THREE ESSAYS ON INFORMATION SECURITY POLICY COMPLIANCE:

THE ROLE OF SOCIAL INFLUENCE

by

ADEL YAZDANMEHR

Presented to the Faculty of the Graduate School of

The University of Texas at Arlington in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT ARLINGTON

August 2017

ACKNOWLEDGEMENT

Writing this thesis was one the most difficult tasks I have undertaken. However, there are many who have played the larger role by their endless sacrifices and supports, which I would like to express my special thanks of gratitude to them.

To my mentor, Dr. Jingguo Wang

Your paramount guidance, support, and patience helped me to grow as a scholar and an independent thinker.

To my lovely wife, Tanin

You are my rock, your strength in indulging my bad moods, your unyielding support for past nine years, is a testament to your love.

To my Son, Daniel

Your smiles are the greatest motivational speech one can ever have.

To my parents, Reza and Shahla

You are the ones who I owed the most, thank you for letting your only son to live 7500 miles far from you knowing that you cannot visit him. I am where I am because of you. I love you so much.

To Tanin's parents, Saeed and Parvin

Your unwavering trust and unending support gave me the strength to overcome the challenges I faced. Your life story and graduate school experience are my inspiration.

To my Sister, Rana

You are my champion, having you with our parents gave me piece of mind.

To my dissertation committee members, Dr. Wendy Casper and Dr. Mary Whiteside

You are the best, not only your many valuable comments improved the quality of this dissertation immensely but also your moral support helped me get through many difficulties.

To my friend, Dr. Zhiyong Zhang,

Your friendship is much appreciated. Your insightful discussions always led me to many fascinating research ideas.

June 07, 2017

ABSTRACT

THREE ESSAYS ON INFORMATION SECURITY POLICY COMPLIANCE:

THE ROLE OF SOCIAL INFLUENCE

Adel Yazdanmehr, PhD

The University of Texas at Arlington, 2017

Supervising Professor: Jingguo Wang

Motivating employees to comply with information security policies (ISP) is a major challenge for organizations. Employees who do not comply with these policies can impose a serious threat to the safety of organizational information assets. Information security scholars drawing upon several theories have investigated various factors that can help motivate employees to comply with the ISP. Among many factors, social influence proved to be an effective force in motivating employee compliance behavior. However, its role and various effects on employee ISP compliance as well as its utilization mechanisms have not been deeply investigated.

This dissertation is a collection of three papers addressing a series of related questions including (1) through which psychological processes social influence may be internalized and then affect employee compliance; (2) how social influence, at both organizational micro and macro level, alter the effectiveness of well-established motivational rule-following models; and finally (3) how we can utilize social influence to successfully motivate employees to comply. Accordingly, the first essay focuses on how personal norms regarding ISP affect employee compliance. In particular, it examines how such norms are shaped and activated to motivate employee compliance. In addition, the second essay introduces a social contingency model proposing that the well-established rule-following approaches of command-and-control and self-

regulatory are contingent upon organizational rules ethical climate as well as employee susceptibility to interpersonal influence. Finally, the third essay discusses the role of collective responsibility and peer monitoring in motivating ISP compliance.

Table of Contents

INTRODUCTION

Motivating employees to comply with information security policies (ISP) is a major challenge for organizations. Employees who do not comply with these policies can impose a serious threat to the safety of the organizational information assets (Willison and Warkentin 2013). This is because these employees often have authority to access to the organizational sensitive information. In the same vein, information security managers have expressed such a concern in various instances (Poll 2015; PwC 2015; Verizon 2016). Accordingly, many information security scholars (D'Arcy and Herath 2011; Herath and Rao 2009a, 2009b; Posey and Roberts 2013; Siponen and Vance 2010; Wang et al. 2015) drawing upon several theories (e.g., general deterrence or protection motivation theory) have investigated various factors that can motivate employees to comply with the ISP. However, despite the recent improvements in this field, our understanding of this phenomenon is still limited (Guo et al. 2011).

The objective of this dissertation is to investigate the role of social influence in motivating employee compliance behavior. Social influence has been manifested as social pressure, subjective norms, or normative beliefs in previous literature (Bulgurcu et al. 2010; Herath and Rao 2009a; Siponen et al. 2010). However, to the best of my knowledge, its role and various effects on employee compliance as well as its utilization mechanisms have not been deeply investigated.

This dissertation poses a series of questions including (1) through which psychological processes social influence may be internalized and then affect employee compliance; (2) how social influence, at both organizational micro and macro level, alter the effectiveness of well-established motivational rule-following models; and finally (3) how we can utilize social influence to effectively motivate employees to comply with ISP. Through three essay we answer the foregoing questions.

In the first essay, we explore the role of norms in employee compliance with an organizational ISP. Drawing upon norm activation theory (Schwartz 1977), social norms theory (Cialdini and Trost 1998), and ethical climate literature (Victor et al. 1988), we introduce a model to examine how ISP-related personal norms are developed and then activated to affect employee ISP compliance. In particular, we propose that ISP-related personal norms lead to ISP compliance, and the effect is strengthened by ISP-related ascription of personal responsibility and awareness of consequences. Social norms related to ISP (including injunctive, descriptive and subjective norms); awareness of consequences, and ascription of personal responsibility shape personal norms; and finally, social norms related to ISP are the product of principle ethical climate in an organization. We test our research model using data collected through Amazon Mechanical Turk. Our results showed that ISP-related personal norms lead to ISP compliance. Ascription of personal responsibility toward ISP positively moderated the relationship. ISP-related social norms, such as injunctive and subjective norms, which were the product of a principle ethical climate, shaped ISP-related personal norms.

In the second essay, we introduce a social contingency model to examine how the interaction of the micro and macro aspects of social influence with the command-and-control and self-regulatory approaches affect ISP compliance. Previous studies have primarily focused on the command-and-control (the perception of detection and reaction to behavior) and self-regulatory (perceived legitimacy of the rules and value convergence with the rules) approaches to investigate ISP compliance (Bulgurcu et al. 2010; D’Arcy and Herath 2011; Guo et al. 2011; Herath and Rao 2009a, 2009b; Hu et al. 2011; H. Li et al. 2010; Liang et al. 2013; Myyry et al. 2009; Siponen and

Vance 2010; Son 2011; Tyler and Blader 2005). Information security literature considers social influence as opinions of important others (Dugo and Marshall 2007; Guo et al. 2011; Herath and Rao 2009a; Ifinedo 2012) and normative beliefs (Bulgurcu et al. 2010; Herath and Rao 2009b; Pahnila et al. 2007; Siponen et al. 2010). A novel perspective in this essay is the enrichment of the social influence concept by including both rules ethical climate and individual susceptibility to interpersonal influence. This allows us to investigate the moderating effect of these two at both the macro level (i.e., employees' perception of the rules adherence environment, as represented by rules ethical climate) and micro level (i.e., employees' seeking and observing common practices via interaction with their peers, as represented by susceptibility to interpersonal influence). Accordingly, extending prior studies, this essay investigates the moderating role of social influence within an organization such that both rules ethical climate and susceptibility to interpersonal influence weaken the effect of the command-and-control and self-regulatory approaches on employee ISP compliance. Using survey data collected from employees on Amazon Mechanical Turk, we showed that both rules-oriented ethical climate and susceptibility to interpersonal influence weaken the effects of command-and-control and self-regulatory on ISP compliance.

In the third essay, we adopt peer monitoring from management context to the information security context and then investigate its effectiveness in motivating employees to comply with the ISP. Peer monitoring, which happens when employees observe their peers' behavior and respond to their misconducts either by reporting or correcting them, have shown to have a great potential to increase employee performance (Dickenson and Mclntyre 1997; Jong 2010; Loughry and Tosi 2008; Marks 2001; Marks and Panzer 2004). Drawing on the literature from organizational prosocial behavior and management, this essay investigates (1) the effectiveness of peer monitoring in motivating employee ISP compliance, (2) the mechanisms through which peer monitoring influence employee ISP compliance, and (3) the social context (group reward structure) that promotes the perception of peer monitoring. We tested our hypotheses with 891 valid responses collected via Qualtrics panel. Our results showed that peer monitoring in the group is positively associated with employee ISP compliance, and such an effect is partially mediated by commitment to the ISP and perceived deterrence of ISP noncompliance. In addition, peer monitoring in the group was induced by perception of collective responsibility, which itself was a product of perception responsibility by commission and responsibility by omission.

In summary, this dissertation deepens the understanding of role of social influence in employee ISP compliance. First, it provides the framework showing that how social influence can be formed, can be internalized and then activated to motive employees to comply with the ISP. Then, it investigates the interplay between the well-established motivational approaches and social influence (at both micro and macro level). Finally, it adopts the approaches that are based on social influence into the information security setting and then analyzes their effectiveness and contextual factors. The results show that social norms can be shaped through the organizational climate and shape employees' personal norms, which eventually will be activated to guide employee to comply with the ISP. Further, the results show that organizational ethical climate and susceptibility to interpersonal influence weakens the impact the well-studied command-and-control and self-regulatory approaches. Finally, the results show that peer monitoring (as a strategy that is rooted in social influence) is an effective means in motivating employee ISP compliance. In addition, it indicates that the effect of peer monitoring is mediated by perceived deterrence as well as commitment to the ISP. Finally, it asserts that collective responsibility norm in a group can induce employee to do peer monitoring.

Chapter One:

Employees’ Information Security Policy Compliance: A Norm Activation Perspective

1.1. INTRODUCTION

The information security policy (ISP) of an organization defines a set of rules and policies related to employees' access and use of organizational information assets. It usually describes employees' responsibilities and the consequences of policy violations (Bulgurcu et al. 2010; Hu et al. 2011). However, regardless of the breadth and clarity of an ISP, without employee compliance, it cannot successfully serve as an effective countermeasure to information security violations. Therefore, ways to improve and motivate employee compliance with an ISP has drawn a lot of attention (Liang et al. 2013; Liu et al. 2014; Siponen et al. 2006; Vance et al. 2012; Zhao and Xue 2009).

Because employees often work in a group or team within an organization, the behavior or opinion of one is likely to influence another's (Cialdini and Trost 1998). In exploring employee compliance with ISP, social norms in the form of normative beliefs (Bulgurcu et al. 2010; Pahnila et al. 2007), social pressure (Herath and Rao 2009b), social influence (Johnston and Warkentin 2010), and subjective norms (Herath and Rao 2009a; Ifinedo 2012) have been recognized as important factors. However, as Torgler (2002) posits, "when working with social norms, we have the difficulty of specifying their exact meaning" (p. 663). Similarly, the information security literature does not have a unanimous definition and categorization of social norms. Some studies refer to them as subjective norms or social pressure from peers and superiors (Siponen et al. 2010), others refer to them as descriptive and subjective norms (Bulgurcu et al. 2010; Herath and Rao 2009a), and in some cases, normative beliefs and social pressure have been used interchangeably. Existing studies commonly emphasize external motivators that directly influence behavior. Yet, how such external normative influences are internalized and consequently alter ISP compliance behavior has been barely investigated.

