE for each construct was also greater than the corresponding latent variable correlations. Table 45 presents latent variable

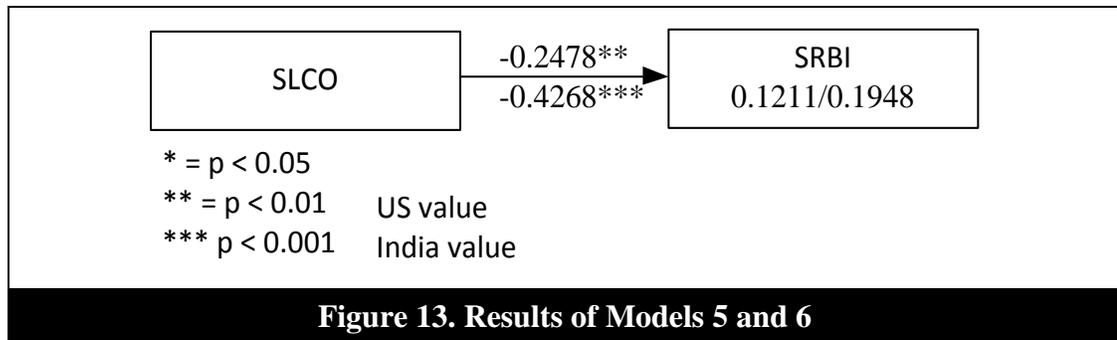
correlations for the India sample with the square root of AVE along the diagonal. As depicted in Table 43, the factor loadings for each item exceeded cross loadings by at least 0.1 in every instance. These tests suggest that the India sample exhibits discriminant validity.

**Table 45. Model 6: Latent Variable Correlations for India Sample**

	LFIT	SLCO	SLEA	SLPO	SRBI	TRAN
LFIT	<b>0.9121</b>					
SLCO	-0.4633	<b>0.9379</b>				
SLEA	-0.4099	0.6074	<b>0.9153</b>			
SLPO	-0.3402	0.7815	0.5979	<b>0.9316</b>		
SRBI	0.1309	-0.4177	-0.3812	-0.3562	<b>0.9651</b>	
TRAN	-0.4151	0.6933	0.3986	0.6706	-0.3224	<b>0.9222</b>

**Structural Model**

The structural model was assessed in SmartPLS using the second stage model which included the latent variable scores of the lower order constructs as items for the higher order constructs (Becker et al., 2012). Figure 13 presents the results of models 5 and 6, excluding redundant relationships presented in previous figures.



The data suggests that perceptions of social learning that favor compliant behavior encountered during childhood and adolescence increases perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job ( $\beta = 0.3110$ ;  $p\text{-value} < 0.001$ ). Similarly, perceptions of social learning that favor compliant behavior encountered during childhood and adolescence increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.2404$ ;  $p\text{-value} < 0.001$ ). The data provides support for hypotheses 1a and 1b. The data also suggests that perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.2894$ ;  $p\text{-value} < 0.001$ ). The data provides support for hypothesis 2.

The data provides evidence that perceptions of learning fit increase perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.1059$ ;  $p\text{-value} < 0.05$ ). The data provides support for hypothesis 3.

The data suggests that differential reinforcement increases perceptions of social learning in favor of compliance. The data provides evidence that perceptions of differential reinforcement from childhood and adolescence increase perceptions of social learning that favor compliant behavior encountered during childhood and adolescence ( $\beta = 0.4393$ ;  $p\text{-value} < 0.001$ ). The data also provides evidence that perceptions of differential reinforcement from one's previous job increase perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job ( $\beta = 0.3989$ ;  $p\text{-value} < 0.001$ ). Similarly, the data provides evidence that perceptions of

differential reinforcement from one's current job increase perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.2485$ ;  $p\text{-value} < 0.001$ ). The data provides support for hypotheses h4a, h4b, and h4c.

The data provide evidence that perceptions of social learning that favor compliant behavior encountered during tenure at one's current job decreases intentions to engage in security risk-taking behavior ( $\beta = -0.2478$ ;  $p\text{-value} < 0.01$ ). The data provides support for hypothesis 5.

Statistical evidence does not exist to suggest that organizational size influences social learning at one's current organization ( $\beta = -0.0333$ ;  $p\text{-value} > 0.05$ ). The data do not provide support for hypothesis 6. However, the data provide evidence that security training increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.3141$ ;  $p\text{-value} < 0.001$ ). Thus, the data provide support for hypothesis 7. Table 46 presents each hypothesis with its coefficient, t-value, p-value, and whether the hypothesis was supported by the data.

<b>Table 46. Model 5: Statistical Support for Hypotheses for US Sample</b>				
Relationship	Coefficient	t-value	p-value	Supported
h1a: SLEA → SLPO	0.3110	5.3920	$p < 0.001$	Yes
h1b: SLEA → SLCO	0.2404	4.2452	$p < 0.001$	Yes
h2: SLPO → SLCO	0.2894	4.2566	$p < 0.001$	Yes
h3: LFIT → SLCO	0.1059	2.1258	$p < 0.05$	Yes
h4a: DREA → SLEA	0.4393	7.1236	$p < 0.001$	Yes
h4b: DREP → SLPO	0.3989	8.1386	$p < 0.001$	Yes
h4c: DREC → SLCO	0.2485	4.2160	$p < 0.001$	Yes
h5: SLCO → SRBI	-0.2478	3.3320	$p < 0.01$	Yes
h6: SIZE → SLCO	-0.0333	0.7923	$p > 0.05$	No
h7: TRAN → SLCO	0.3141	4.3399	$p < 0.001$	Yes

Age, education, gender, income, job position, organizational size, tenure, work experience were used as control variables. All control variables were statistically insignificant. Table 47 presents the coefficient, t-value, p-value, and whether the relationship was supported for each control variable.

<b>Table 47. Model 5: Statistical Support for Control Variables for US Sample</b>				
Control Variable	Coefficient	t-value	p-value	Supported
Age	0.0227	0.2847	p > 0.05	No
Education	-0.0211	0.3339	p > 0.05	No
Gender	-0.1247	1.8888	p > 0.05	No
Income	-0.0362	0.5548	p > 0.05	No
IT employee	-0.1058	1.5680	p > 0.05	No
Manager	-0.0082	0.1230	p > 0.05	No
Organizational size	-0.0034	0.0489	p > 0.05	No
Scenario	0.0606	0.9761	p > 0.05	No
Tenure	0.1142	1.5954	p > 0.05	No
Work experience	-0.1503	1.6357	p > 0.05	No

The model explained 12.11 percent of the variance in intentions to engage in security risk-taking behavior, 52.06 percent of the variance in social learning (current organization), 30.62 percent of the variance in social learning (previous organization), and 19.30 percent of the variance in social learning (adolescence and childhood). Table 48 presents the R<sup>2</sup> values for each endogenous construct.

<b>Table 48. Model 5: R<sup>2</sup> Values for Endogenous Constructs for US Sample</b>	
Construct	R <sup>2</sup> Value
SLCO	0.5206
SLEA	0.1930
SLPO	0.3062
SRBI	0.1211

For the India sample, the data suggest that perceptions of social learning that favor compliant behavior encountered during childhood and adolescence increases perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job ( $\beta = 0.4422$ ;  $p\text{-value} < 0.001$ ). Similarly, perceptions of social learning that favor compliant behavior encountered during childhood and adolescence increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.1517$ ;  $p\text{-value} < 0.05$ ). The data provides support for hypotheses 1a and 1b. The data also suggests that perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.4128$ ;  $p\text{-value} < 0.001$ ). The data provides support for hypothesis 2.

The data provides evidence that perceptions of learning fit decrease perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = -0.1113$ ;  $p\text{-value} < 0.05$ ). The data provides support for hypothesis 3.

The data suggests that differential reinforcement increases perceptions of social learning in favor of compliance. The data provides evidence that perceptions of differential reinforcement from childhood and adolescence increase perceptions of social learning that favor compliant behavior encountered during childhood and adolescence ( $\beta = 0.6143$ ;  $p\text{-value} < 0.001$ ). The data also provides evidence that perceptions of differential reinforcement from one's previous job increase perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job ( $\beta = 0.3593$ ;  $p\text{-value} < 0.001$ ). Similarly, the data provides evidence that perceptions of

differential reinforcement from one's current job increase perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.1463$ ;  $p\text{-value} < 0.01$ ). The data provides support for hypotheses h4a, h4b, and h4c.

The data provide evidence that perceptions of social learning that favor compliant behavior encountered during tenure at one's current job decrease intentions to engage in security risk-taking behavior ( $\beta = -0.4268$ ;  $p\text{-value} < 0.001$ ). The data provides support for hypothesis 5.

Statistical evidence does not exist to suggest that organizational size influences social learning at one's current organization ( $\beta = -0.0097$ ;  $p\text{-value} > 0.05$ ). The data do not provide support for hypothesis 6. However, the data provide evidence that security training increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.2520$ ;  $p\text{-value} < 0.01$ ). Thus, the data provide support for hypothesis 7. Table 49 presents each hypothesis with its coefficient, t-value, p-value, and whether the hypothesis was supported by the data.

<b>Table 49. Model 6: Statistical Support for Hypotheses for India Sample</b>				
Relationship	Coefficient	t-value	p-value	Supported
h1a: SLEA → SLPO	0.4422	6.4941	$p < 0.001$	Yes
h1b: SLEA → SLCO	0.1517	2.2240	$p < 0.05$	Yes
h2: SLPO → SLCO	0.4128	4.5149	$p < 0.001$	Yes
h3: LFIT → SLCO	-0.1113	2.2442	$p < 0.05$	Yes
h4a: DREA → SLEA	0.6143	14.3512	$p < 0.001$	Yes
h4b: DREP → SLPO	0.3593	5.4948	$p < 0.001$	Yes
h4c: DREC → SLCO	0.1463	3.2221	$p < 0.01$	Yes
h5: SLCO → SRBI	-0.4268	6.3334	$p < 0.001$	Yes
h6: SIZE → SLCO	-0.0097	0.2917	$p > 0.05$	No
h7: TRAN → SLCO	0.2520	3.1539	$p < 0.01$	Yes

Age, education, gender, income, job position, organizational size, tenure, work experience were used as control variables. All control variables were statistically insignificant in the India sample. Table 50 presents the coefficient, t-value, p-value, and whether the relationship was supported for each control variable.