In an organization, there are two general types of norms: social and personal norms (Kerr 1995). Social norms, grounded in social interactions among individuals, broadly define behavioral rules based on common beliefs about how people should act in a particular situation. They indirectly promote a group's well-being through informal rewards and sanctions founded on group expectations. On the other hand, personal norms are private and internalized norms grounded in one's beliefs and values. They influence behavior when an individual feels their most important values are endangered (Stern et al. 1999). In extension, reward and sanctions are self-imposed (Biel and Thøgersen 2007). Personal norms produce norm-based behavior (Schwartz 1977), while social norms may affect behavior after an individual accepts and internalizes them as personal norms. In fact, the presence of personal norms diminishes the direct effect of social norms in explaining a behavior (Klöckner and Blöbaum 2010; Thøgersen 1999).

To broaden the understanding of the role norms play in motivating ISP compliance behavior, this study proposes a research model rooted in norm activation theory (Schwartz 1977), social norms theory (Cialdini and Trost 1998), and ethical climate literature (Victor et al. 1988). We argue that ISP-related personal norms are a determinant of ISP compliance behavior. Through the lens of norm activation theory (Schwartz 1977) from sociological literature, we propose that awareness of consequence and ascription of personal responsibility in ISP compliance positively moderates the effect of ISP-related personal norms on ISP compliance behavior. Building off the theory of social norms (Cialdini and Trost 1998), we propose that ISP-related social norms, including descriptive, injunctive, and subjective norms, shape ISP-related personal norms. Lastly, we propose that ISP-related social norms are the product of a principle ethical climate.

The proposed research model integrates theories on norms from social psychology literature (Cialdini and Trost 1998) to explain ISP compliance behavior. It recognizes the important role of ISP-related personal norms and explores how they are formed and activated. We tested the research model using data collected through Amazon Mechanical Turk, which comprises 201 valid responses from working professionals in a diverse set of organizations. The findings may help organizations better motivate employees to comply with the ISP.

The paper is organized as follows: Section 2 introduces the theoretical background. Section 3 then develops the hypotheses, and section 4 describes the research method. Next, section 5 presents the analysis and results. Finally, section 6 discusses the theoretical and practical implications as well as future research directions.

1.2. THEORETICAL BACKGROUND

1.2.1. Effect of Personal Norms: Norm Activation Theory

Norm activation theory (Schwartz 1977) posits that personal norms are the immediate antecedent of one's behavior. Personal norms are defined as self-expectations enforced through the anticipation of self-punishments and self-rewards. Although grounded in internalized values, this self-based code of conduct is also the outcome of an individual's perception of social expectations (Schwartz 1977). An individual may engage in socially acceptable behavior to avoid social sanctions, but they may continue following those norms due to internal motives, such as improving self-image (Kelman 1958).

The theory further suggests that personal norms affect behavior once they are activated (Schwartz 1977). Here, activation refers to directing an individual's focus to their beliefs in their decision-making process. While following personal norms may enhance self-regard and avoid self-criticism, it could also result in such costs as extra effort and time. If the benefits outweigh the costs, the behavior is likely to happen (Schwartz 1973). However, if the costs are significant, that may negate the motive to comply with personal norms.

Successful neutralization allows the violation of personal norms without self-sanctions (Schwartz 1973). Two common neutralization approaches that undermine the activation of personal norms are denial of consequences and denial of personal responsibility for the act (Schwartz 1973). The former involves underestimating the negative outcomes of an action to justify it (Agnew and Peters 1986; Siponen and Vance 2010), while the latter involves considering the action in question as beyond one's control or outside one's realm of responsibility (Agnew and Peters 1986; Siponen and Vance 2010).

To overcome neutralization approaches and activate personal norms, two conditions are required. First, an individual must realize that their behavior affects the welfare of others, which is known as awareness of consequences. The latter may be physical or psychological. Second, an individual must accept personal responsibility for the consequences of their behavior. This is termed ascription of personal responsibility.

Schwartz (1977) originally developed norm activation theory to rationalize altruistic behavior. It was mostly applied in a pro-environmental context to explain pro-environmental behaviors, such as conservation behavior (Barnett and Karson 1989), pro-environmental buying (Thøgersen 1999), recycling (Brekke et al. 2010), travel mode choice (Klöckner and Matthies 2004), and car use (Bamberg and Schmidt 2003). To the best of our knowledge, we are the first to apply this theory in the context of information security.

1.2.2. Theory of Social Norms: Personal Norms Formation

Social norms are implicit and explicit rules and standards that members of a group learn through socialization—direct and indirect communication and interactions with others. They guide or restrain behavior through social sanctions, not the force of law, and can be categorized into descriptive, injunctive and subjective norms (Cialdini and Trost 1998).

Descriptive norms are grounded in an individual's perception of how others act in a specific situation (Cialdini and Trost 1998). For example, people typically stand up and clap at the end of a concert. The desire to follow descriptive norms is rooted in amplifying the efficacy of social behavior. Descriptive norms help individuals determine the appropriate behavior in similar situations (Cialdini et al. 1991). In other words, having noticed what others do in a similar situation, individuals perceive sufficient social support for a particular behavior in a new or uncertain, but similar, situation (Reno et al. 1993).

Injunctive norms involve perceptions of approval and disapproval of certain behaviors, the moral rules of a group, and what "should" be done (Cialdini et al. 1991). These behaviors often garner social acceptance or others' approval (Opp 1982). The desire to follow injunctive norms is rooted in an individual's social nature and tendency to build, develop, and maintain social relationships with others to gain resources and social support.

Subjective norms are defined as what an individual believes important others (e.g., family, friends, and supervisors) expect them to do in a specific situation (Cialdini and Trost 1998). The motivations to follow them are similar to that of injunctive norms: to build, develop, and maintain social relationships and particularly to earn others' approval. However, subjective norms guide an individual based on their perception of what those important to them expect as opposed to what everyone else, in general, expect (Cialdini and Trost 1998).

The social norms and cost of deviance in the group encourages members to act in ways that they consider other members think they "should." The degree to which social norms regulate behavior depends on whether the individual has accepted and internalized them as opposed to just learning them (Staub 1972). Internalization refers to the process of an individual accepting a norm as intrinsically satisfying and in line with their own value system (Kelman 1958). An individual who has internalized social norms is likely to conform to expected behaviors even when they are not observed or externally sanctioned (Perugini et al. 2003). Through internalization, social norms become personal norms (Schwartz 1977; Schwartz and Howard 1981).

1.2.3. Principle Ethical Climate

The ethical climate of an organization describes the moral atmosphere of the workplace. In extension, a principle ethical climate is an aspect of the organizational climate. In this kind of environment, employees place a high priority on obeying rules, policies, and professional codes (Victor et al. 1988), all of which factor into their ethical decision-making (Barnett and Vaicys 2000; Hollinger and Clark 1982). In other words, employees working in a principle ethical climate have a positive regard for rule adherence and policy compliance. It therefore could consequently shape social norms in terms of ISP compliance (Adkins and Russell 1994; Posner 1992; Thomas 2013), which may be considered ethical behavior as it is a specific type of rule adherence.

An organizational climate typically has a particular referent, such as a climate for diversity (McKay et al. 2009), safety (Cooper and Phillips 2004), or ethics (Victor et al. 1988). It is suggested that the inclusion of organizational climate should be consistent with the research topic of a study, which is ISP compliance behavior in this case (Ashkanasy et al. 2004). Since principle ethical climate refers to employees' shared perception of the company procedures, practices, and policies (Reichers and Schneider 1990), in this study, we postulate that it creates a proper reference for employee's ISP-related decisions, and we argue that it shapes social norms regarding ISP compliance.

1.3. HYPOTHESIS

Figure 1.1 shows our research model, which consists of three parts. We propose that ISP-related personal norms have a positive influence on ISP compliance (Hypothesis 1). ISP-related awareness of consequences and ascription of personal responsibility not only positively influence personal norms, but also positively moderate the effect of personal norms on ISP compliance (Hypothesis 2-5). Moreover, ISP-related descriptive, injunctive, and subjective norms lead to ISP-related personal norms (Hypothesis 6-8). Finally, principle ethical climate shapes ISP-related descriptive, injunctive, and subjective norms (Hypothesis 9a-c).

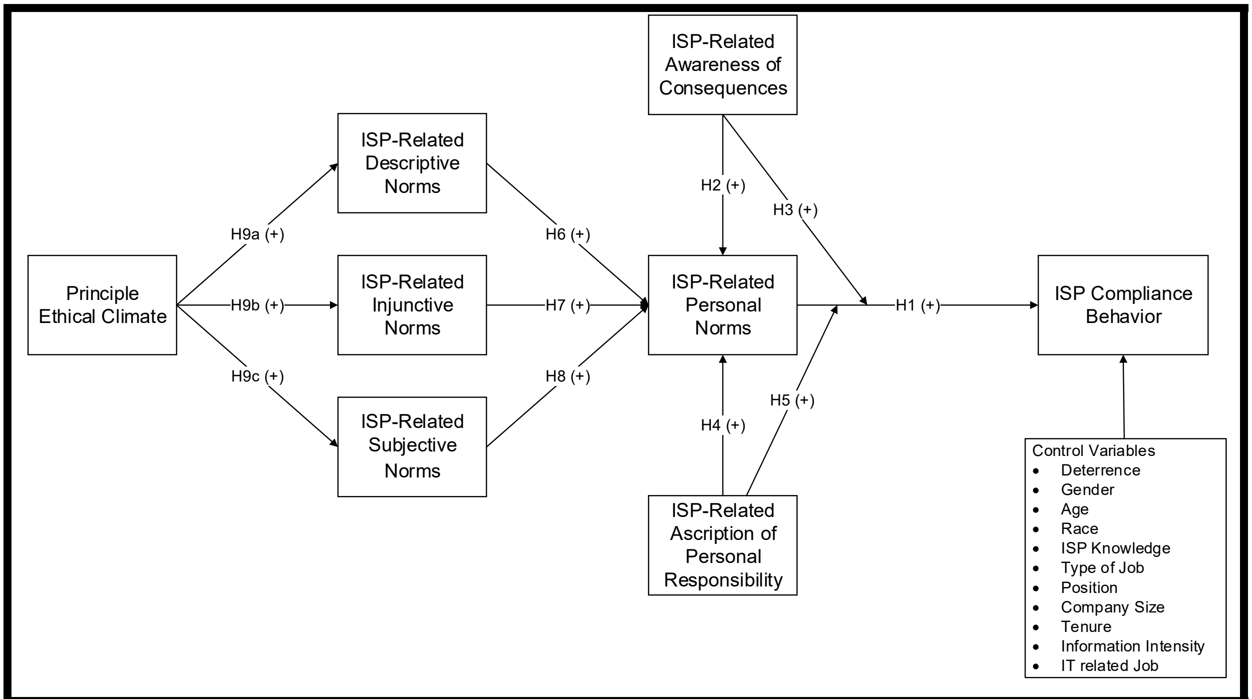

ISP-Related Awareness of Consequences
ISP-Related Descriptive Norms
Principle Ethical Climate
ISP-Related Injunctive Norms
ISP-Related Subjective Norms
ISP-Related Personal Norms
ISP Compliance Behavior
ISP-Related Ascription of Personal Responsibility
H9a (+)
H9b (+)
H9c (+)
H6 (+)
H7 (+)
H8 (+)
H2 (+)
H3 (+)
H1 (+)
H4 (+)
H5 (+)
Control Variables
Deterrence
Gender
Age
Race
ISP Knowledge
Type of Job
Position
Company Size
Tenure
Information Intensity
IT related Job

Figure 1.1. Research Model

1.3.1. Effect of Personal Norms

Norm activation theory suggests that personal norms are the primary factor that influences behavior (Schwartz 1977). We define ISP-related personal norms as the employee’s own values, views, and expectations about ISP compliance through self-punishments and self-rewards. They may be experienced as feelings of obligation (rather than a rational sense of right and wrong) (Schwartz 1977) that motivate an employee to engage in ISP compliance. Adhering to ISP-related personal norms imply that an employee's ISP-related decisions are in line with their own belief system (Osterhus 1997).

According to rational choice theory (Akers 1990; Paternoster and Simpson 1996), the psychological costs and benefits of violating or complying with ISP could trigger the development of ISP-related personal norms. In extension, if an employee experiences psychological benefits from satisfying ISP-related personal norms, they would consider ISP compliance behavior as a rewarding act (Vandenbergh 2005). Therefore, we argue that if an employee considers following ISP-related personal norms in ISP-related decisions as a moral obligation, they will comply with ISP. Recent research in the information security literature also revealed that personal norms are a determinant factor that affects the way employees deal with organizational issues, including those related to appropriate computer behaviors and Internet use (Ifinedo 2014; Li et al. 2014; Myyry et al. 2009). Therefore, we propose that:

H$_1$: *ISP-related personal norms have a positive influence on ISP compliance.*

We expect ISP-related awareness of consequences and ascription of responsibility will positively moderate the relationship between ISP-related personal norms and ISP compliance. We define ISP-related awareness of consequences as the awareness an employee has about the negative or positive consequences of their ISP-related behavior on the welfare of their coworkers or the organization as a whole. Previous information security studies examined information security awareness but not ISP-related awareness of consequence (Bulgurcu et al. 2010; Siponen and T. 2000; Wu et al. 2012). Information security awareness refers to employee's general knowledge about requirements stated in security policies and their objectives, rather than consequences of ISP-related behavior on an organization and its employees (Bulgurcu et al. 2010; Siponen and T. 2000). Our definition is more in the line with the overall assessment of consequence (Bulgurcu et al. 2010), except in our definition focal group is employee's coworkers or the organization while the latter focuses on the individual her/himself. Secondly, we define ISP-related ascription of responsibility as the employee's feelings of responsibility for the negative or positive consequences of their ISP-related behavior. Here, responsibility is the sense of connection with the destiny of the organization and coworkers.

The tendency to adopt neutralization approaches, including denial of consequence and responsibility, lowers the probability of ISP-related personal norms inducing ISP compliance behavior (Schwartz 1973). Understanding the importance of consequences and responsibility regarding ISP-related acts lowers the chance neutralization approaches being adopted toward ISP-related personal norms (Schwartz 1973). However, without ISP-related consequence awareness, the feeling of moral obligation (personal norms) is less likely to manifest as ISP compliance (Biel and Thøgersen 2007). An employee with a low awareness of consequences has a vague idea of the potential negative or positive outcomes of their acts on their coworkers or the organization. Such an employee is more likely to neutralize their ISP-related personal norms with the denial of consequence approach. Similarly, an employee with a high awareness of consequences is aware of both broad and detailed consequences of their acts on their coworkers or the organization. Thus, it is expected that such an employee would considers their coworkers' welfare and avoid denial of consequence when making an ISP-related decision (Schwartz 1968). Therefore, we expect a more successful transition of ISP- related personal norms to ISP compliance in an employee with a high ISP-related awareness of consequence. Accordingly, we hypothesize that:

H$_2$: *ISP related awareness of consequences positively moderates the effect of ISP-related personal norms on ISP compliance.*

When making an ISP-related decision, an employee with low ascription of personal responsibility toward ISP is more likely to use the denial of responsibility approach to justify violating ISP-related personal norms (Schwartz and Howard 1980). Similarly, an employee with high ascription of personal responsibility toward ISP is more likely to feel responsible to protect information assets and avoid the denial of responsibility approach. Thus, the latter employee is expected to show stronger transition of their ISP-related personal norms to ISP compliance behavior (Schwartz 1973). Therefore, we argue that an employee's ISP-related ascription of personal responsibility affects the manifestation of ISP-related personal norms into ISP compliance behavior. Accordingly, we hypothesize that:

H$_3$: *ISP-related ascription of personal responsibility positively moderates the effect of the ISP-related personal norms on ISP compliance.*

1.3.2. Effect of Social Norms

The theory of social norms suggests that individuals are more likely to internalize (in the form of personal norms) behavior approved by others in the group (Cialdini and Trost 1998). We argue that ISP-related descriptive, injunctive, and subjective norms play a significant role in shaping an employees' perception of ISP compliance. In fact, internalization of social norms shapes employee perception of ISP and their future behavior. We argue that if an employee perceives that "everybody follows the organization's ISP" (descriptive norms), "everybody thinks it is wrong to violate the organization's ISP'' (injunctive norms), and/or "their manager thinks it is wrong to violate the ISP'' (subjective norms), then they are more likely to believe they are morally obligated to follow the ISP (personal norms). Prior studies have confirmed the above line of reasoning in different contexts (Bobek et al. 2013; Osterhus 1997; Thøgersen 1999). We define ISP-related descriptive norms as an employee's perception of the majority of coworkers' ISP compliance behavior. In general, descriptive norms arise from the idea that if everybody is doing a particular act in a particular situation, it must be an expected behavior (Cialdini et al. 1990; Sheeran and Orbell 1999). Therefore, if a high number of employees respond to an ISP-related situation in a similar way, an employee will perceive that particular way as the correct behavior (Thibaut and Kelley 1959). The information security literature sparsely explored the influence of peer behavior as a motivational source for an individual's behavior in uncertain situations (Thompson et al. 1991; Viswanath Venkatesh , Michael G . Morris , Gordon B . Davis et al. 2003). We argue that an employee, in an effort to be more accurate and efficient (Cialdini and Trost 1998) in their ISP-related decisions, observe their coworkers' behaviors and internalizes perceived behaviors as the correct behavior in regard to ISP compliance. Thus, we hypothesize that:

H$_4$: *ISP-related descriptive norms are positively associated with ISP-related personal norms.*

We define ISP-related injunctive norms as an employee's perception of what the majority of their coworkers' think they should do in ISP-related situations. The information security literature highlighted the importance of injunctive norms and showed that they can influence ISP-related behavior (Herath and Rao 2009a). Beside observing the majority of coworkers' behavior (ISP descriptive norms), employees recognize reasonable and acceptable ISP behavior through their perception of the majority of coworkers' expectations (ISP injunctive norms). A social benefit or penalty is behind the motivation to follow injunctive norms (Cialdini and Trost 1998). An employee's perception of the majority's values (injunctive norms) will shape their perception of ISP compliance behavior. When an employee perceives that ISP compliance is what the majority believe is what should be done, they are more likely to internalize ISP compliance behavior as part of their values to meet their colleagues' expectations and improve their relationships. Accordingly we hypothesize that:

H$_5$: *ISP-related injunctive norms are positively associated with ISP-related personal norms.*

We define ISP-related subjective norms as an employee's perceptions about what those important to them think they should do in ISP-related situations. ISP-related subjective norms are injunctive norms with a specific referent. In general, an individual is more likely to follow subjective norms to meet the expectations of those important to them (Herath and Rao 2009a). In the information security literature, studies on the perceptions of employees about expectations of relevant others (Karahanna et al. 1999; Viswanath Venkatesh , Michael G . Morris , Gordon B . Davis et al. 2003) suggest that top managers, supervisors and peers in information systems department are among the most relevant references when they make an ISP-related decision (Herath and Rao 2009a; Karahanna et al. 1999). In extension, we argue that, when an employee perceives that ISP compliance is what their supervisor or manager thinks they should do, they are more likely to internalize ISP compliance behavior as part of their own values to satisfy the expectation of and improve their relationship with their supervisor or manager. Thus, we hypothesize that:

H$_6$: *ISP-related subjective norms are positively associated with ISP-related personal norms.*

1.3.3. Principle Ethical Climate and ISP-related Social Norms

Whether an employee considers the organization to have a principle ethical climate shapes ISP-related social norms (Chan et al. 2005; Herath and Rao 2009a). In this type of ethical climate, employees place higher value on following rules, policies, and standards (Victor et al. 1988), and the former can serve as a guiding principle. In other words, in developing ISP-related norms, employees may consider the prevalent attitude toward organizational policies and rules and accordingly make a decision in an ISP-related situation. A principal ethical climate can offer a useful reference point for acceptable ISP-related behaviors, or ISP-related descriptive norms. In addition, by demonstrating the viewpoints of the majority, including important others' expectations of proper ISP-related behavior, a principle ethical climate presents a sound reference for ISP-related injunctive and subjective norms. Thus, overall, a principle ethical climate would help provide relevant ideas about the majority's behaviors (descriptive) and expectations (injunctive norms), including those of supervisors and upper management (subjective norms). Therefore, we hypothesize:

$\mathbf{H_{7a}}$: *A perceived principle ethical climate has a positive influence on ISP-related descriptive norms.*

$\mathbf{H_{7b}}$: *A perceived principle ethical climate has a positive influence on ISP-related injunctive norms.*

$\mathbf{H_{7c}}$: *A perceived principle ethical climate has a positive influence on ISP-related subjective norms.*

1.4. RESEARCH METHODOLOGY

To test our model we used the survey method. We did a comprehensive literature review and formed the preliminary instrument using pre-existing items from previous studies to ensure the reliability and validity of items (Straub 1989). We adapted some of the items to the context of information security policy compliance whenever needed. We did a pretest and refined our instruments. The survey participants were recruited through Amazon Mechanical Turk (MTurk) via an online survey.

1.4.1. Instrument Development

We started item development by prudent investigation of the literature. We asked several experienced information systems faculty and Ph.D. students who had experience in survey research methods to give us feedback on our preliminary measurement items and ensure that the items are well-defined and consistent with each construct (i.e., face validity). We measured all the key constructs in the model using multiple items with 7-point Likert scales. They were modeled as reflective constructs.

The measurement of ISP compliance behavior was adapted from Tyler and Blader (2005) and modified to fit the context of ISP. We adapted the items for ISP-related personal norms, awareness of consequences, and ascription of personal responsibility from the context of social psychology (Schwartz 1977; Steg and de Groot 2010). ISP-related descriptive and subjective norms came from prior literature in information security (Anderson and Agarwal 2010; Herath and Rao 2009a). ISP-related injunctive norms were adapted from prior literature in social psychology (Cialdini and Trost 1998) and tax aversion (Bobek et al. 2013). Lastly, principle ethical climate was from organizational behavior and ethics literature (Victor et al. 1988). Table 1.1 lists all the constructs along with their measurement items.