<b>Table 50. Model 6: Statistical Support for Control Variables for India Sample</b>				
Control Variable	Coefficient	t-value	p-value	Supported
Age	0.0941	0.8853	p > 0.05	No
Education	-0.0382	0.4719	p > 0.05	No
Gender	-0.0200	0.2998	p > 0.05	No
Income	-0.0397	0.6297	p > 0.05	No
IT employee	0.0870	1.0799	p > 0.05	No
Manager	-0.0426	0.7200	p > 0.05	No
Organizational size	0.0170	0.2086	p > 0.05	No
Scenario	-0.0637	0.8892	p > 0.05	No
Tenure	-0.0359	0.3246	p > 0.05	No
Work experience	-0.0147	0.1241	p > 0.05	No

The model explained 19.48 percent of the variance in intentions to engage in security risk-taking behavior, 72.09 percent of the variance in social learning (current organization), 37.74 percent of the variance in social learning (previous organization), and 46.15 percent of the variance in social learning (adolescence and childhood). Table 51 presents the R<sup>2</sup> values for each endogenous construct.

<b>Table 51. Model 6: R<sup>2</sup> Values for Endogenous Constructs for India Sample</b>	
Construct	R <sup>2</sup> Value
SLCO	0.7209
SLEA	0.3774
SLPO	0.4615
SRBI	0.1948

Comparing the US and India samples shows that the India sample exhibited higher coefficients for several relationships. The higher differences were most prominent in the relationships between social learning (childhood and adolescence) and social learning (previous organization), between social learning (previous organization) and social learning (current organization), and between differential reinforcement and social learning (childhood and adolescence). The US sample exhibited higher coefficients in the relationships between learning fit and social learning (current organization), between differential association and social learning (current organization), and between social learning (current organization) and intentions to engage in security risk-taking behavior. The same hypotheses were supported across both samples. Table 52 presents the primary differences between the US and India samples.

<b>Table 52. Comparison of Path Coefficients for US and India Samples</b>		
<b>Relationship</b>	<b>Coefficient (US – India)</b>	<b>Supported (US/India)</b>
h1a: SLEA → SLPO	-0.1312	Yes/Yes
h1b: SLEA → SLCO	0.0887	Yes/Yes
h2: SLPO → SLCO	-0.1234	Yes/Yes
h3: LFIT → SLCO	0.2172	Yes/Yes
h4a: DREA → SLEA	-0.1750	Yes/Yes
h4b: DREP → SLPO	0.0396	Yes/Yes
h4c: DREC → SLCO	0.1022	Yes/Yes
h5: SLCO → SRBI	0.1790	Yes/Yes
h6: SIZE → SLCO	-0.0236	No/No
h7: TRAN → SLCO	0.0621	Yes/Yes

The India sample also exhibited higher  $R^2$  values for all of the endogenous constructs. The most substantial differences were in the  $R^2$  values for: social learning (childhood and adolescence), social learning (previous organization), and social learning

(current organization). Table 53 presents differences between R<sup>2</sup> values for the US and India samples.

<b>Table 53. Comparison of R<sup>2</sup> Values for US and India Samples</b>	
Construct	R <sup>2</sup> Values (US – India)
SLCO	-0.2003
SLEA	-0.1844
SLPO	-0.1553
SRBI	-0.0737

### **Models 7 and 8: Security Damaging Behavior in the US and India**

Models 7 and 8 represent security damaging behavior in the US and India, respectively. The measurement model and structural model are examined below.

#### ***Measurement Model***

The US sample exhibited high composite reliabilities for all reflective scales. Composite reliabilities should exceed 0.70. The composite reliabilities for the US model exceeded 0.90 as depicted in Table 54, suggesting that the measures are reliable.

<b>Table 54. Model 7: AVE and Composite Reliability for US Sample</b>		
	AVE	Composite Reliability
LFIT	0.8381	0.9539
SDBI	0.8442	0.9420
SLCO	0.8254	0.9341
SLEA	0.7738	0.9112
SLPO	0.8828	0.9576
TRAN	0.9050	0.9662

The India sample also exhibited high composite reliabilities for all reflective scales. All composite reliability scores exceeded 0.90 as depicted in Table 55. The composite reliability scores exceeded the recommended cutoff of 0.70, suggesting reliable measures.

	AVE	Composite Reliability
LFIT	0.8320	0.9519
SDBI	0.9143	0.9697
SLCO	0.8797	0.9564
SLEA	0.8377	0.9393
SLPO	0.8679	0.9517
TRAN	0.8504	0.9446

The US sample exhibited high factor loadings as depicted in Table 56. AVE was also above 0.5 for all constructs as depicted in Table 54. The values suggest that the US sample exhibits convergent validity.

	LFIT	SDBI	SLCO	SLEA	SLPO	TRAN
LFIT1	<b>0.9301</b>	-0.0964	0.2251	0.0953	0.1064	0.0747
LFIT2	<b>0.9266</b>	-0.0669	0.2019	0.0847	0.0964	0.0462
LFIT3	<b>0.8900</b>	-0.1075	0.1157	0.0519	0.0290	0.0431
LFIT4	<b>0.9145</b>	-0.0710	0.1140	0.0626	0.0647	0.0401
SDBI1	-0.0879	<b>0.8824</b>	-0.2213	-0.2013	-0.1846	-0.0050
SDBI2	-0.1059	<b>0.9355</b>	-0.2433	-0.1825	-0.2252	-0.0362
SDBI3	-0.0599	<b>0.9375</b>	-0.2320	-0.1761	-0.1863	-0.0296
SLCO1	0.1699	-0.2815	<b>0.8695</b>	0.4003	0.3941	0.4392
SLCO2	0.1731	-0.2252	<b>0.9513</b>	0.4715	0.4435	0.4298
SLCO3	0.1892	-0.1824	<b>0.9029</b>	0.4495	0.4544	0.3996
SLEA1	0.0973	-0.2145	0.4595	<b>0.8562</b>	0.3262	0.2125

SLEA2	0.1048	-0.1694	0.4400	<b>0.8979</b>	0.3307	0.1715
SLEA3	0.0214	-0.1491	0.3779	<b>0.8844</b>	0.3781	0.1855
SLPO1	0.1176	-0.2242	0.4564	0.3800	<b>0.9339</b>	0.1723
SLPO2	0.0622	-0.1717	0.4887	0.3898	<b>0.9515</b>	0.1674
SLPO3	0.0724	-0.2198	0.3796	0.3278	<b>0.9332</b>	0.1390
TRAN1	0.0705	-0.0410	0.4619	0.2146	0.1857	<b>0.9491</b>
TRAN2	0.0610	-0.0407	0.4435	0.2246	0.1437	<b>0.9483</b>
TRAN3	0.0357	0.0093	0.4214	0.1757	0.1575	<b>0.9565</b>

Though slightly different from the US sample, the India sample also exhibited high factor loadings as depicted in Table 57. AVE was also above 0.5 for all constructs as depicted in Table 55. The values suggest that the India sample also exhibits convergent validity.

For the US sample, the square root of AVE for each construct was greater than the corresponding latent variable correlations. Table 58 presents latent variable correlations for the US sample with the square root of AVE along the diagonal. As depicted in Table 56, the factor loadings for each item exceeded cross loadings by at least 0.1 in every instance. These tests suggest that the US sample exhibits discriminant validity.

<b>Table 57. Model 8: Loadings and Cross Loadings for India Sample</b>						
	LFIT	SDBI	SLCO	SLEA	SLPO	TRAN
LFIT1	<b>0.9206</b>	0.1642	-0.4270	-0.3794	-0.3321	-0.3561
LFIT2	<b>0.9341</b>	0.1078	-0.4472	-0.3936	-0.3164	-0.3832
LFIT3	<b>0.8961</b>	0.0700	-0.4228	-0.3659	-0.3062	-0.3918
LFIT4	<b>0.8971</b>	0.1480	-0.3903	-0.3549	-0.2845	-0.3846
SDBI1	0.1414	<b>0.9724</b>	-0.2924	-0.2345	-0.2462	-0.2326
SDBI2	0.0914	<b>0.9356</b>	-0.1996	-0.2000	-0.1957	-0.1707
SDBI3	0.1418	<b>0.9603</b>	-0.2472	-0.2397	-0.2355	-0.2346
SLCO1	-0.4350	-0.2566	<b>0.9132</b>	0.5443	0.6992	0.6435
SLCO2	-0.4307	-0.2656	<b>0.9490</b>	0.5611	0.7567	0.6662

SLCO3	-0.4382	-0.2182	<b>0.9510</b>	0.6027	0.7419	0.6414
SLEA1	-0.3765	-0.2272	0.4747	<b>0.8896</b>	0.4546	0.3514
SLEA2	-0.3620	-0.2629	0.5964	<b>0.9359</b>	0.5785	0.3546
SLEA3	-0.3893	-0.1633	0.5819	<b>0.9197</b>	0.5922	0.3877
SLPO1	-0.2724	-0.1960	0.6835	0.5340	<b>0.9044</b>	0.6222
SLPO2	-0.3352	-0.2572	0.7472	0.5717	<b>0.9455</b>	0.6214
SLPO3	-0.3401	-0.2128	0.7512	0.5646	<b>0.9443</b>	0.6314
TRAN1	-0.3441	-0.1213	0.6102	0.3759	0.6100	<b>0.9325</b>
TRAN2	-0.3898	-0.2563	0.6678	0.3829	0.6278	<b>0.9232</b>
TRAN3	-0.4123	-0.2414	0.6377	0.3435	0.6163	<b>0.9108</b>

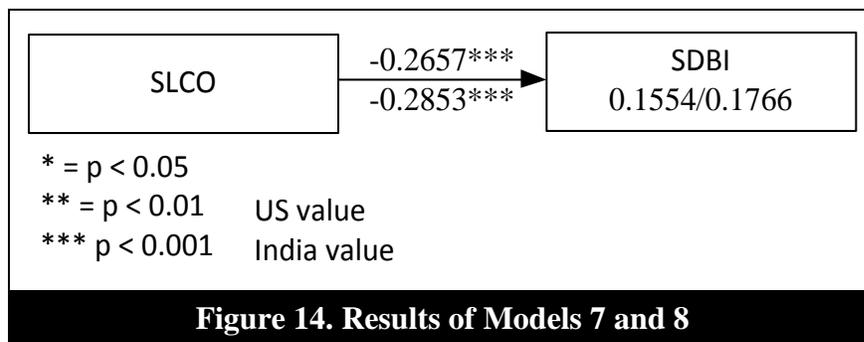
<b>Table 58. Model 7: Latent Variable Correlations for US Sample</b>						
	LFIT	SDBI	SLCO	SLEA	SLPO	TRAN
LFIT	<b>0.9155</b>					
SDBI	-0.0923	<b>0.9188</b>				
SLCO	0.1952	-0.2530	<b>0.9085</b>			
SLEA	0.0856	-0.2027	0.4852	<b>0.8797</b>		
SLPO	0.0897	-0.2168	0.4742	0.3918	<b>0.9396</b>	
TRAN	0.0591	-0.0262	0.4656	0.2161	0.1711	<b>0.9513</b>

For the India sample, the square root of AVE for each construct was also greater than the corresponding latent variable correlations. Table 59 presents latent variable correlations for the India sample with the square root of AVE along the diagonal. As depicted in Table 57, the factor loadings for each item exceeded cross loadings by at least 0.1 in every instance. These tests suggest that the India sample exhibits discriminant validity.