Table 1.1. Measurement Items

Constructs	Items	Source
Principle Ethical Climate	Everyone is expected to stick by company rules and procedures. Successful people in this company strictly obey the company policies. It is very important to follow strictly the company’s rules and procedures here.	(Victor et al. 1988)
Awareness of Consequences	I believe violation of the organization's ISP will cause serious troubles to other employees. I believe violation of the organization's ISP will cause serious damages to the organization. I worry about problems caused by violation of the organization's ISP.	(Schwartz 1977; Steg and de Groot 2010)
Ascription of Personal Responsibility	I believe that I am co-responsible for the protection of the organization's ISP. I feel responsible to do something against violation of the organization's ISP. I feel responsible to help my colleagues comply with the organization's ISP.	(Schwartz 1977; Steg and de Groot 2010)
Personal Norms	I feel morally obligated to comply with the organization's ISP. I feel guilty if I do not comply with the organization's ISP. I am willing to put extra effort into complying with the organization's ISP on a regular basis.	(Schwartz 1977; Steg and de Groot 2010)
Descriptive Norms	I believe other employees comply with the organization's ISP. I think most employees in my organization follow the organization's ISP I am convinced other employees in my organization comply with the organization's ISP. It is likely that the majority of other employees in my organization comply with the organization's ISP.	(Anderson and Agarwal 2010; Cialdini and Trost 1998; Herath and Rao 2009a)
Injunctive Norms	I believe other employees in my organization would feel embarrassed not to comply with the organization's ISP	(Bobek et al. 2013; Schwartz

	I believe other employees in my organization would feel ashamed if they violate the organization's ISP. I believe other employees in my organization would feel guilty if they violate the organization's ISP.	1977; Steg and de Groot 2010)
Subjective Norms	My boss thinks that I should follow the organization's ISP. Computer technical specialists in my organization think that I should follow the organization's ISP. Top management in my organization thinks I should follow organization's ISP. The information security department in my organization thinks that I should follow organization.	(Anderson and Agarwal 2010; Cialdini and Trost 1998; Herath and Rao 2009a)
ISP Compliance Behavior	How often do you comply with the organization's ISP? How often do you use the organization's ISP to guide what you do on the job? How often do you seek information about the organization's ISP before acting? How often do you follow the Organization's ISP about how you should use information systems related resources?	(Tyler and Blader 2005)
Deterrence	If I violate the Organization's ISP, I would probably be caught. The chance to be caught is high, if I do not follow the organization's ISP Employees are properly monitored for policy violations. My organization disciplines employees if they break the organization's ISP. If I repeatedly break the organization's ISP, my organization terminates me. If I were caught violating the organization's ISP, I would be severely punished.	(Herath and Rao 2009b)
ISP Knowledge	How would most of your coworkers characterize you with regard to the level of KNOWLEDGE you have about your organization’s information security policies? How would other employees characterize you with regard to the level of KNOWLEDGE you have about your organization’s information security policies?	(Bloch et al. 1989)

1.4.2. Survey Administration

We first conducted a pilot study with MBA students at a major university in the southwest United States. We refined our instrument and then carried out an online survey with working professionals recruited through Amazon's Mechanical Turk (MTurk) as the respondents. MTurk is an online crowdsourcing labor market. It provides a platform through which you can hire people to perform diverse tasks in exchange for payment. MTurk has been suggested to be a reliable source for data collection in prior studies (Buhrmester et al. 2011; Paolacci et al. 2010; Rand 2012). Buhrmester et al. (2011) found that it represents the American population better than student data. Further, it enables us to reach a broader spectrum of respondents.

We used Qualtrics to create the online survey. At the beginning of the survey after the consent form, we defined of ISP and gave examples of typical information security policies. We filtered out respondents who were not employed or whose job did not require them to comply with

ISP. We also limited our respondents to those in the United States. We obtained 201 validated responses. The data includes 116 men and 85 women. Table 1.2 shows other demographic information.

Table 1.2. Demographic Characteristics of Participants

Gender		Information intensiveness of your company		Size of your department	
Male	116	Not information intensive at all	2	1-10 employees	49
Female	85	Some	29	11-20 employees	51
Age		Quite a Bit	89	21-30 employees	35
18-25	36	An Extreme Amount	45	31-40 employees	20
26-35	90	Highly information intensive	40	40+ employees	46
36-45	36	Years you have been at this company		Size of your company	
46-55	24	Less than one year	10	Fewer than 500 employees	79
56-65	11	1-5 years	119	500–999	34
66-75	3	6-10 years	44	1,000–4,999	29
76-85	1	11-15 years	18	5,000–10,000	9
Race		15+ years	10	1,000+ employees	5
White/Caucasian	162	Position		Type of Job	
African American	13	Upper Management	6	Full Time	168
Hispanic	7	Middle Management	35	Part Time	33
Asian	13	Lower Management	50		
Native American	3	Non-management	110		
Other	3				

1.5. ANALYSIS AND RESULTS

We used the partial least squares (PLS) approach to test and estimate the structural model. A component-based approach for estimation, PLS does not suffer from identification issues and violation of normality when compared to covariance-based approaches (Wynne W. Chin 1998). In addition, this study focuses on understanding the effect of various factors on ISP compliance, rather than emphasizing the fit between observed correlations and model parameters (Gefen, D. W. Straub, et al. 2000). Furthermore, our model has not been tested in the information security literature yet, which makes the nature of our study more exploratory, rather than confirmatory. SmartPLS version 2.0.M3 (Ringle et al. 2005) was used in the estimation.

1.5.1. Measurement Validation

Prior to testing the structural model, we evaluated the psychometric properties of the measurement items. All constructs were modeled as reflective latent constructs. Item reliability, convergent validity, and composite reliability as well as factor and cross loadings were calculated for each construct to assure the measurement quality of the constructs (Gefen, D. W. Straub, et al. 2000; Rand 2012). Convergent and discriminant validities were investigated using the following approaches. First, all other cross correlations are smaller than the square root of the average variance extracted (AVE) of all constructs (Gefen and Straub 2005). Second, all constructs' AVEs are higher than 0.5, which suggests the construct-related variance is higher than error variance. Third, as the correlations among all constructs are very small, all constructs are distinct from each other (Gefen and Straub 2005; Hair et al. 2009). Lastly, the loading of all items were highest on their intended constructs (Gefen, D. W. Straub, et al. 2000). All factor loadings were close to or higher than 0.70 (Chin and Marcolin 1995) with significant t-values, showing that around or more than 50 percent of the variance shared among items for each construct (Wynne W Chin 1998). All the mentioned results suggest sufficient convergent and discriminant validities

The data for the independent and dependent variables were gathered from the same survey instrument. Thus, the common method bias (CMV) could have biased the study (Podsakoff, MacKenzie, Lee, et al. 2003). To determine whether it was a concern, we carried out Harman's one-factor test (Podsakoff, MacKenzie, Lee, et al. 2003). We executed an exploratory factor analysis with measurement items for all constructs (Podsakoff, MacKenzie, Lee, et al. 2003). Nine factors came out from the analysis, which explained 76.73 percent of the data variance. No single factor was found that explained the majority of the variance. The largest variance explained by a factor was 33 percent. Therefore, we conclude that CMV is not a major concern.

Table 1.3. Factor Loadings And Cross-Loadings

	PR	AC	APR	PN	DN	IN	SN	COM	DET	KN
PR1	**0.87**	0.25	0.33	0.42	0.34	0.23	0.57	0.34	0.37	0.06
PR2	**0.90**	0.34	0.41	0.51	0.42	0.39	0.34	0.39	0.55	-0.01
PR3	**0.89**	0.40	0.38	0.57	0.32	0.38	0.39	0.41	0.51	-0.02
AC1	0.30	**0.86**	0.29	0.49	0.26	0.29	0.25	0.41	0.47	0.06
AC2	0.34	**0.91**	0.39	0.52	0.25	0.37	0.41	0.51	0.55	0.14
AC3	0.28	**0.68**	0.55	0.43	0.15	0.34	0.08	0.29	0.32	0.07
APR1	0.46	0.45	**0.83**	0.49	0.32	0.33	0.37	0.42	0.30	0.17
APR2	0.19	0.28	**0.81**	0.37	0.31	0.30	0.02	0.27	0.18	0.07
APR3	0.32	0.39	**0.80**	0.42	0.33	0.39	0.12	0.31	0.24	0.12
PN1	0.51	0.49	0.40	**0.86**	0.32	0.42	0.42	0.37	0.46	-0.04
PN2	0.45	0.48	0.39	**0.84**	0.26	0.51	0.34	0.36	0.49	-0.08
PN3	0.45	0.48	0.53	**0.79**	0.35	0.32	0.36	0.52	0.35	0.07
DN1	0.37	0.28	0.34	0.33	**0.94**	0.42	0.41	0.34	0.39	0.02
DN2	0.35	0.23	0.35	0.32	**0.92**	0.41	0.37	0.30	0.41	-0.03
DN3	0.33	0.23	0.40	0.33	**0.90**	0.40	0.35	0.34	0.40	-0.02
DN4	0.44	0.27	0.37	0.37	**0.92**	0.38	0.47	0.38	0.44	0.00
IN1	0.34	0.34	0.37	0.45	0.39	**0.91**	0.22	0.32	0.34	-0.01
IN2	0.33	0.35	0.32	0.47	0.33	**0.93**	0.18	0.31	0.37	-0.04
IN3	0.35	0.40	0.46	0.45	0.47	**0.88**	0.21	0.29	0.36	0.07
SN1	0.48	0.33	0.22	0.48	0.36	0.27	**0.84**	0.46	0.35	0.09
SN2	0.41	0.32	0.26	0.36	0.42	0.21	**0.90**	0.39	0.25	0.14
SN3	0.42	0.22	0.16	0.36	0.40	0.16	**0.87**	0.43	0.28	0.11
SN4	0.37	0.25	0.21	0.34	0.35	0.10	**0.85**	0.34	0.25	0.10
COM1	0.51	0.43	0.32	0.43	0.53	0.35	0.61	**0.69**	0.44	0.09
COM2	0.22	0.37	0.34	0.38	0.19	0.23	0.30	**0.78**	0.22	0.13
COM3	0.23	0.38	0.28	0.36	0.08	0.27	0.18	**0.79**	0.32	0.03
COM4	0.31	0.35	0.35	0.35	0.29	0.16	0.31	**0.81**	0.34	0.04
DET1	0.44	0.56	0.25	0.47	0.29	0.32	0.22	0.36	**0.87**	-0.18
DET2	0.43	0.51	0.27	0.46	0.32	0.32	0.22	0.32	**0.85**	-0.17
DET3	0.43	0.47	0.32	0.36	0.34	0.30	0.17	0.30	**0.73**	0.05
DET4	0.49	0.51	0.29	0.44	0.45	0.31	0.32	0.43	**0.86**	0.07
DET5	0.41	0.27	0.18	0.37	0.40	0.33	0.34	0.33	**0.76**	-0.05
DET6	0.48	0.47	0.21	0.47	0.43	0.38	0.35	0.41	**0.90**	-0.03
KN1	0.02	0.08	0.14	-0.01	-0.02	0.02	0.13	0.09	-0.06	**0.97**
KN2	0.01	0.14	0.16	-0.04	0.00	0.00	0.11	0.10	-0.05	**0.97**

PR: Principle, AC: ISP related Awareness of Consequence, APR: ISP related Ascription of Personal Responsibility, PN: ISP related Personal Norms, DN: ISP related Descriptive Norms, IN: ISP related Injunctive Norms, SN: ISP related Subjective Norms, DET: Deterrence, COM: ISP Compliance Behavior, KN: ISP Knowledge.