<b>Table 59. Model 8: Latent Variable Correlations for India Sample</b>						
	LFIT	SDBI	SLCO	SLEA	SLPO	TRAN
LFIT	<b>0.9121</b>					
SDBI	0.1336	<b>0.9562</b>				
SLCO	-0.4633	-0.2632	<b>0.9379</b>			
SLEA	-0.4099	-0.2368	0.6071	<b>0.9153</b>		
SLPO	-0.3402	-0.2389	0.7815	0.5979	<b>0.9316</b>	
TRAN	-0.4151	-0.2260	0.6935	0.3986	0.6706	<b>0.9222</b>

### *Structural Model*

The structural model was assessed in SmartPLS using the second stage model which included the latent variable scores of the lower order constructs as items for the higher order constructs (Becker et al., 2012). Figure 14 presents the results of models 5 and 6, excluding redundant relationships presented in previous figures.



The data suggests that perceptions of social learning that favor compliant behavior encountered during childhood and adolescence increases perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job ( $\beta = 0.3110$ ;  $p$ -value  $< 0.001$ ). Similarly, perceptions of social learning that favor compliant behavior encountered during childhood and adolescence increases perceptions of social

learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.2404$ ;  $p\text{-value} < 0.001$ ). The data provides support for hypotheses 1a and 1b. The data also suggests that perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.2893$ ;  $p\text{-value} < 0.001$ ). The data provides support for hypothesis 2.

The data provides evidence that perceptions of learning fit increase perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.1059$ ;  $p\text{-value} < 0.05$ ). The data provides support for hypothesis 3.

The data suggests that differential reinforcement increases perceptions of social learning in favor of compliance. The data provides evidence that perceptions of differential reinforcement from childhood and adolescence increase perceptions of social learning that favor compliant behavior encountered during childhood and adolescence ( $\beta = 0.4393$ ;  $p\text{-value} < 0.001$ ). The data also provides evidence that perceptions of differential reinforcement from one's previous job increase perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job ( $\beta = 0.3990$ ;  $p\text{-value} < 0.001$ ). Similarly, the data provides evidence that perceptions of differential reinforcement from one's current job increase perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.2484$ ;  $p\text{-value} < 0.001$ ). The data provides support for hypotheses h4a, h4b, and h4c.

The data provide evidence that perceptions of social learning that favor compliant behavior encountered during tenure at one's current job decreases intentions to engage in

security damaging behavior ( $\beta = -0.2657$ ;  $p\text{-value} < 0.001$ ). The data provides support for hypothesis 5.

Statistical evidence does not exist to suggest that organizational size influences social learning at one's current organization ( $\beta = -0.0335$ ;  $p\text{-value} > 0.05$ ). The data do not provide support for hypothesis 6. However, the data provide evidence that security training increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.3143$ ;  $p\text{-value} < 0.001$ ). Thus, the data provide support for hypothesis 7. Table 60 presents each hypothesis with its coefficient, t-value, p-value, and whether the hypothesis was supported by the data.

<b>Table 60. Model 7: Statistical Support for Hypotheses for US Sample</b>				
Relationship	Coefficient	t-value	p-value	Supported
h1a: SLEA → SLPO	0.3110	5.0632	$p < 0.001$	Yes
h1b: SLEA → SLCO	0.2404	3.6362	$p < 0.001$	Yes
h2: SLPO → SLCO	0.2893	3.9034	$p < 0.001$	Yes
h3: LFIT → SLCO	0.1059	2.2863	$p < 0.05$	Yes
h4a: DREA → SLEA	0.4393	8.4752	$p < 0.001$	Yes
h4b: DREP → SLPO	0.3990	7.4569	$p < 0.001$	Yes
h4c: DREC → SLCO	0.2484	4.6662	$p < 0.001$	Yes
h5: SLCO → SDBI	-0.2657	3.8235	$p < 0.001$	Yes
h6: SIZE → SLCO	-0.0335	0.7127	$p > 0.05$	No
h7: TRAN → SLCO	0.3143	4.5574	$p < 0.001$	Yes

Age, education, gender, income, job position, organizational size, tenure, work experience were used as control variables. The data provide evidence that age increases intentions to engage in security damaging behavior ( $\beta = 0.1820$ ;  $p\text{-value} < 0.05$ ). The data also provide evidence that being an IT employee increases intentions to engage in security damaging behavior ( $\beta = 0.2438$ ;  $p\text{-value} < 0.01$ ). All other control variables were

statistically insignificant. Table 61 presents the coefficient, t-value, p-value, and whether the relationship was supported for each control variable.

<b>Table 61. Model 7: Statistical Support for Control Variables for US Sample</b>				
Control Variable	Coefficient	t-value	p-value	Supported
Age	0.1820	2.0251	p < 0.05	Yes
Education	-0.0767	1.0386	p > 0.05	No
Gender	-0.0383	0.6026	p > 0.05	No
Income	0.0540	0.8357	p > 0.05	No
IT employee	0.2438	3.2743	p < 0.01	Yes
Manager	0.0763	1.1064	p > 0.05	No
Organizational size	0.0498	0.8593	p > 0.05	No
Scenario	0.0721	1.2012	p > 0.05	No
Tenure	-0.0471	0.6431	p > 0.05	No
Work experience	-0.0814	0.7993	p > 0.05	No

The model explained 15.54 percent of the variance in intentions to engage in security damaging behavior, 52.05 percent of the variance in social learning (current organization), 30.62 percent of the variance in social learning (previous organization), and 19.30 percent of the variance in social learning (adolescence and childhood). Table 62 presents the R<sup>2</sup> values for each endogenous construct.

<b>Table 62. Model 7: R<sup>2</sup> Values for Endogenous Constructs for US Sample</b>	
Construct	R <sup>2</sup> Value
SDBI	0.1554
SLCO	0.5205
SLEA	0.1930
SLPO	0.3062

For the India sample, the data suggest that perceptions of social learning that favor compliant behavior encountered during childhood and adolescence increases

perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job ( $\beta = 0.4422$ ; p-value  $< 0.001$ ). Similarly, perceptions of social learning that favor compliant behavior encountered during childhood and adolescence increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.1513$ ; p-value  $< 0.05$ ). The data provides support for hypotheses 1a and 1b. The data also suggests that perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.4129$ ; p-value  $< 0.001$ ). The data provides support for hypothesis 2.

The data provides evidence that perceptions of learning fit decrease perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = -0.1113$ ; p-value  $< 0.05$ ). The data provides support for hypothesis 3.

The data suggests that differential reinforcement increases perceptions of social learning in favor of compliance. The data provides evidence that perceptions of differential reinforcement from childhood and adolescence increase perceptions of social learning that favor compliant behavior encountered during childhood and adolescence ( $\beta = 0.6143$ ; p-value  $< 0.001$ ). The data also provides evidence that perceptions of differential reinforcement from one's previous job increase perceptions of social learning that favor compliant behavior encountered during tenure at one's previous job ( $\beta = 0.3593$ ; p-value  $< 0.001$ ). Similarly, the data provides evidence that perceptions of differential reinforcement from one's current job increase perceptions of social learning

that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.1462$ ;  $p\text{-value} < 0.01$ ). The data provides support for hypotheses h4a, h4b, and h4c.

The data provide evidence that perceptions of social learning that favor compliant behavior encountered during tenure at one's current job decrease intentions to engage in security damaging behavior ( $\beta = -0.2853$ ;  $p\text{-value} < 0.001$ ). The data provides support for hypothesis 5.

Statistical evidence does not exist to suggest that organizational size influences social learning at one's current organization ( $\beta = -0.0091$ ;  $p\text{-value} > 0.05$ ). The data do not provide support for hypothesis 6. However, the data provide evidence that security training increases perceptions of social learning that favor compliant behavior encountered during tenure at one's current job ( $\beta = 0.2522$ ;  $p\text{-value} < 0.001$ ). Thus, the data provide support for hypothesis 7. Table 63 presents each hypothesis with its coefficient, t-value, p-value, and whether the hypothesis was supported by the data.

**Table 63. Model 8: Statistical Support for Hypotheses for India Sample**

Relationship	Coefficient	t-value	p-value	Supported
h1a: SLEA $\rightarrow$ SLPO	0.4422	6.0862	$p < 0.001$	Yes
h1b: SLEA $\rightarrow$ SLCO	0.1513	2.2648	$p < 0.05$	Yes
h2: SLPO $\rightarrow$ SLCO	0.4129	4.5418	$p < 0.001$	Yes
h3: LFIT $\rightarrow$ SLCO	-0.1113	2.0337	$p < 0.05$	Yes
h4a: DREA $\rightarrow$ SLEA	0.6143	12.4408	$p < 0.001$	Yes
h4b: DREP $\rightarrow$ SLPO	0.3593	5.6997	$p < 0.001$	Yes
h4c: DREC $\rightarrow$ SLCO	0.1462	3.3463	$p < 0.001$	Yes
h5: SLCO $\rightarrow$ SDBI	-0.2853	4.0063	$p < 0.001$	Yes
h6: SIZE $\rightarrow$ SLCO	-0.0091	0.2656	$p > 0.05$	No
h7: TRAN $\rightarrow$ SLCO	0.2522	3.5611	$p < 0.001$	Yes

Age, education, gender, income, job position, organizational size, tenure, work experience were used as control variables. All control variables were statistically insignificant in the India sample. Table 64 presents the coefficient, t-value, p-value, and whether the relationship was supported for each control variable.

<b>Table 64. Model 8: Statistical Support for Control Variables for India Sample</b>				
Control Variable	Coefficient	t-value	p-value	Supported
Age	-0.1350	1.1814	p > 0.05	No
Education	-0.1113	1.0881	p > 0.05	No
Gender	-0.0524	0.7664	p > 0.05	No
Income	-0.0056	0.0720	p > 0.05	No
IT employee	0.1013	1.2793	p > 0.05	No
Manager	-0.0322	0.3654	p > 0.05	No
Organizational size	-0.1377	1.9097	p > 0.05	No
Scenario	0.1224	1.4656	p > 0.05	No
Tenure	0.1236	1.5269	p > 0.05	No
Work experience	-0.0901	0.6804	p > 0.05	No

The model explained 17.66 percent of the variance in intentions to engage in security compliant behavior, 72.09 percent of the variance in social learning (current organization), 37.74 percent of the variance in social learning (previous organization), and 46.15 percent of the variance in social learning (adolescence and childhood). Table 65 presents the R<sup>2</sup> values for each endogenous construct.