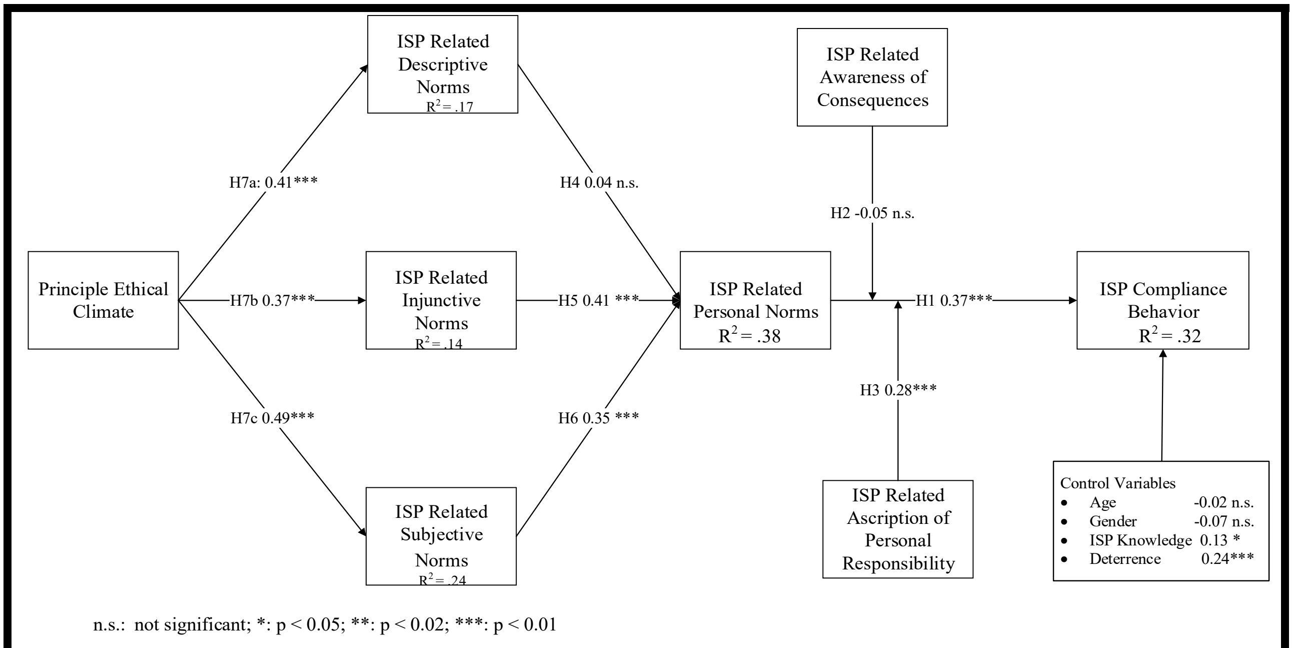
Table 1.4. Reliability, Average Variance Extracted And Construct Correlation Matrix

	AVE	CR	AL	PR	AC	APR	PN	DN	IN	SN	COM	DET	KN
Perceived Principle Ethical Climate	0.78	0.91	0.86	**0.88**									
Awareness Of Consequence	0.68	0.86	0.76	0.37	**0.82**								
Ascription Of Responsibility	0.66	0.85	0.75	0.42	0.47	**0.81**							
Personal Norms	0.69	0.87	0.78	0.56	0.58	0.53	**0.83**						
Descriptive Norms	0.84	0.96	0.94	0.41	0.28	0.39	0.37	**0.92**					
Injunctive Norms	0.83	0.93	0.89	0.37	0.40	0.42	0.50	0.44	**0.91**				
Subjective Norms	0.75	0.92	0.89	0.49	0.33	0.24	0.45	0.44	0.22	**0.87**			
Compliance	0.59	0.85	0.77	0.43	0.50	0.42	0.50	0.37	0.34	0.47	**0.77**		
Deterrence	0.69	0.93	0.91	0.54	0.56	0.30	0.52	0.45	0.39	0.33	0.44	**0.83**	
ISP Knowledge	0.94	0.97	0.94	0.01	0.11	0.16	-0.02	-0.01	0.01	0.12	0.10	-0.06	**0.97**

AVE, Average Variance Extracted; CR, Composite Reliability; AL, Cronbach's alpha.
Note: The diagonal represent the square root of (AVE) values.

1.5.2. Hypothesis Testing

To test the hypotheses, we first ran the main effects model without the interaction terms (Carte and Russell 2003). We performed a t-test using bootstrapping with 600 re-samples to examine the statistical significance of path coefficients. Figure 1.2 shows the standardized PLS path coefficients, paths significance (based on a two-tailed test), and the amount of variances explained. In PLS, R^2 in the endogenous constructs suggests the explanatory power of the model. Results indicate that the factors studied in the model explain almost 38 percent of the variance in personal norms and consequently 32 percent of the variance in information security policy behavior. The model can be considered a satisfactory and valid model since the percentages of variance explained were greater than 10 (Faulk and Miller 1992).



n.s.: not significant; *: $p < 0.05$; **: $p < 0.02$; ***: $p < 0.01$

Fig. 1.2. PLS results

The results indicate that ISP-related personal norms have a significant effect (β= .37; p<0.001) on ISP compliance, which supports H1. To test the moderating effects (H2 and H3), we followed a product-indicator approach (Chin et al. 2003) in which by cross-multiplying the items of relevant constructs, a multiplicative term was created and then standardized to prevent multicollinearity (Aiken et al. 1991). The interaction terms were added to the main effects model. The results indicate that the ISP-related awareness of consequence does not moderate (T-statistics=0.78, β=− .05, ΔR^2=0.00) the relationship between personal norms and ISP compliance (not supporting H2), while ISP-related ascription of personal responsibility positively (β= .28; p<0.05; ΔR^2=0.05) moderates the relationship between personal norms and ISP compliance (supporting H3) (refer to Table 1.5 and Figure 1.2). In addition, we tested the moderation effect of ISP-related ascription of personal responsibility on the relationship between ISP-related personal norms and ISP compliance following Carte and Russell's (2003) method. We evaluated the significance of the difference between the variance explained by the moderating effect and main effect using the following F-statistics:

$$F(df_{Interaction} - df_{main}, N - df_{Interaction} - 1) = \frac{\Delta R^2/(df_{Interaction} - df_{main})}{(1 - R^2{}_{Interaction})/(N - df_{Interaction} - 1)}$$

The F-statistics for the moderating effect of ISP-related ascription of personal responsibility was 15.12 and significant (p<0.01). We further validated the moderating effect using Cohen's f^2, which compares the R^2 value of the interaction effect on the main effect with the following equation (Chin et al. 2003): $f^2 = (R^2{}_{Interaction} - R^2{}_{Main})/\ (1 - R^2{}_{Main})$ = (0.362-0.312) / (1-0.312) = 0.072. It indicates a medium effect (Chin et al. 2003). Overall, the results provide evidence that ISP-related ascription of personal responsibility moderates the relationship between ISP-related personal norms and ISP compliance.

The results also suggest that ISP-related descriptive norms do not have any association (T-statistics=0.61, β= .04) with ISP-related personal norms (H5 not supported), while ISP-related injunctive (β= .41; p<0.001) and subjective norms have a significant effect (β= .35; p<0.001) on ISP-related personal norms (supporting H6 and H7). These results emphasize that injunctive and subjective norms mainly shape personal norms. Next, the results indicate a principal ethical climate has a significant effect on the development of ISP-related descriptive (β= .41; p<0.001), injunctive (β= .37; p<0.001), and subjective norms (β= .49; p<0.001) (supporting H7a, b, and c).

The information security literature has investigated the effect of organization deterrence motivators, such as perceived certainty of detection and severity of the punishment, and showed that they contribute to ISP compliance (Herath and Rao 2009a). In this study, we tested deterrence as a control variable. The results show that it has a significant effect on ISP compliance (β= .24; p<0.02), which is consistent with prior studies. Moreover, having knowledge about the organizational ISP can be a decisive factor that leads to ISP compliance (Bulgurcu et al. 2010). In this study, we considered ISP knowledge as a control variable. The results show a significant effect of ISP knowledge on compliance behavior (β= .13; p<0.05).

1.5.3. Post Hoc Analyses

The insignificant relationship between ISP-related descriptive norms and ISP-related personal norms is not in line with what was proposed in this paper. Thus, in search of a possible explanation, we looked at the social norms literature again. One possible explanation is the fact that ISP-related descriptive norms emerge from observing other coworkers, while ISP-related injunctive and subjective norms pertain to the general expectation of coworkers and relevant others, such as a supervisor or boss. Thus, by observing others, an employee can learn others' expectations and gradually develop their perception of ISP-related injunctive and subjective norms. Therefore, it may be likely that ISP-related descriptive norms shape them. To test this proposition, we conducted a post hoc analysis and found that ISP-related descriptive norms are positively associated with ISP-related injunctive (β= .45; p<0.001) and subjective norms (β= .44; p< .001).

The lack of support for the moderation effect of ISP-related awareness of consequence can be explained by the fact that an employee becomes aware of the consequences of their ISP-related behavior before feeling responsible for it. The information system literature also revealed that information security awareness, in general, could raise employee's awareness of their responsibilities about an organization's information assets (D'Arcy et al. 2009; Straub and Welke 1998). Thus, it is possible that an employee's overall ISP-related awareness of consequence influences their ISP-related ascription of personal responsibility, rather than moderating the relationship between ISP-related personal norms and ISP compliance. Our post hoc analysis showed that ISP-related awareness of consequence positively affects ISP-related ascription of personal responsibility (β=0.56; p<0.01).

Table 1.5. Hypothesis Results

Hypothesis	Hypothesis Direction	Path Coefficient	T-Value	Significance (Two-Tailed)	Supported?
H1	PN -> COM (+)	0.37	4.83	P<0.001	Yes
H2	DN -> PN (+)	0.04	0.61	n.s.	No
H3	IN -> PN (+)	0.41	5.54	P<0.001	Yes
H4	SN -> PN (+)	0.35	4.96	P<0.001	Yes
H5	PN*AC -> COM (+)	-0.05	0.78	n.s.	No
H6	PN*APR -> COM (+)	0.28	2.86	P<0.005	Yes
H7A	PR -> DN (+)	0.41	5.38	P<0.001	Yes
H7B	PR -> IN (+)	0.37	5.95	P<0.001	Yes
H7C	PR -> SN (+)	0.49	6.46	P<0.001	Yes
Control Variables	Age -> COM	-0.02	1.40	n.s.	-
	Gender -> COM	-0.07	1.62	n.s.	-
	ISP KN -> COM	0.13	2.18	p<0.05	-
	DET -> COM	0.25	3.12	p<0.02	-

PR: Principle, AC: Awareness of Consequence, APR: Ascription of Personal Responsibility, PN: Personal Norms, DN: Descriptive Norms, IN: Injunctive Norms, SN: Subjective Norms, DET: Deterrence, COM: Compliance Behavior, KN: ISP Knowledge

1.6. DISCUSSION AND CONCLUSION

This study suggests personal norms play an important role in ISP compliance. We investigated the antecedents of ISP-related personal norms as well as its activators. We showed that ISP-related social norms of the organization shape ISP-related personal norms. We also showed that ISP-related personal norms are more likely to influence ISP compliance behavior when employees feel personal responsibility for it. In addition, this study connects the concept of a principle ethical climate to the ISP compliance literature and shows that a principle ethical climate can play an important role in shaping ISP-related social norms. This is especially important since the information security literature rarely studied the effect of principle ethical climate.

1.6.1. Theoretical Implications

This study moves beyond the often-studied deterrence and protection motivation theory (Herath and Rao 2009a; Siponen et al. 2006; Woon et al. 2005) perspectives in understanding ISP compliance. Our model combines different concepts from social psychology literature (Cialdini and Trost 1998; Schwartz 1977; Stern et al. 1999) into a single framework to explain ISP compliance behavior. Thus, our key contribution is we are among the first to investigate the overlooked factor of ISP-related personal norms as an important predictor of ISP compliance behavior. The results are especially interesting because they offer a potential alternative explanation other than well-established factors, such as subjective norms, monitoring, and punishment for ISP-related compliance behavior.

This paper theoretically contributes to the information security literature by adopting well-established social psychology theories of norm activation (Schwartz 1977) and social norms (Cialdini and Trost 1998) into the information security literature. Furthermore, this study contributes to norm activation (Schwartz 1977) and social norms theory (Cialdini and Trost 1998) by operationalizing it in an organizational setting. This is remarkable, considering that norm activation theory primarily has been operationalized in prosocial and environmental settings (Klöckner and Blöbaum 2010; Schwartz 1977; Thøgersen 1999). We contend that our model introduces multi-theoretical perspectives on ISP compliance behavior. Thus, our model can be considered a core framework for future studies examining the role of ISP-related personal norms in information security.

1.6.2. Practical Implications

We believe the findings from our study should help businesses and IT managers better understand the antecedents of ISP compliance behavior and how to manage their employees. Moreover, the implications of this study can help organizations improve their information security programs and policies. The results suggest that changes in the working environment in favor of compliance are advantageous and help shape ISP-related personal norms and thereby increase ISP compliance. As an achievable practice, we suggest that organizations create a principle ethical climate and encourage ISP-related social norms to enhance ISP compliance.

In addition, based on the results, information security managers can encourage ISP compliance becoming a social norm by integrating information security policies in daily business processes. By expanding the literature on what motivate employees to comply with ISP, this study can help organization implement systems to change or improve the organizational ethical climate in favor of more employee compliance with the ISP.

1.6.3. Limitations and Future Research

This study may have burden some limitations that may provide possibility for further investigation. First, our results are restricted to employees who work in the United States. Thus, it is possible that cultural values threaten the generalizability of the results. Moreover, our model explains only a fraction of variance in ISP compliance. It is obvious there are factors we did not examine. Future research can explore such factors as employees' personal characteristics or organization culture to enhance the understanding of ISP compliance. Furthermore, because workers self-report answers to a survey concerning compliance, there is the possibility of responses being skewed toward ISP compliance. We suggest that future studies use other approaches or data sources to measure ISP compliance behavior.

Chapter Two:

Peers Matter: The Role of Social Influence on Information Security Policy Compliance

2.1. INTRODUCTION

Prior studies in information security suggest that not only organizational enforcement (Herath and Rao 2009) but also personal preferences and desires (Myyry et al. 2009) influence the degree to which employees comply with their orgnaizational informaiton security policy (aka ISP compliance). Along this line, many researchers (Bulgurcu et al. 2010; D'Arcy and Herath 2011; Guo et al. 2011; Herath and Rao 2009a, 2009b; Hu et al. 2011; Li et al. 2010; Liang et al. 2013; Myyry et al. 2009; Siponen and Vance 2010; Son 2011; Yazdanmehr and Wang 2016) have overtly investigated the extrinsically oriented *command-and-control* approach and the intrinsically oriented *self-regulatory* approach. The former refers to the method by which organizations control rule compliance behavior through the perception of how they detect and react to (i.e., punish) ISP violation or noncompliance, whereas the latter refers to the extent to which one's rule compliance behavior is directed by perceived legitimacy of organizational rules and value convergence with these rules (Tyler and Blader 2005).

Extending prior studies, this research note proposes a social contingency model and investigates the moderating role of social influence within an organization. Whenever an individual changes his or her behavior in response to cues from other influencing agents, it can be said that social influence has taken place (Kelman 1974). Social influence can manifest at both the macro- and micro- levels. At the macro-level, it can be an implicitly strong and definite climate in an organization, signaling whether following company rules and procedures is an ethically expected behavior, often referred to as rules-oriented ethical climate (Victor et al. 1988). It provides a powerful normative system informing employees about the organizational common practices and priorities on dealing with ethical dilemmas regarding following organizational policies and procedures (Barnett and Vaicys 2000; Brass et al. 1998; Gaertner 1991; Victor et al.

1988). Its importance, with respect to the ethical behavior of employees (e.g., ISP compliance), has been well-known. A novel perspective explored in this research note is an examination of how rules-oriented ethical climate moderates the effects of the two regulatory approaches (i.e., command-and-control and self-regulatory) on ISP compliance.

At the micro level, social influence manifests as peer interactions through which other employees convey acceptable and expected viewpoints, reasons for an action, and logical consequences of expected behaviors. In fact, changes in an individual's behavior are often viewed as an outcome of interactions with other individuals perceived to be similar, desirable, or experts (Rashotte 2007). Social interactions can also direct an individual's attention to a particular social cue and make that behavior more pronounced (Salancik and Pfeffer 1978). An individual's *susceptibility to interpersonal influence* reflects the degree to which they accept such interpersonal influences (Bearden et al. 1989). The concept denotes both the tendency to seek out information about appropriate behaviors from peers and the willingness to conform to the expectations of peers in terms of appropriate behavior (c.f., Bearden et al. 1989). We argue that, similar to rules-oriented ethical climate, susceptibility to interpersonal influence sets up a boundary condition for the effects of command-and-control and self-regulatory approaches on ISP compliance.

Examining the moderating role of the two aspects of social influence can advance the understanding of the effectiveness of command-and-control and self-regulatory approaches in motivating ISP compliance. In this research note, we find that both rules-oriented ethical climate and susceptibility to interpersonal influence weaken the effects of aforementioned approaches on ISP compliance. To the best of our knowledge, the present research represents the first endeavor to examine the effectiveness of well-established command-and-control and self-regulatory approaches from a social influence perspective, thereby providing a deeper understanding of the phenomenon. Macro- and micro- level influences can affect employee responsiveness to both approaches. From a practical perspective, our findings provide useful insights to managers on how to develop an organizational climate that can enhance ISP compliance.

2.2. THEORETICAL BACKGROUND

2.2.1. ISP Compliance and Rule-Following Approaches

In studying compliance behavior, two primary perspectives are taken: instrumental and normative (Tyler 1990). The instrumental perspective assumes that individuals are motivated mainly by self-interest and respond as per the swift, tangible rewards and punishments associated with an act (Tyler 1990). The normative perspective, in contrast, assumes that individuals are driven primarily by what they consider to be legitimate and consistent with their values. It argues that individuals comply with rules to the degree that they perceive the rules as acceptable (i.e., legitimate) and consistent with the values of their own (Sutinen and Kuperan 1999; Tyler 1990). In the context of ISP compliance, the command-and-control and the self-regulatory approaches have been examined as the two primary motivational forces (Bulgurcu et al. 2010; D'Arcy and Herath 2011; Guo et al. 2011; Herath and Rao 2009a, 2009b; Hu et al. 2011; Li et al. 2010; Liang et al. 2013; Myyry et al. 2009; Siponen and Vance 2010; Son 2011).

The command-and-control approach follows the instrumental view (Tyler and Blader 2005). It considers that employees as rational actors are self-interested, and compliance behavior is a function of perceived costs and benefits (Becker 1968; Tyler and Blader 2005). Accordingly, organizations could actively enforce rules by providing incentives to encourage desired behavior and/or sanctions to discourage undesirable behavior to increase compliance (Sutinen and Kuperan 1999; Tyler 2009; Tyler and Blader 2005).

In the context of ISP compliance, researchers have recognized that few organizations implement rewarding policies for ISP compliance but most rely on sanctions (D'Arcy et al. 2009; D'Arcy and Hovav 2007; Herath and Rao 2009a; Lee et al. 2004; Pahnila et al. 2007; Siponen and Vance 2010; Straub 1990). A combination of both organizational detection and reaction to ISP violations or noncompliance, measured through employees' perception, is often specified as immediate determinants of compliance behavior. From the view of an organization, the command-and-control approach is to inform potential wrongdoers about: (1) the probability that the noncompliance act will be detected is high, and (2) there will be a punishment that outweighs possible benefits achieved by noncompliance (Geerken and Gove 1975). These are two essential aspects of the command-and-control approach considered in the context of ISP compliance (D'Arcy et al. 2009; Gibbs 1975; Nagin and Pogarsky 2001; Parker 1998; Straub and Nance 1990; Tittle 1980).

The self-regulatory approach considers intrinsic desires as the primary drivers of behavior. There are two types of intrinsic motivation for compliance: (1) value congruence, i.e., the extent to which the organization has values consistent with those of the employees; (2) legitimacy, i.e., the extent to which the organization is led by legitimate authorities and structured around legitimate rules (Tyler 1990; Tyler and Blader 2005). Value congruence considers individuals' desires to follow their sense of personal values, and personal values can in turn motivate compliance when they are in line with those rules (Kranz and Haeussinger 2014; Malhotra et al. 2008; Robinson and Darley 1995). The other type of intrinsic motivation, legitimacy, is associated with individuals' intrinsic obligation to follow the demands of a legitimate authority (Tyler 2006). When rules (e.g., ISP) dictated by the authorities are perceived as legitimate, high compliance is expected. Legitimacy and value convergence are correlated but distinct elements, each capturing a unique part of the self-regulatory approach (Tyler 2006).

2.2.2. Rules-oriented Ethical Climate

Ethical climate, in general, refers to the shared perception of what is ethically appropriate and how ethical issues should be handled (Victor et al. 1988). By providing standards, normative structures, policies, and routines, an ethical climate signals an organization's priorities on solutions to ethical dilemmas (Wyld and Jones 1997). Through ethical climate, individuals acquire an exclusive set of experiences and relationships with others in the organization that eventually affect their ethical judgment—they develop a unique understanding of what is an ethical issue, how critical an issue is, and how to react to it (Ferrell and Gresham 1985; Hunt and Vitell 1986; Sutherland et al. 1992; Trevino 1986). In an organization with a high level of ethical climate, employees are exposed to peers who have uniform and consistent expectations about the most appropriate (i.e., ethical) behaviors (Mischel 1977), resulting in the formation of clear ethical judgments (Shin 2012). Conversely, in an organization with a low level of ethical climate, employees are exposed to peers who have inconsistent views regarding ethical behaviors, resulting in uncertain ethical judgments (Shin 2012). Thus, a strong ethical climate in the organization is expected to help employees make clear ethical judgments, especially when they face an ethical dilemma (Banerjee et al. 1998; Trevino 1986) in which there is a conflict between individuals' own interest and collective rationality (e.g., following rules-oriented ethical climate) (Kahan 1974; Pillutla and Chen 1999).