<b>Table 65. Model 8: R<sup>2</sup> Values for Endogenous Constructs for India Sample</b>	
Construct	R <sup>2</sup> Value
SDBI	0.1766
SLCO	0.7209
SLEA	0.3774
SLPO	0.4615

Comparing the US and India samples shows that the India sample exhibited higher coefficients for several relationships. The higher differences were most prominent in the relationships between social learning (childhood and adolescence) and social learning (previous organization), between social learning (previous organization) and social learning (current organization), and between differential reinforcement and social learning (childhood and adolescence). The US sample exhibited higher coefficients in the relationships between learning fit and social learning (current organization), between differential association and social learning (current organization). The same hypotheses were supported across both samples. Table 66 presents the primary differences between the US and India samples.

<b>Table 66. Comparison of Path Coefficients for US and India Samples</b>		
Relationship	Coefficient (US – India)	Supported (US/India)
h1a: SLEA → SLPO	-0.1312	Yes/Yes
h1b: SLEA → SLCO	0.0891	Yes/Yes
h2: SLPO → SLCO	-0.1236	Yes/Yes
h3: LFIT → SLCO	0.2172	Yes/Yes
h4a: DREA → SLEA	-0.1750	Yes/Yes
h4b: DREP → SLPO	0.0397	Yes/Yes
h4c: DREC → SLCO	0.1022	Yes/Yes
h5: SLCO → SRBI	0.0196	Yes/Yes
h6: SIZE → SLCO	-0.0244	No/No
h7: TRAN → SLCO	0.0621	Yes/Yes

The India sample also exhibited higher  $R^2$  values for all of the endogenous constructs. The most substantial differences were in the  $R^2$  values for: social learning (childhood and adolescence), social learning (previous organization), and social learning

(current organization). Table 67 presents differences between  $R^2$  values for the US and India samples.

<b>Table 67. Comparison of <math>R^2</math> Values for US and India Samples</b>	
<b>Construct</b>	<b><math>R^2</math> Values (US – India)</b>
SDBI	-0.0212
SLCO	-0.2004
SLEA	-0.1844
SLPO	-0.1553

## **CHAPTER IX**

### **DISCUSSION**

This study provides an in-depth analysis of the effect social learning has on information security behaviors. The review in this study provides evidence that social forms of control, such as the social learning environment, are underrepresented in the literature. However, the few variables that have been used to examine the effect of social influence have demonstrated that social variables strongly explain security behavior. Thus, to provide a more robust examination of social controls, this study uses Akers' social learning theory to explain and predict why and how the social environment influences information security behaviors. The paper also seeks to understand how previous learning experiences influence security behaviors. Little research has been conducted to determine the external sources of influence that explain why employees behave as they do within their current organization. Thus, we examine general rule-related social learning in childhood and adolescence, and security-specific learning encountered in individuals' previous and current job positions.

In order to examine these ideas, qualitative interviews were conducted with 20 employees who had worked for at least two organizations. Although ASLT was the primary guiding framework for the interviews, theoretical sensitization was used to ensure that multiple ideas and perspectives were considered. From the qualitative

interviews, general patterns emerged. These patterns were explored more fully through an online survey of US and India respondents. The quantitative results confirm many of the qualitative insights gained during the interviews. The contributions of the study are now discussed.

### **Theoretical Contributions**

The paper provides insight into the study of social learning and into the study of information security behaviors.

#### ***Contributions to Social Learning Theories***

In this study, we examined concepts from Akers' social learning theory and Bandura's social learning theory. Akers' social learning theory is a prominent criminological theory and Bandura's social learning theory is a prominent sociological theory. First, based on insight from the qualitative study, we find that Akers' representation of differential association as a reflective dimension of social learning may be somewhat misguided in studies of employee behavior in organizations. The qualitative study suggests that differential reinforcement is highly contextual and may not have the lasting effect on behavior suggested by Akers. Individuals change their behavior from one context to another because of changes in reinforcement in those environments. Thus, we find that reinforcement acts more as a contextual motivator. That is, reinforcement provides motivation to follow the behaviors learned through the social learning process. As such, we present differential reinforcement as a dependent variable influencing the social learning process. Since our study was primarily concerned with social learning in organizational settings, we cannot make claims about differential reinforcement in other

settings. Akers' social learning theory has been used to study a number of behaviors, such as youth smoking and alcohol use. In these situations, reinforcement may be less contextual due to clearer societal perceptions of smoking and alcohol use among youth. In these situations, it may be appropriate to examine differential reinforcement as a dimension of social learning.

Second, this study finds that social learning from previous life-periods may influence social learning in one's current job. Although Akers' suggests that social learning is mostly stable and should affect beliefs and behavior across groups (Ronald L. Akers, 2009), few studies have examined social learning beliefs across groups (i.e., organizations). And no study to our knowledge has examined social learning across organizations in the context of policy compliance and noncompliance. Through the qualitative and quantitative studies, we show that social learning from previous life-periods, namely from childhood and from a previous organization, does have a substantial influence on one's current beliefs, intentions, and behaviors. The quantitative models explained 50 percent of the variance in current, security-specific social learning in the US sample and 70 percent of the variance in the India sample. These  $R^2$  values represent strong effect sizes in the social sciences. Although this study shows that previous life-periods influence social learning in the present, much of the variance is still unexplained (between 30-50 percent). This confirms Akers' assertion that social learning is mostly stable, but that it can also be influenced by context (Ronald L. Akers, 2009).

Third, this study identifies learning fit as an important construct when examining social learning from previous life-periods. As evidenced in the study, social learning from

previous life-periods has an influence on current learning. Values, beliefs, and behaviors learned earlier in life are somewhat stable. As evidenced in the interviews, these stable beliefs can be viewed as an individual's preferred values, beliefs, and behaviors. However, in organizations, individuals may be asked to act differently than their preferred *modus operandi*. Through the interviews and survey, we identify learning fit as another motivator of social learning to complement reinforcement. Individuals feel comfortable operating under their preferred values, beliefs, and behaviors. When the social environment supports their preferred values, there is no conflict for the employee and the employee acts according to their preferred values, beliefs, and behaviors. However, when there is not a fit between the social environment and an individual's learned values, beliefs, and behaviors, discomfort exists. The individual is torn between two sets of values and beliefs and hesitates between the different value systems. This leads to only a partial adoption of the social learning beliefs shared in the social environment.

Finally, we compare Akers' social learning theory with Bandura's social learning theory as models to explain and predict employees' security behaviors in organizations. Through the quantitative study, we find that Akers' social learning construct is strong predictor of security behavior. We find that Akers' social learning construct is partially mediated by self-efficacy, from Bandura's social learning theory. This result suggests that both learning theories can provide insight. It also suggests that Bandura's social learning theory alone does not offer a complete perspective of the social learning environment. This finding also challenges Akers' assertion that self-efficacy is not a

strong explanation for behavior. We find that self-efficacy is important in certain circumstances. However, we only find that self-efficacy is a strong predictor of behavior in the US sample. In the India sample, self-efficacy was not a statistically significant predictor of security behavior. One possible explanation for this finding is the cultural differences between the US and India. The national culture in India is more collectivistic than the individualistic culture in the US. The focus on collectivism in India may place greater emphasis on the need to adhere to socially distributed values and standards. Self-efficacy is an individualistic assessment of one's ability to perform a task. Thus, it may be that self-efficacy is of less importance when compared with the social learning environment in collectivist cultures. Additionally, Bandura's self-efficacy construct exhibited mixed results across the models, while social learning was more consistent. This finding suggests that Akers' social learning theory may provide a better explanation of behavior as compared to Bandura's social learning theory. These assertions should be further tested.

### ***Contributions to Information Security Research***

The study also provides important insight into the study of information security behaviors. First, we provide further evidence that social influence is an important construct in the study of information security behavior. Informal, social control may exert greater influence over behavior than formal, administrative control (Ghoshal, Korine, & Szulanski, 1994; Lange, 2008). The few simple examinations of informal control in behavioral information security research also show the relative strength of informal controls (Herath & Rao, 2009a, 2009b). By failing to adequately examine informal, social

controls, behavioral information security research has missed a crucial explanatory and predictive system of control. This study identifies a social learning construct that can be used in future research.

Second, this study draws attention to the importance of considering previous life-periods when studying information security behavior. Behavioral InfoSec research has noted the importance of examining different time-periods (Willison & Warkentin, 2013). However, those time periods have been limited to cross-sectional examinations in a single organization. Few, if any, studies examine influences external to the organization. This study demonstrates that employees' security beliefs and behaviors are heavily influenced by external sources. Without this knowledge, it is difficult to determine how to combat noncompliant behavior or how to support compliant behavior. Understanding how influential learning in previous life-periods is can help researchers develop controls to build on positive learning and correct negative learning.

Third, this study identifies how the organization may be able to influence social learning in favor of compliant behavior. The qualitative study identifies two high-level types of employees, employees who have been socialized in previous life-periods to believe that rules are unimportant and employees who have been socialized in previous life-periods to believe that rules are important. Based on qualitative insight, we identified different ways to manage these two types of employees. Individuals who believe that rules are unimportant need some form of external influence to prompt them to pay attention to and follow social norms in favor of compliant behavior. Following rules is contrary to their preferred value system. In many of the interviews, the motivator that

influenced these employees was fear of formal sanctions, such as termination. Employees who believed that rules were unimportant were willing to adopt social learning in favor of rule compliance when sanctions were known.

Managing employees who believe that rules are important is different. These individuals were not motivated by sanctions. Although they knew the sanctions existed and were also afraid of them, their behavior was more motivated by internal drives. They also seemed to take comfort in the existence of formal control mechanisms such as sanctions. In fact, some of these employees even helped to establish stricter rules and more secure working environments. Their values provide intrinsic motivation to engage in secure behaviors and follow organizational policy. These individuals simply need an environment that promotes rule-following behavior. However, based on the interviews, it is clear that these environments do not always exist. When faced with environments that do not support rule-following behavior, these individuals experience discomfort and may uneasily abandon protective behaviors to follow the social norms.

The quantitative study provides similar insight. The quantitative study suggests that individuals are more likely to notice and follow social learning in favor of compliance when compliant behaviors are reinforced through formal and informal reward and punishment. Similarly, individuals are more likely to notice and adopt compliant social beliefs when their own beliefs match the dominant beliefs in the social environment.

Third, we find that the social learning construct may be a useful addition to the study of protection motivation behaviors. Protection motivation theory and fear appeals

theory, two similar and complementary theories, are commonly used in information security research to explain employees' security behaviors (Herath & Rao, 2009b; Johnston & Warkentin, 2010; Johnston, Warkentin, & Siponen, 2015; Vance et al., 2012). This study demonstrates that social learning influences self-efficacy and response efficacy and is partially mediated by self-efficacy. Thus, social learning can be added to protection motivation theory and fear appeals theory as a predictor of coping appraisals (i.e., self-efficacy and response efficacy).

Fourth, the study finds interesting, yet mixed results with control variables across the eight models. In the US sample, IT employees exhibited higher intentions to engage in proactive security behavior than non-IT employees. However, they also exhibited higher intentions to engage in security damaging behavior than non-IT employees. This is somewhat alarming. IT employees tend to have elevated access to information systems to perform their job duties. They are also more experienced users of IT and may be better able to launch attacks against the organization. Although it is expected that IT employees would be more engaged in proactive responsibilities because of their responsibility over organizational IT, it is alarming that they are also more intent on damaging those same systems than non-IT employees.

In the India sample, IT employees exhibited lower intentions to engage in security compliant behavior than non-IT employees, but did not exhibit higher intentions to engage in proactive security behavior than non-IT employees. This is also concerning. One possible explanation for the lower intentions to engage in security compliant behavior is that IT employees believe that they know how to protect the organization

better than is mandated in the information security policy. Although this may be positive if the IT employee truly knows better than the policy, it may be damaging when IT employees don't know better than the policy. IT is also concerning that IT employees in India did not exhibit higher intentions to engage in proactive security behavior than non-IT employees. As the primary defense against security threats, IT employees should be proactively engaged in securing information systems.

Other findings suggest that in India, education decreases intentions to engage in security compliant behaviors. Similarly, in the US sample, education decreases proactive security behavior. Again, one possible explanation is that educated individuals feel that they know better how to protect computers better than policy or that policy is over cautious. Although education decreased positive security behavior, work experience increased security compliant behavior in the US.

### ***International Contributions***

This study also highlights some important distinctions between security practices across nations. From the quantitative study, it is apparent from path coefficients and  $R^2$  values that in India, social learning has a stronger influence on social learning across time periods and on employees' intentions to engage in positive security behavior and avoid negative security behavior. This can likely be explained by the predominantly collectivist national culture in India (Hofstede et al., 2010). Social collectives are of greater importance in India than in the individualistic US culture. Thus, it stands to reason that Indians will be more concerned with social influence and adhering to the collective influence of peers. This may also explain why self-efficacy was not influential on

behavior in the presence of the social learning construct. Self-efficacy is a construct that represents individualistic perceptions. When adopted as a covariate with social learning, the importance of self-efficacy may have been diminished by the importance of the goals and beliefs of the social collective.

The study also shows that learning fit increases social learning in favor of compliance in the US, but decreases social learning in favor of compliance in India. The data show that the means for learning fit in the US (3.1498), where 4 means perfect fit, are higher than the mean in India (2.1929). Further, the India sample also shows that the respondents felt that the organization valued security more than they did compared to the US sample. This partially explains the positive coefficient in the US sample and the negative coefficient in the India sample. One possible explanation for the difference is the greater power distance between employees and employers in India compared to the US (Hofstede et al., 2010) Greater power distance may lead to perceptions that rules are stricter (Ortega, Giannotta, & Ciairano, 2013). The perceptions of strictness may cause the rules to appear more unreasonable, thereby decreasing perceptions of learning fit. These assertions should be explored further in future research.

### **Managerial Contributions**

The results of this study provide important direction for managers. First, the results highlight possible changes to hiring procedures, particularly in organizations with highly confidential information. The study shows that social learning from previous life-periods, including previous employers can influence social learning perceptions in the current organization, thereby influence intentions to engage in secure behavior. Hiring

managers should begin to consider the security-related socialization that individuals experience in prior jobs and general, rule-related socialization in previous life-periods. Such practices may be particularly important when hiring individuals to work in very secure areas with highly sensitive information. Similarly, hiring managers should carefully examine the fit between the employee's preferred values and beliefs pertaining to rules and information security, and the values and beliefs that exist in the organizational environment. Greater fit can increase motivation to engage in secure behaviors and avoid negative security behaviors.

Second, managers may be able to focus less on influencing individual users and more on the social learning environment. The social learning environment has a strong influence on security intentions. Thus, if managers are able to influence the social learning environment, they are likely to see more widespread individual behavioral improvements. This study shows that managers can influence social learning by ensuring that reinforcement is in place to encourage positive behavior and to discourage negative behavior. Developing a strong social learning environment that favors compliant behavior is particularly motivating for individuals who believe, in general, that rules are important. Many employees simply need support from management and the social environment to prompt positive security behavior. Although punishment has its place to deter individuals who do not believe rules are important, social support is the greatest motivator for individuals who believe in rule following.

## **Limitations and Future Research**

Although the study provided interesting results, it was not without limitations. One of the largest limitations of the study was time. Because we studied social learning across contexts, time is an important factor. Ideally, we would have tracked employees' social learning experiences through childhood and across several job transitions through a longitudinal study. A longitudinal study would provide a more robust examination of normative influence across time. However, our time was limited and it was not feasible to conduct a longitudinal study of the length required to assess the variables in the study. Therefore, we relied on self-report methods of social learning in prior organizations and life-periods. Although this is a limitation, life experiences can be collected and analyzed from a single interaction between the researcher and participant (Presser, 2008). Rather than examine social learning in different periods, we studied how perceptions of social learning in different periods influence social learning perceptions in one's current organization. Future research should consider examining individuals as they transition to a new job. Following individuals through a transition of this sort could provide new insight to our model.

The focus on social learning in prior life periods also limits the study to those who have had a least two jobs in their lifetime. Although this somewhat limits the extension of the model to new entrants to the job market, this study contributes to research on ASLT and information security behavior by examining social learning across different groups. Thus, we made a tradeoff. Future research should consider the external influences that influence social learning perceptions for new entrants to the job market.

Additionally, time limits our ability to explore other types of understudied controls. For example, the interaction between controls with extrinsic and intrinsic motivational orientations is not well represented by ASLT. Theories of motivation, such as self-determination theory (Ryan & Deci, 1985, 2000), would be better suited for such an examination. To explore interactions between controls with different motivational orientations, a separate exploration, model, and instrument would need to be designed and conducted. Ideally, this study would produce a developed theory of security-related corruption control. However, such an effort will require multiple studies over an extended period of time. Although this is a limitation of our study, it also presents opportunities for future studies.

Further, we rely primarily on survey research to test the theoretical model. While survey research is useful and widely used in the IS discipline, it possesses limitations. First, we rely on self-report data from employees. While self-report surveys are used heavily in behavioral InfoSec research (Crossler et al., 2013), self-reports may not accurately reflect the phenomenon under study. Rather, self-reports reflect perceptions of the phenomenon. Thus, our examination is scoped to employee perceptions and intentions. Finally, surveys are not always representative of the larger population unless random sampling is used. We employed a research panel from Amazon Turk. In many studies, diversity in respondents is set as an alternative to random sampling, which research panels often provide (Posey et al., 2013). Randomly sampling from the population of all employees is not realistic. Thus, we relied on research panels to ensure a diverse and heterogeneous population.

We also obtained differing results between the qualitative and quantitative studies regarding the influence of organizational size on social learning that favors compliance with information security policies. In the qualitative study, organizational size was identified as a contextual factor that increased the likelihood that security policies were instituted within the organization and that social support was present to promote adherence to the security policies. Smaller organizations were less likely to have strong policies and social support. However, in the quantitative study, the relationships between organizational size and social learning was not statistically significant. It may be that other factors, such as reinforcement, are more important to the social learning process than organizational size. It could also be that industry and organizational size interact and the effect of organizational size on social learning is only prominent for certain industries. These ideas could be examined in future research.

Finally, we did not examine distinct differences between the US and India samples, namely culture and government regulations. Thus, we are unable to say for certain why the two samples differed on some of the variables. This study was primarily exploratory in nature. Although we did not include explanatory variables, we have provided possible explanations for the differences. Future research should determine whether these assertions are supported by data.

## **CHAPTER X**

### **CONCLUSION**

Information security continues to be a primary concerns for organizations.

Employees can be a great asset to information security in organizations or a threat to information security. We have shown how the social environment influences security perceptions and intentions. Social learning research may benefit more from the study of Akers' social learning theory than from Bandura's social learning theory or protection motivation theory. This study findings that self-efficacy and response efficacy, which are commonly placed as mediators in other models are inconsistent. Social learning may provide a better explanation of behavior than self-efficacy and response efficacy.

Researchers should continue to study the effects of the social learning environment on information security behaviors. A greater emphasis should be placed on learning how managers can influenced the social learning environment to improve information security behavior. Researchers must also continue to study other types of understudied security controls, such as outcome-oriented controls and intrinsically oriented controls. Research into these controls may provide new avenues of control for practitioners. Researchers should also carefully consider how organizational context influences information security controls. This study finds that international differences in culture, regulations, and IT infrastructure may create differences in security beliefs and behavioral intentions.

## REFERENCES

- Agnew, R. (1991). A longitudinal test of social control theory and delinquency. *Journal of Research in Crime and Delinquency*, 28(2), 126-156.
- Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckman (Eds.), *Action control: From cognition to behavior*. Heidelberg: Springer.
- Akers, R. L. (1985). *Deviant behavior: A social learning approach*. Belmont, CA: Wadsworth.
- Akers, R. L. (1990). Rational choice, deterrence, and social learning theory in criminology: The path not taken. *Journal of Criminal Law and Criminology*, 81(3), 653-676.
- Akers, R. L. (1996). Is differential association/social learning cultural deviance theory? *Criminology*, 34(2), 229-247.
- Akers, R. L. (1998). *Social learning and social structure: A general theory of crime and deviance*. Boston, MA: Northeastern University Press.
- Akers, R. L. (2009). *Social learning and social structure: A general theory of crime and deviance*. New Brunswick, NJ: Transaction Publishers.
- Akers, R. L., & Lee, G. (1996). A longitudinal test of social learning theory: Adolescent smoking. *Journal of Drug Issues*, 26(2), 317-343.
- Bandura, A. (1977a). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, 84(2), 191-215.
- Bandura, A. (1977b). *Social learning theory*. Englewood Cliffs, NJ: Prentice Hall.
- Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Englewood Cliffs, NJ: Prentice Hall.
- Barker, J. R. (1993). Tightening the iron cage: Concertive control in self-managing teams. *Administrative Science Quarterly*, 38(3), 408-437.

- Barki, H., Rivard, S., & Talbot, J. (2001). An integrative contingency model of software project risk management. *Journal of Management Information Systems*, 17(4), 37-69.
- Baron, R. M., & Kenny, D. A. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, 51(6), 1173-1182.
- Becker, J.-M., Klein, K., & Wetzels, M. (2012). Hierarchical latent variable models in PLS-SEM: guidelines for using reflective-formative type models. *Long Range Planning*, 45(5), 359-394.
- Bénabou, R., & Tirole, J. (2003). Intrinsic and extrinsic motivation. *The Review of Economic Studies*, 70(3), 489-520.
- Blumstein, A. (1978). Introduction. In A. Blumstein, J. Cohen & D. Nagin (Eds.), *Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates*. Washington D.C.: National Academy of Sciences.
- Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, W. R. (2009). If someone is watching, I'll do what I'm asked: manditoriness, control, and information security. *European Journal of Information Systems*, 18, 151-164.
- Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk: A new source of enexpensive, yet high-quality, data? *Perspectives on Psychological Science*, 6(1), 3-5.
- 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.
- Cardinal, L. B. (2001). Technological innovation in the pharmaceutical industry: The use of organizational control in managing research and development. *Organization Science*, 12, 19-36.
- Chen, Y. R., K R, & Wen, K.-W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, 29(3), 157-188.
- Chin, W. W. (1998). The Partial Least Squares Approach to Structural Equation Modeling. In G. A. Marcoulides (Ed.), *Modern Business Research Methods* (pp. 295-336). Mahwah, NJ: Lawrence Erlbaum Associates.