Whether ethical climate is multi-dimensional or uni-dimensional is debatable. Nevertheless, in this study, we follow the many scholars who consider it to be a multi-dimensional construct. The most established classification is the one provided by Victor et al. (1988), which is built on Kohlberg's (1981) moral development theory and Gouldner's (1957) moral philosophy. Based on their typology, ethical climate consists of two dimensions, namely ethical approach and ethical referent. Ethical approach is also known as ethical criterion, which can be principle, benevolence, or egoism. Principle ethical criterion refers to the consideration of the application and interpretation of the rules, whereas benevolence and egoism ethical criterion consider the well-being of others and an individual's self-interest, respectively (Victor et al. 1988). Ethical referent is also called the locus of analysis, which focuses on the individual, local, or cosmopolitan level. While the individual level emphasizes the self, the local level focuses on the immediate social context surrounding the individual (e.g., organizational practices), and the cosmopolitan level goes beyond the immediate organization or group (e.g., professional codes) as the prime referent for moral reasoning (Victor et al. 1988). Applying the above criteria, Victor et al. (1988) empirically classified ethical climates into five types: rules (company policies and procedures adherence), law and code (violation of laws), caring (welfare of others), instrumental (self-interest), and independence (personal beliefs adherence).

Rules-oriented ethical climate focuses on a company's policies and procedures adherence (Victor et al. 1988). It can act as a psychological utility for the macro-level social influence within an organization because (1) it is based on the ethical criterion of principle and the local locus of analysis (Victor et al. 1988), which is the focus of this study; (2) it offers the best framework for demonstrating accepted and expected behaviors related to established rules and policies (i.e., information security policies) in the company (Chan et al. 2005; Schneider 1975; Victor et al. 1988); and (3) it captures employees' perception of organizational policies, code of ethics, and top management actions regarding ethics (Jaramillo et al. 2006), reflecting the essence of a uni-dimensional ethical climate (Shin 2012).

A strong rule-oriented ethical climate in the organization may lead to individuals' clear judgement that rule compliance is more of an ethics issue (i.e., ethical decision frame). The absence of such an influence leads to ambiguous understanding about whether complying with the rules is an ethical matter, and thus directs an individual's attention to the risks and punishments/rewards associated with rule compliance decisions or to the rules legitimacy and rules convergence with his or her own values (intrinsic desire) (i.e., business decision frame) (Tenbrunsel and Messick 1999). Thus, the presence of informational cue about the degree to which organization members follow the rules (e.g., rules-oriented ethical climate) is likely to diminish the impact of other sources of reasoning (e.g., command-and-control and self-regulatory) (c.f., Tenbrunsel and Messick 1999).

2.2.3. Susceptibility to Interpersonal Influence

Interpersonal sources of influence refer to the non-organizational personal sources through which employees consider obtaining information related to an issue at hand (Bearden et al. 1989; Mourali et al. 2005; Yang et al. 2015). They can be peers with whom an individual interacts face-to-face, and/or others with whom an employee would like to be associated psychologically (e.g., reference group) (Bearden et al. 1989). Susceptibility to interpersonal influence is viewed as a representation of social influence at the micro organizational level in this study because it closely resembles an employee's tendency to seek and accept the influence from others in the company.

The main distinction between interpersonal influence and other sources of influence (e.g., command-and-control or self-regulatory) is that, in interpersonal exchanges, the communicators have the opportunity to get clarifications and instant feedbacks (Mourali et al. 2005). Such a feature makes interpersonal communications an appealing source in one's decision making process. As such, employees' tendency to be influenced by an interpersonal source, or their susceptibility to interpersonal influence (SPI; Bearden et al. 1989), could play a significant role in changing the impact of other sources of influence on their behavior. In this study, we show that susceptibility to interpersonal influence diminishes the effect of rule-following approaches on ISP compliance.

Interpersonal influence is typically channelled through either informational influence or normative influence (Deutsch and Gerard 1955). Accordingly, susceptibility to interpersonal influence has two dimensions, namely susceptibility to informational influence and susceptibility to normative influence (Bearden et al. 1989). Both types of influences are distinct but synthesize a specific phenomenon of an individual's tendency to be influenced by others.

Susceptibility to informational influence reflects an individual's tendency to seek out and accept information from others as a valid indication of reality. It may occur when an individual is actively requesting information from knowledgeable others or when they make an assumption by observing others' behavior (Park and Lessig 1977). Susceptibility to normative influence reflects an individual's tendency to observe and conform to the expectations of others. It may happen when an individual attempts to identify with a reference group to enhance his or her image in the eyes of important others (i.e., value expressiveness influence) (Bearden and Etzel 1982; Kelman 1961; Park and Lessig 1977). It may also occur when an individual complies with others' expectations to gain rewards or avoid punishments (i.e., utilitarian influence) (Bearden and Etzel 1982; Burnkrant and Cousineau 1975; Park and Lessig 1977).

In the context of this study, susceptibility to interpersonal influence happens when an employee tries to learn more about a proper way of ISP compliance, by seeking out information from their peers, and/or when an employee conforms to others' expectations regarding how to comply with ISP. Informational influence may be associated with such behaviors as discussing with peers, asking for peers' advices, and sending inquiries to information security professionals (e.g., IT department) regarding ISP compliance. Normative influence may be linked to such behaviors as mimicking the behaviors of those an employee admires, and/or seeking for important others' approval for ISP compliance.

Previous research indicates that susceptibility to interpersonal influence is a key factor in shaping individuals' attitudes, norms, values, and aspirations in the context of smoking and drinking (Yang et al. 2013) and music piracy (Yang et al. 2015), among others. However, its role as a moderator in general and its interplay with rule-following approaches in particular has not been investigated yet.

2.3. HYPOTHESIS DEVELOPMENT

2.3.1. Effects of the Command-and-Control and Self-Regulatory Approaches on ISP Compliance

We expect the command-and-control approach to positively affect ISP compliance. Following rational choice theory (Becker 1968; Cornish and Clarke 1986; Paternoster and Simpson 1996), employees' compliance decision can be a function of their percieved costs and benefits of ISP compliance. The command-and-control approach informs employees what is the chance to be detected and what is the punishment they would face if they do not comply with the ISP. If the company is strict on ISP noncompliance (e.g., strong monitoring system along with severe punishments), employees may consider that the cost of ISP noncompliance is high and thus comply with the ISP. The command-and-control approach has traditionally been used as a primary strategy to encourage ISP compliance (D'Arcy and Herath 2011; Straub 1990). Accordingly, we hypothesize that:

H$_1$: *The command-and-control approach is positively associated with employee ISP compliance.*

We expect the self-regulatory approach to be positively related to employee ISP compliance. When employees perceive the organizational ISP as legitimate, they are more inclined to follow it. Congruence between an individual's values and the organizational ISP can enhance and endorse those values and thereby motivate ISP compliance because employees tend to behave in line with their values (Tyler and Blader 2005). Therefore, the self-regulatory approach relies on an employee's intrinsic desire to follow the ISP. Consistent with this reasoning, Myyry et al. (2009) found that employee moral reasoning and values are the key drivers of ISP compliance. Li et al. (2014), in the context of Internet use, found that the self-regulatory approach is more effective than the command-and-control approach in affecting individuals' complying with Internet use policy. Similarly, Son (2011) reported that perceived legitimacy and value convergence contribute significantly to ISP compliance. Yazdanmehr and Wang (2016) showed that personal norms regarding ISP lead to better ISP compliance. Accordingly, we hypothesize that:

H_2: *The self-regulatory approach is positively associated with employee ISP compliance.*

2.3.2. The Moderating Role of Rules-oriented Ethical Climate

Rules-oriented ethical climate provides situational cues prompting an employee to understand that adhering to organizational policies is ethical (Messick 1999; Shin 2012). In an organization with a strong rules-oriented ethical climate, employees who engage in ISP decision making have a clear understanding of what constitutes an ethical or unethical ISP-related behavior (Shin 2012). Such employees are more likely to base their ISP-related decisions upon ethics considerations (i.e., the ethical decision frame) (Tenbrunsel and Messick 1999). On the contrary, in an organization with a weak rules-oriented ethical climate, employees may not have a clear understanding of whether adhering to organizational policies is ethical or not (Shin 2012). Therefore, they are more likely to rely on the command-and-control and/or self-regulatory approaches as alternatives to ethical climate in their ISP decision making.

Given that rules-oriented ethical climate can play an important role in forming employees' ISP-related decisions (Barnett and Schubert 2002; Kramer and Messick 1996), we argue that in an organization with a strong rules-oriented ethical climate, employees who debate on whether to comply with the ISP are largely expected to find solutions using the cues from such a climate (Barnett and Schubert 2002; Kramer and Messick 1996). This could weaken other drivers (i.e., command-and-control and self-regulatory) affecting employees' choice. Accordingly, we hypothesize that:

H$_3$: *Rules-oriented ethical climate negatively moderates the effect of command-and-control approach on ISP compliance, in such a way that the effect is less pronounced when an organization's rules-oriented ethical climate is high than low.*

H$_4$: *Rules-oriented ethical climate negatively moderates the effect of self-regulatory approach on ISP compliance, in such a way that the effect is less pronounced when an organization's rules-oriented ethical climate is high than low.*

2.3.3. The Moderating Role of Susceptibility to Interpersonal Influence

Employees with different levels of susceptibility to interpersonal influence may display different levels of responsiveness to the command-and-control approach. Relative to individuals with low levels of susceptibility to interpersonal influence, those with high levels tend to make their decision based upon the information collected from others, the desire to be accepted by others (Bonabeau 2004), and the passion to gain reputational benefits (Kuran 1997; Sunstein 1996) or positive self-image (Wrong 1961). Moreover, mimicking the behaviors of important others helps people discount the perceived risk of ISP noncompliance (Wang et al. 2011). We expect that those who have high susceptibility to interpersonal influence may emulate their peers and discount the effect of organizational sanction threats. They are likely to view the behavior as acceptable or believe adopting it may enhance their self-image or social status. Thus, the command-and-control approach has less impact on employee ISP compliance for those with higher levels of susceptibility to interpersonal influence. Accordingly, we hypothesize that:

H$_5$: *Susceptibility to interpersonal influence negatively moderates the effect of command-and-control approach on ISP compliance in such a way that the effect is less pronounced when susceptibility to interpersonal influence is high than low.*

Similarly, susceptibility to interpersonal influence can undermine the impact of self-regulatory on ISP compliance. Those with a high level of susceptibility may regard making decisions based upon one's inner feelings or beliefs as immature or selfish; as a result, they are often encouraged to sacrifice personal goals for a good relationship with others (Yang and Laroche 2011). In contrast, employees with a low level of susceptibility have the autonomy to ignore social influence constraints (Mourali and Yang 2013), and make decisions based on their own internal attitudes and thoughts, without taking into account the attitudes and thoughts of others (Yang et al. 2015). Translating these findings into our study context, it is expected that employees who are less susceptible to interpersonal influence would follow their own values and assumptions (self-regulatory) regarding ISP compliance, thereby resulting in a stronger impact of the self-regulatory approach on ISP compliance behavior. Accordingly, we hypothesize that:

H$_6$: *Susceptibility to interpersonal influence negatively moderates the effect of the self-regulatory approach on ISP compliance in such a way that the effect is less pronounced when susceptibility to interpersonal influence is high than low.*

Figure 2.1 summarizes these hypotheses and presents the social contingency model of ISP compliance.