- Chin, W. W. (2010). How to write up and report PLS analyses. In V. Esposito Vinzi, W. W. Chin, J. Henseler & H. Wang (Eds.), *Handbook of partial least squares: Concepts, methods and applications* (pp. 655-690): Springer.
- Chin, W. W., Marcolin, B. L., & Newsted, P. N. (2003). A partial least squares approach for measuring interaction effects: results from a Monte Carlo simulation study and an electronic mail emotion/adoption study. *Information Systems Research, 14*(2), 189-217.
- Clark, J. G., Au, Y. A., Walz, D. B., & Warren, J. (2011). Assessing researcher publication productivity in the leading information systems journals: A 2005-2009 update. *Journal of the Association for Information Systems, 29*, 459-504.
- Corbin, J., & Strauss, A. (1990). Grounded theory method: Procedures, canons, and evaluative criteria. *Qualitative Sociology, 13*(1), 3-21.
- Creswell, J. W. (2007). *Qualitative inquiry and research design: Choosing among five approaches*. Thousand Oaks, CA: Sage.
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101.
- D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences, 43*(6), 1091-1124.
- D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems, 20*, 643-658.
- D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems, 31*(2), 285-318.
- D'Arcy, J., & Hovav, A. (2007a). Deterring internal information systems misuse. *Communications of the ACM, 50*(10), 113-117.
- D'Arcy, J., & Hovav, A. (2007b). Towards a best fit between organizational security countermeasures and information systems misuse behaviors. *Journal of Information System Security, 3*(2), 3-31.
- D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research, 20*(1), 79-98.

- Deci, E. L., Koestner, R., & Ryan, R. M. (1999). A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation. *Psychological Bulletin*, *125*(6), 627-668.
- Diamantopoulos, A., & Sigauw, J. A. (2006). Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. *British Journal of Management*, *17*, 263-282.
- Diamantopoulos, A., & Winklhofer, H. M. (2001). Index construction with formative indicators: An alternative to scale development. *Journal of Marketing Research*, *38*.
- Doty, D. H., & Glick, W. H. (1994). Typologies as a unique form of theory building: Toward improved understanding and modeling. *Academy of Management Review*, *19*(2), 230-251.
- Eisenberger, R., Pierce, W. D., & Cameron, J. (1999). Effects of reward on intrinsic motivation—negative, neutral, and positive: Comment on Deci, Koestner, and Ryan (1999). *Psychological Bulletin*, *125*(6), 677-691.
- Fairclough, N., Mulderrig, J., & Wodak, R. (1997). Critical discourse analysis. In T. A. van Dijk (Ed.), *Discourse Studies: A Multidisciplinary Introduction* (pp. 357-378). London: SAGE Publications.
- Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equations models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39-50.
- Frey, B. S. (1997). *Not just for the money: An economic theory of personal motivation*. Brookfield, VT: Edward Elgar.
- Gagne, M., & Deci, E. L. (2005). Self-determination theory and work motivation. *Journal of Organizational Behavior*, *26*(4), 331-362.
- Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the AIS*, *16*(1), 91-109.
- Ghoshal, S., Korine, H., & Szulanski, G. (1994). Interunit communication in multinational corporations. *Management Science*, *40*(1), 96-110.
- Glasser, B. G. (1978). *Theoretical sensitivity: Advances in the methodology of grounded theory*. Mills Valley, CA: The Sociology Press.

- Glasser, B. G. (1992). *Emerging vs. forcing: Basics of grounded theory analysis*. Mills Valley, CA: The Sociology Press.
- Gosain, S. (2004). Enterprise information systems as objects and carriers of institutional forces: The new iron cage? *Journal of the Association for Information Systems*, 5(4), 151-182.
- Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, 32, 242-251.
- Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, 28(2), 203–236.
- Harney, A. (2011). China's copycat culture. *Latitude*.  
<http://latitude.blogs.nytimes.com/2011/10/31/chinas-copycat-culture/>
- Harrington, S. J. (1996). The effect codes of ethics and personal denial of responsibility on computer abuse judgements and intentions. *MIS Quarterly*, 20(3), 257-278.
- Harris, E. A., Perlroth, N., Popper, N., & Stout, H. (2014). A sneaky path into Target customers' wallets. *The New York Times*.  
<http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html>
- Herath, T., & Rao, H. R. (2009a). 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. (2009b). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18, 106-125.
- Hirschi, T. (1969). *Causes of Delinquency*. Berkeley, CA: University of California Press.
- Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the mind* (3rd ed.). New York, NY: McGraw-Hill.
- Hollenbeck, J. R., Beersma, B., & Schouten, M. E. (2012). Beyond team types and taxonomies: A dimensional scaling conceptualization for team description. *Academy of Management Review*, 37(1), 82-106.
- Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management*, 49(2), 99–110.

- Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policy: The critical role of top management and organizational culture. *Decision Sciences*, 43(4), 615-659.
- 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.
- Hwang, S., & Akers, R. L. (2003). Substance use by Korean adolescents: A cross-cultural test of social learning, social bonding, and self-control theories. In G. F. Jensen & R. L. Akers (Eds.), *Advances in criminological theory: Social learning theories and the explanation of crime* (Vol. 11, pp. 39-64). Brunswick, NJ: Transaction Publishers.
- Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research*, 30(2), 199-218.
- Jensen, G. F., & Akers, R. L. (2003). Taking social learning global: Micro-macro transitions. In G. F. Jensen & R. L. Akers (Eds.), *Advances in criminological theory: Social learning theory and the explanation of crime* (Vol. 11, pp. 9-38). New Brunswick, NJ: Transaction Publishers.
- Johnson, P., & Gill, J. (1993). *Management control and organizational behaviour*. London: Paul Chapman.
- 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. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, 39(1), 113-134.
- Krohn, M. D. (1999). Social learning theory: The continuing development of a perspective. *Theoretical Criminology*, 3(4), 462-476.
- Krohn, M. D., Lizotte, A. J., Thornberry, T. P., Smith, C., & McDowall, D. (1996). Reciprocal causal relationships among drug use, peers, and beliefs: A five-wave panel model. *Journal of Drug Issues*, 26(2), 405-428.
- Krohn, M. D., Skinner, W. F., Massey, J. L., & Akers, R. L. (1985). Social learning theory and adolescent cigarette smoking: A longitudinal study. *Social Problems*, 32(5), 455-473.

- Lange, D. (2008). A multidimensional conceptualization of organizational corruption control. *Academy of Management Review*, 33(3), 710-729.
- Lee, S. M., Lee, S.-G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, 41(6), 707-718.
- Lehman, D. W., & Ramanujam, R. (2009). Selectivity in organizational rule violations. *Academy of Management Review*, 34(4), 643-657.
- Leidner, D., & Kayworth, T. (2006). A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS Quarterly*, 30(2), 357-399.
- Leonard, L. N. K., Cronan, T. P., & Kreie, J. (2004). What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics? *Information & Management*, 42(1), 143-158.
- Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, 48(4), 635–645.
- Lincoln, Y. S., Lynham, S. A., & Guba, E. G. (2011). Paradigmatic controversies, contradictions, and emerging confluences, revisited. In N. K. Denzin & Y. S. Lincoln (Eds.), *The SAGE handbook of qualitative research* (pp. 97-128). Thousand Oaks, CA: SAGE Publications.
- Lowry, P. B., Moody, G., Galletta, D., & Vance, A. (2012). The drivers in the use of online whistle-blowing reporting systems. *Journal of Management Information Systems*.
- MacKinnon, D., Lockwood, C., & Hoffman, J. (2002). A comparison of methods to test mediation and other intervening variable effects. *Psychological Methods*, 7(1), 83-104.
- March, J. G., & Simon, H. A. (1958). *Organizations*. New York, New York: Wiley.
- Mason, W., & Suri, S. (2012). Conducting behavioral research on Amazon's Mechanical Turk. *Behavioral Research Methods*, 44(1), 1-23.
- Merton, R. K. (1938). Social structure and anomie. *American Sociological Review*, 3, 672-682.
- Mintzberg, H. T. (1979). *The structuring of organizations*. Englewood Cliffs, NJ: Prentice Hall.

- Mintzberg, H. T. (1983). *Structure in fives: Designing effective organizations*. Englewood Cliffs, NJ: Prentice Hall.
- Morris, R. G., & Higgins, G. E. (2010). Criminological theory in the digital age: The case of social learning theory and digital piracy. *Journal of Criminal Justice*, 38(4), 470-480.
- 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.
- Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46(4), 815-825.
- NIST. (2009). Recommended security controls for federal information systems and organizations. Gaithersburg, MD: National Institute of Standards and Technology.
- Ortega, E., Giannotta, F., & Ciairano, S. (2013). Cross national comparison of the effects of parental strictness of rules on adolescents' well-being in Italy and the Netherlands. *European Journal of Child Development*, 1, 157-172.
- Palvia, P. C., Palvia, S. C. J., & Whitworth, J. E. (2002). Global information technology: A meta analysis of key issues. *Information & Management*, 39(5), 403-414.
- Paolacci, G., Chandler, J., & Ipeirotis, P. G. (2010). Running experiments on Amazon Mechanical Turk. *Judgment and Decision Making*, 5(5), 411-419.
- Peace, A. G., Galletta, D., & Thong, J. Y. L. (2003). Software privacy in the workplace: A model and empirical test. *Journal of Management Information Systems*, 20(1), 153-177.
- Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly*, 31(4), 623-656.
- Ponemon, I. (2013). 2013 cost of data breach study: Global analysis. Traverse City, MI: Ponemon Institute.
- Posey, C., Bennett, R. J., & Roberts, T. L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security*, 30(6), 486-497.
- Posey, C., Bennett, R. J., Roberts, T. L., & Lowry, P. B. (2011). When computer monitoring backfires: Privacy invasions and organizational injustice as precursors to computer abuse. *Journal of Information Systems Security*, 7(1), 24-47.

- Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly*.
- Pratt, T. C., Cullen, F. T., Blevins, K. R., Daigle, L. E., & Madensen, T. D. (2006). The empirical status of deterrence theory: A meta-analysis. In F. T. Cullen, J. P. Wright & K. R. Blevins (Eds.), *Taking stock: The status of criminological theory* (pp. 37-76). New Brunswick, NJ: Transaction Publishers.
- Pratt, T. C., Cullen, F. T., Sellers, C. S., Winfree, T., Jr, Madensen, T. D., Daigle, L. E., . . . Gau, J. M. (2010). The empirical status of social learning theory: A meta-analysis. *Justice Quarterly*, 27(6), 765-802.
- Presser, L. (2008). *Been a heavy life: Stories of violent men*. Chicago, IL: University of Illinois Chicago.
- Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, 34(4), 757-778.
- Ringle, C. M., Wende, S., & Will, A. (2005). *SmartPLS*. Hamburg, Germany: SmartPLS.
- Rogers, M. K. (2001). *A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study*. (Doctor of Philosophy), University of Manitoba, Winnipeg, Manitoba.
- Ruiz-Palomino, P., & Martinez-Cañas, R. (2011). Supervisor role modeling, ethics-related organizational policies, and employee ethical intention: The moderating impact of moral ideology. *Journal of Business Ethics*, 102(4), 653-668.
- Ryan, R. M., & Deci, E. L. (1985). *Intrinsic motivation and self-determination in human behavior*. New York, NY: Plenum Press.
- Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist*, 55(1), 68-78.
- Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), 487-502.
- Siponen, M., Willison, R., & Baskerville, R. (2008). *Power and practice in information systems security research*. Paper presented at the 29th International Conference on Information Systems, Paris, France.

- Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency*, 34(4), 495-518.
- Sobel, M. E. (1982). Asymptotic confidence intervals for indirect effects in structural equation models. *Sociological Methodology*, 13, 290-312.
- Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, 48, 296-302.
- Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, 34(3), 503-522.
- Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). Information security policies in the UK healthcare sector: A critical evaluation. *Information Systems Journal*, 22(1), 77-94.
- Stogner, J. M., Miller, B. L., & Marcum, C. D. (2013). Learning to e-cheat: A criminological test of Internet facilitated academic cheating. *Journal of Criminal Justice*, 24(2), 175-199.
- Straub, D., & Welke, R. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 22(4), 441-469.
- Straub, D. W., Jr. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255-276.
- Straub, D. W. J., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, 14(1), 45-60.
- Sutherland, E. H. (1947). *Principles of Criminology* (4th ed.). Philadelphia, PA: J. B. Lippincott.
- Sykes, G., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, 22(6), 664-670.
- Tompkins, P. K., & Cheney, G. (1985). Communication and unobtrusive control in contemporary organizations. In R. D. McPhee & P. K. Tompkins (Eds.), *Organizational communication: Traditional themes and new directions* (pp. 179-210). Newbury Park, CA: Sage.
- Van Alstyne, M. W. (1997). The state of network organization: A survey in three frameworks. *Journal of Organizational Computing*, 7(3), 83-151.

- Vance, A., & Siponen, M. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing*, 24(1), 21-41.
- Vance, A., Siponen, M., & Pahlila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, 49, 190-198.
- Venkatraman, N. (1989). The concept of fit in strategy research: Toward verbal and statistical correspondence. *Academy of Management Review*, 14(3), 423-444.
- Vroom, V. H. (1964). *Work and Motivation*. Oxford, UK: Wiley.
- Wang, S.-N., & Jensen, G. F. (2003). Explaining delinquency in Taiwan: A test of social learning theory. In R. L. Akers & G. F. Jensen (Eds.), *Advances in criminological theory: Social learning theories and the explanation of crime* (Vol. 11). Brunswick, NJ: Transaction Publishers.
- Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, 20, 267-284.
- Warkentin, M., Straub, D., & Malimage, K. (2012). *Measuring secure behavior: A research commentary*. Paper presented at the Annual Symposium on Information Assurance, Albany, NY.
- Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, 18, 101-105.
- Warren, D. E. (2003). Constructive and destructive deviance in organizations. *Academy of Management Review*, 28(4), 622-632.
- Wetzels, M., Odekerken-Schöder, G., & Oppen, C. V. (2009). Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS Quarterly*, 33(1), 177-195.
- Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 37(1), 1-20.
- Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24, 2799-2816.

- Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: a study of insider security contravention. *Journal of the American Society for Information Science and Technology*, 58(2), 212-222.
- Wright, B. M., & Barker, J. R. (2000). Assessing concertive control in the term environment. *Journal of Occupational & Organizational Psychology*, 73(3), 345-361.
- Xue, Y., Liang, H., & Wu, L. (2011). Punishment, justice, and compliance in mandatory IT settings. *Information Systems Research*, 22(2), 400-414.
- Yin, R. K. (2002). *Case Study Research: Design and Methods* (3rd ed.): SAGE Publications.
- Zafar, H., & Clark, J. G. (2009). Current state of information security research in IS. *Communication of the Association for Information Systems*, 24(1), 557-596.
- Zey-Ferrell, M., & Ferrell, O. C. (1982). Role-set configuration and opportunity as predictors of unethical behavior in organizations. *Human Relations*, 35(7), 587-604.

**APPENDIX A**

**CODING OF INFOSEC RESEARCH**

<b>Table A1. Information Security Studies by Control Type</b>													
<b>Study</b>	<b>Is a moderation-based contingency model?</b>	<b>Type 1 - PBC</b>	<b>Type 2 - OBC</b>	<b>Type 3 – PCON</b>	<b>Type 4 – OCON</b>	<b>Type 5 - PCS</b>	<b>Type 6 - OCS</b>	<b>Type 7 – PSCS</b>	<b>Type 8 - OSCS</b>	<b>Type 9 – PCC</b>	<b>Type 10 - OCC</b>	<b>Type 11 – PSCC</b>	<b>Type 12 - OSCC</b>
(Boss et al., 2009)*		X	X			X	X						
(Bulgurcu et al., 2010)*		X		X		X							
(Chen & Wen, 2012)*	X	X				X							
(D'Arcy & Devaraj, 2012)		X				X		X					
(D'Arcy & Hovav, 2007a)		X								X			
(D'Arcy & Hovav, 2007b)		X				X				X			
(D'Arcy et al., 2009)		X	X			X				X			
(Guo et al., 2011)**		X		X		X				X			

(Harrington, 1996)	X	X				X				X			
(Herath & Rao, 2009a)*		X	X	X		X				X			
(Herath & Rao, 2009b)*		X	X	X		X				X	X		
(Hovav & D'Arcy, 2012)	X	X				X				X			
(Hu, Xu, Dinev, & Ling, 2011)		X				X							
(Hu et al., 2012)		X	X										X
(Johnston & Warkentin, 2010)*		X	X	X			X						
(Lee et al., 2004)		X		X		X				X			
(Leonard et al., 2004)	X	X	X	X	X	X							
(Li et al., 2010)*	X	X		X		X		X		X		X	
(Lowry et al., 2012)		X	X								X	X	X
(Myry et al., 2009)*		X								X	X	X	
(Ng et al., 2009)*	X	X				X				X	X		
(Peace, Galletta,		X		X		X							

& Thong, 2003)													
(Posey, Bennett, & Roberts, 2011)	X	X		X						X			
(Posey, Bennett, Roberts, et al., 2011)		X				X							
(Puhakainen & Siponen, 2010)*		X		X						X	X		
(Siponen & Vance, 2010)*		X				X		X					
(Son, 2011)*		X				X				X	X		
(Spears & Barki, 2010)*		X	X							X	X		
(D. W. Straub, Jr, 1990)		X				X				X			
(D. W. J. Straub & Nance, 1990)	X	X				X							
(Vance & Siponen, 2012)		X				X		X					
(Vance et al., 2012)*		X	X				X			X	X		
(Warkentin et al., 2011)*		X	X	X								X	

(Workman et al., 2008)		X	X				X				X		
(Xue et al., 2011)*		X	X			X				X	X		

\*Study primarily examines compliance and not forms of noncompliance

\*\*Study primarily examines nonmalicious and not malicious forms of noncompliance

## APPENDIX B

### INTERVIEW QUESTIONS

Interview Question
What has influenced your beliefs and behaviors regarding information security behaviors?
When you were a child and adolescent, how did your family react to laws/social norms/authority?
When you were an adolescent, how did your closest friends react to laws/social norms/authority?
Where did you work prior to working at your current organization? What was your position? What did you organization do?
In your prior organization, who was most important to you? Is there anyone who was a model to you?
Why are these people so important to you?
How did those people feel about computer security/computer security policies?
How did your organization respond to people who violated computer security policies? How did the important people in your prior organization respond to people who violated computer security policies? What rewards and punishments existed in your organization related to computer security?
In your current organization, who is most important to you? Is there anyone who is a model to you?
Why are these people so important to you?
How did those people feel about computer security/computer security policies?
How does your organization respond to people who violate computer security policies? How do the people who are important to you in your current organization respond to people who violate computer security policies? What rewards and punishments exist in your organization related to computer security?
How do you feel about computer security/computer security policies?
Knowing that the purpose of this study is to understand how your information security beliefs and behaviors developed, is there anything else we haven't discussed that has influenced your security beliefs and behaviors?

## **APPENDIX C**

### **SURVEY QUESTIONNAIRE**

The survey consisted of the primary survey questions presented in Table C1. The survey also contained two filtering questions asking how many organizations the person had worked for and how often the user used computers for work. If the respondent had not worked for at least two organizations, they were dropped from the responses. If the respondent did not use computers multiple times per week, the responses were dropped. Respondents were also asked questions to determine if they were paying careful attention to the questions (i.e., please answer “Strongly Agree” for this question). Three of these questions were included in the survey. If the respondent failed any of these questions, the responses were dropped. Demographic information was also collected, including: age, gender, education, income, job tenure, work experience, job position, and organizational size.

Unless otherwise stated, all questions were answered on a 7-point Likert scale from “Strongly Disagree” to “Strongly Agree.”

The survey contained vignettes to assess SRBI and SDBI. Direct questioning of negative behavior can be influenced by desirability bias. Thus, we included a scenario where a character committed an SRB or SDB. Afterward, the respondent was asked to assess whether their own behaviors would be similar to the characters in the same situation. Four vignettes were created, two vignettes with SRBs and two vignettes with

SDBs. Each respondent was randomly assigned one SRB vignette and one SDB vignette.

The SRB vignettes were:

- 1) Taylor is preparing to leave on vacation. Taylor's coworker Alex has been asked to complete Taylor's work while Taylor is away. Company policies state that employees should not share their passwords. However, Taylor shares his password with Alex so that Alex can access important files while Taylor is on vacation.
- 2) Taylor is working on a project for an important client. While Taylor is at lunch at a restaurant, the client calls Taylor and asks Taylor to send them information about the project as quickly as possible. Company policies state that employees should not access the company's computer systems from an unsecured network. However, Taylor connects to the restaurant's unsecured network and accesses the company's computer system to find the information for the client.

The SDB vignettes were:

- 1) Taylor has computerized access to important client lists at work. The client lists are worth a lot of money and Taylor knows someone at a previous organization who might be interested in secretly purchasing the lists. Every day, Taylor writes down information about the clients he helps so that he can later sell the information. After collecting enough information, Taylor sells the client lists.
- 2) Taylor has been treated poorly by his organization. Taylor is planning to quit, but before leaving Taylor wants to get even with the organization for the mistreatment. Taylor has a friend who knows about computer hacking. Taylor asks the friend about some viruses that could harm an organization's computer systems. After learning about a particular virus, Taylor downloads the virus onto a USB device and plugs the USB device into several computers at work to infect the computer systems.

**Table C1. Survey Questions**

Construct	Question	Source	Type of Measurement
Proactive security behavior intentions (PINT)	I do more than is required by my organization's information security policies to protect my computer system at work.	Adapted from (Boss et al., 2009)	First-order reflective
	I keep aware of the latest security threats so I can better protect my computer system.		
	I take extra precautions beyond those required by my organization to protect computerized information at work.		
Policy compliance intentions (CINT)	I intend to comply with the requirements of the ISP of my organization in the future.	Adapted from (Bulgurcu et al., 2010)	First-order reflective
	I intend to use information and technology resources according to the requirements of the ISP of my organization in the future.		
	I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information and technology in the future.		
Security risk-taking behavior intentions	If you were Taylor, what is the likelihood	Adapted from (D'Arcy et al., 2009)	First-order reflective

(SRBI) and Security damaging behavior intentions (SDBI)	that you would [action performed in scenario]?  <i>(scale from: very unlikely to very likely)</i> If I were Taylor, I could see myself [action performed in the scenario]. If I were Taylor, I would [action performed in the scenario].		
<b>Social Learning (adolescence and childhood) (SLEA)</b>			
General rule-related definitions in favor of compliance (DFCA)	Following rules is important. Rules are in place for a good reason. Complying with rules is good.	Developed from qualitative data based on (Ronald L. Akers, 2009; R L Akers & Lee, 1996)	Second-order reflective
Differential association (parents) (DAPA)	Growing up, my parent(s)/legal guardian(s) believed that I should:  <i>(scale from: always disobey rules to always follow rules)</i> Growing up, my parent(s)/legal guardian(s) believed that following rules is:  <i>(scale from: always unimportant to always important)</i>	Developed from qualitative data based on (Ronald L. Akers, 2009; R L Akers & Lee, 1996)	Third-order reflective- formative
Differential association (friends) (DAFA)	Growing up, my close friends believed that I should:	Developed from qualitative data based on (Ronald L.	Third-order reflective- formative

	<p><i>(scale from: always disobey rules to always follow rules)</i></p> <p>Growing up, my close friends believed that following rules is:</p> <p><i>(scale from: always useless to always useful)</i></p>	Akers, 2009; R L Akers & Lee, 1996)	
Differential reinforcement (DREA)	<p>Growing up, I was often:</p> <p><i>(scale from: punished for breaking rules to rewarded for breaking rules)</i></p> <p>Reverse coded</p> <p>Growing up, I was often:</p> <p><i>(scale from: punished for following rules to rewarded for following rules)</i></p> <p>Growing up, I was often:</p> <p><i>(scale from: shamed for breaking rules to praised for breaking rules)</i></p> <p>Reverse coded</p> <p>Growing up, I was often:</p> <p><i>(scale from: shamed for following rules to</i></p>	Developed from qualitative data based on formal and informal sanctions/rewards (Johnston et al., 2015)	First-order formative

	<i>praised for following rules)</i>		
Imitation (parents) (IMPA)	Growing up, my parent(s)/legal guardian(s):  <i>(scale from: always violated rules to always followed rules)</i>	Developed from qualitative data based on (Ronald L. Akers, 2009; R L Akers & Lee, 1996)	Third-order reflective-formative
	Growing up, my parent(s)/legal guardian(s):  <i>(scale from: always disobeyed the law to always followed the law)</i>		
	Growing up, my parent(s)/legal guardian(s):  <i>(scale from: defied those in authority to followed those in authority)</i>		
Imitation (friends) (IMFA)	Growing up, my close friends:  <i>(scale from: always violated rules to always followed rules)</i>	Developed from qualitative data based on (Ronald L. Akers, 2009; R L Akers & Lee, 1996)	Third-order reflective-formative
	Growing up, my close friends:  <i>(scale from: always disobeyed the law to always followed the law)</i>		
	Growing up, my close friends:		

	(scale from: were always in trouble to were never in trouble )		
<b>Social Learning (previous organization) (SLPO)</b>			
Security-specific definitions in favor of compliance (DFCP)	At my previous job, following information security policies was important.	Same as previous definitions construct	Second-order reflective
	At my previous job, information security policies were in place for a good reason.		
	At my previous job, complying with information security policies was essential.		
Differential association (manager) (DAMP)	At my previous job, my boss believed that I should:  (scale from: always disobey ISP to always follow ISP)	Same as previous differential association construct	Third-order reflective-formative
	At my previous job, my boss believed that following ISP is:  (scale from: always useless to always useful)		
Differential association (coworker) (DACP)	At my previous job, most of my coworkers believed that I should:  (scale from: always disobey ISP to always follow ISP)	Same as previous differential association construct	Third-order reflective-formative
	At my previous job, most of my coworkers believed that following ISP is:		

	<i>(scale from: always unimportant to always important)</i>		
Differential reinforcement (DREP)	At my previous job, I was often:  <i>(scale from: punished for breaking ISP to rewarded for breaking ISP)</i>  Reverse coded	Same as previous differential reinforcement construct	First-order formative
	At my previous job, I was often:  <i>(scale from: punished for following ISP to rewarded for following ISP)</i>		
	At my previous job, I was often:  <i>(scale from: shamed for violating ISP to praised for violating ISP)</i>  Reverse coded		
	At my previous job, I was often:  <i>(scale from: shamed for following ISP to praised for following ISP)</i>		
Imitation (manager) (IMMP)	At my previous job, my boss:	Same as previous imitation construct	Third-order reflective-formative

	<p><i>(scale from: always violated ISP to always followed ISP)</i></p> <p>At my previous job, my boss:</p> <p><i>(scale from: never kept his/her computer safe to always kept his/her computer safe)</i></p> <p>At my previous job, my boss:</p> <p><i>(scale from: never protected organizational information to always protected organizational information)</i></p>		
Imitation (coworkers) (IMCP)	<p>At my previous job, most of my coworkers:</p> <p><i>(scale from: always violated ISP to always followed ISP)</i></p> <p>At my previous job, most of my coworkers:</p> <p><i>(scale from: never kept his/her computer safe to always kept his/her computer safe)</i></p> <p>At my previous job, most of my coworkers:</p> <p><i>(scale from: never protected organizational information to always protected)</i></p>	Same as previous imitation construct	Third-order reflective-formative

	<i>organizational information)</i>		
<b>Social Learning (previous organization) (SLCO)</b>			
Security-specific definitions in favor of compliance (DFCC)	At my current job, following information security policies is important.	Same as previous definition construct	Second-order reflective
	At my current job, information security policies are in place for a good reason.		
	At my current job, complying with information security policies is essential.		
Differential association (manager) (DAMC)	At my current job, my boss believes that I should:  <i>(scale from: always disobey ISP to always follow ISP)</i>	Same as previous differential association construct	Third-order reflective-formative
	At my current job, my boss believes that following ISP is:  <i>(scale from: always unimportant to always important)</i>		
Differential association (coworker) (DACC)	At my current job, most of my coworkers believe that I should:  <i>(scale from: always disobey ISP to always follow ISP)</i>	Same as previous differential association construct	Third-order reflective-formative
	At my current job, most of my coworkers believe that following ISP is:		

	<i>(scale from: always useless to always useful)</i>		
Differential reinforcement (DREC)	At my current job, I am often:  <i>(scale from: punished for breaking ISP to rewarded for breaking ISP)</i>  Reverse coded	Same as previous differential reinforcement construct	First-order formative
	At my current job, I am often:  <i>(scale from: punished for following ISP to rewarded for following ISP)</i>		
	At my current job, I am often:  <i>(scale from: shamed for violating ISP to praised for violating ISP)</i>  Reverse coded		
	At my current job, I am often:  <i>(scale from: shamed for following ISP to praised for following ISP)</i>		
Imitation (manager) (IMMC)	At my current job, my boss:  <i>(scale from: always violates ISP to always follows ISP)</i>	Same as previous imitation construct	Third-order reflective-formative

	<p>At my current job, my boss:</p> <p><i>(scale from: never keeps his/her computer safe to always keeps his/her computer safe)</i></p>		
	<p>At my current job, my boss:</p> <p><i>(scale from: never protects organizational information to always protects organizational information)</i></p>		
Imitation (coworkers) (IMCC)	<p>At my current job, my coworkers:</p> <p><i>(scale from: always violates ISP to always follows ISP)</i></p>	Same as previous imitation construct	Third-order reflective-formative
	<p>At my current job, my coworkers:</p> <p><i>(scale from: never keeps his/her computer safe to always keeps his/her computer safe)</i></p>		
	<p>At my current job, my coworkers:</p> <p><i>(scale from: never protects organizational information to always protects organizational information)</i></p>		
Learning fit (LFIT)	<p>At my current job, my organization believes that following information security policies is:</p>	Based on insight from qualitative data	First-order reflective

	<p><i>(scale from: much less important than I do to much more important than I do)</i></p> <p>At my current job, my organization believes that information security is:</p> <p><i>(scale from: much less important than I do to much more important than I do)</i></p> <p>At my current job, my organization believes that protecting organizational information is:</p> <p><i>(scale from: much less important than I do to much more important than I do)</i></p> <p>At my current job, my organization believes that information security policies are:</p> <p><i>(scale from: much less valuable than I do to much more valuable than I do)</i></p>		
Severity of sanctions (SEVR)	<p>If I were caught violating information security policies, I would be severely punished.</p> <p>I would be punished harshly if I were caught violating</p>	Adapted from (D'Arcy et al., 2009)	First-order reflective

	information security policies.		
	If I violated information security policy, the punishment would be:  <i>(scale from: not severe at all to very severe)</i>		
Certainty of sanctions (CERT)	If I violated information security policies, I would be caught eventually.	Adapted from (D'Arcy et al., 2009)	First-order reflective
	I would likely be caught if I violated information security policies.		
Formal training (TRAN)	My current organization trains me about information security issues.	Adapted from (D'Arcy et al., 2009)	First-order reflective
	My current organization educates me about my information security responsibilities.		
	My current organization provides me training about information security policies.		
Self-efficacy (SEFF)	I feel capable of following information security policies.	Adapted from (Johnston & Warkentin, 2010)	First-order reflective
	I am confident that I can follow information security policies.		
	I believe that I can successfully comply		

	with information security policies.		
Response efficacy (REFF)	Information security policies work for protection against security threats.	Adapted from (Johnston & Warkentin, 2010)	First-order reflective
	Information security policies are effective for protection against security threats.		
	When following information security policies, the organization is more likely to be protected.		