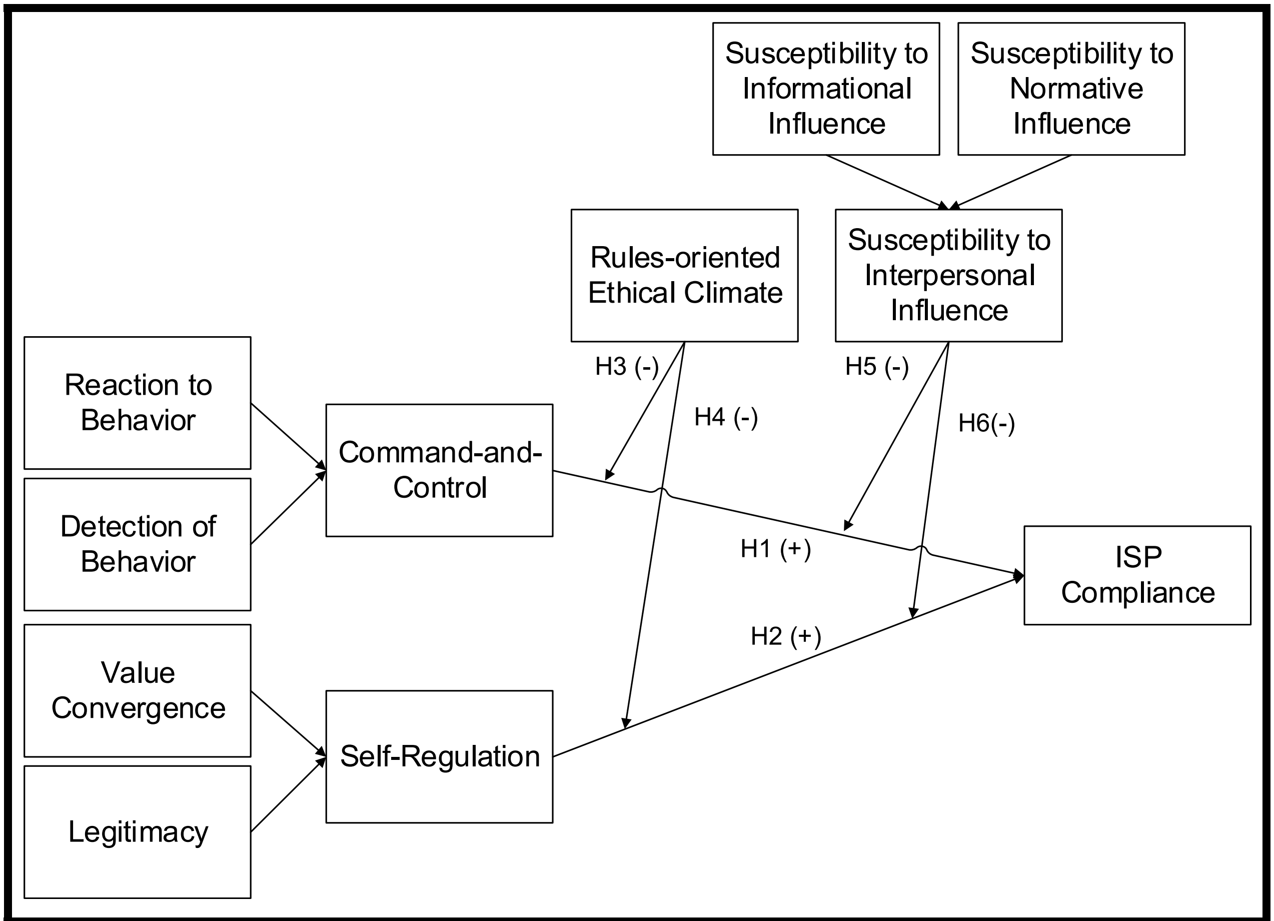


Figure 2.1: A social contingency model of ISP compliance

2.4. RESEARCH METHOD

2.4.1. Data Collection

We collected the data from employees recruited through Amazon Mechanical Turk (or Mturk). To ensure we targeted the right respondents, we placed screening questions at the beginning of the survey and asked participants to indicate whether they are employed part- or full-time at the time of completing the survey. For those who responded yes, we provided the definition of information security policy with illustrative examples. We filtered out participants whose organization did not have an ISP in place or whose job did not require ISP compliance. The sample was restricted only to the residents of the United States. There are a total of 246 valid participants comprised of 124 men (50.4%) and 122 women (49.6%); 217 had a full-time job (88.2%) while 29 had a part-time job (11.8%). Their average age was 39 (see Table 2.1 for detailed demographic characteristics of participants).

2.4.2. Measures

Pre-existing instruments from prior research were adapted to our study. All of the key constructs in the model were measured using multiple items. Following the discussions in the theoretical background section, command-and-control, self-regulatory, and susceptibility to interpersonal influence are conceptually second-order formative constructs[1]. Specifically, the self-regulatory construct has two dimensions, namely legitimacy and value convergence. The measurement items were adapted from Tyler and Blader (2005). Command-and-control has two dimensions, including detection and reaction to behavior, and their items were also adapted from Tyler and Blader (2005). The two dimensions of susceptibility to interpersonal influence are susceptibility to informational influence and susceptibility to normative influence.

The items were adapted from Yang et al. (2015) and Bearden et al. (1989). Organizational rules-oriented ethical climate was assessed by Victor et al.'s (1988) scale. All items used a 7-point Likert scale. Experienced IS faculty members (other than the authors) and Ph.D. students who had experience in survey-based research examined the measurement items to make sure they were clear. One hundred MBA students from a major university in the southwest of the United States carried out a pilot study. The necessary modifications on the survey instruments were made based on the pilot study (See Table 2.2 for the final set of items).

[1] We also modeled these second-order constructs as reflective measurement, but did not find significant difference between the formative and reflective models.

Table 2.1. Demographic Characteristics of Participants

	Total	Percentage		Total	Percentage
Gender			**IT-Related Job**		
Male	124	50.4	Yes	106	43.1
Female	122	49.6	No	140	56.9
Age					
18-25 Years	26	10.6	46-55 Years	34	13.8
26-35 Years	93	37.8	56-65 Years	28	11.4
36-45 Years	62	25.2	66-85 Years	3	1.2
Type of Job			**Race**		
Full-time	217	88.2	White/Caucasian	180	73.2
Part-time	29	11.8	African American	25	10.2
Education			Asian	17	6.9
Less Than High School	0	0.0	Hispanic	16	6.5
High School Graduate	15	6.1	Native American	3	1.2
Some College	58	23.6	Other	5	2.0
College Graduate	124	50.4	**Position**		
Post-Graduate Education	49	19.9	Upper Management	7	2.8
Company Size			Middle Management	56	22.8
Fewer than 500 employees	89	36.2	Lower Management	58	23.6
500–999	46	18.7	Non-management	125	50.8
1,000–4,999	34	13.8	**Tenure**		
5,000–10,000	12	4.9	Less than one year	14	5.7
1,000+ employees	65	26.4	1-5 years	138	56.1
Industry			6-10 years	49	19.9
Information Technology	20	8.1	11-15 years	20	8.1
Financial Services	24	9.8	15+ years	25	10.2
Healthcare	29	11.8	**Information Intensiveness**		
Telecommunications	18	7.3	Not information intensive at all	3	1.2
Retail	59	24.0	Some	42	17.1
Manufacturing	14	5.7	Quite a Bit	75	30.5
Government	33	13.4	An Extreme Amount	72	29.3
Other	49	19.9	Highly information intensive	54	22.0

2.5. DATA ANALYSIS AND RESULTS

We used structural equation modeling to test our model. To validate measurement scales and test the proposed model, the component-based partial least squares (PLS) approach was used.

We chose it because, unlike covariance-based approaches such as LISREL, PLS does not suffer from identification issues or non-normal distributed data (Fornell and Bookstein 1982).

Table 2.2. Measurement Items

	Constructs	Items	Source
	ISP Compliance Behavior	How often do you comply with your organization's ISP? How often do you use your organization's ISP to guide you how to access to and use information assets? How often do you follow the organization's ISP about how you should use information systems related resources? How often do you follow the requirement of your organization's ISP? How often do you do as your organization's ISP request?	(Tyler and Blader 2005)
	Rules Ethical Climate	Successful people in this company go by the book. Everyone is expected to stick by company rules and procedures. Successful people in this company strictly obey the company policies.	(Victor and Cullen 1988)
Command-and-control	Reaction to Behavior	If you are caught breaking the organization's ISP, how much does it hurt you pay or your chances for promotion? If you were caught breaking the organization's ISP, how much would your organization care?	(Tyler and Blader 2005)
	Detection of Behavior	How closely is your work monitored by your organization? How easy is it for your organization to observe whether or not you follow the organization's ISP? How often is your organization paying attention to whether or not you follow the organization's ISP?	(Tyler and Blader 2005)
Self-regulatory	Value Convergence	I find that my values and the values where I work are very similar. What my company stands for is important to me. I agree with the values that define the goals of my company. I think that my employer acts very ethically. I find that my values and the values where I work are very similar.	(Tyler and Blader 2005)
	Legitimacy	People should support their organizational ISP. It is wrong to break organizational ISP, even if you can get away with it. Companies are most successful when employees follow their organizational ISP. Work organizations are most effective when people follow their organizational ISP. Respect for organizational ISP is an important value for employees to have. An employee should accept the organizational ISP, even when they think that those policies are wrong.	(Tyler and Blader 2005)
Susceptibility to Interpersonal Influence	Susceptibility to Informational Influence	To make sure that I correctly follow the organization's ISP, I often observe what others do. I often consult other people to help choose the correct way to comply with the organization's ISP. If I am uncertain whether my action will violate the organization's ISP or not, I often ask my coworkers about it. When I do not know how to comply with a particular information security policy, I usually ask friends or coworkers. If I am uncertain whether my action will comply with the organization's ISP or not, I often ask my coworkers about it.	(Bearden et al. 1989)
	Susceptibility to Normative Influence	I usually comply with the organization's ISP that I think others will approve of. I achieve a sense of belonging by complying with the same information security policies that others comply with. If others can see my compliance behavior, I will often comply with the policies that they expect me to comply with. To maintain a good relationship with my coworkers, I often comply with those policies that they comply with. I feel that complying with a particular ISP policy will enhance my image.	(Bearden et al. 1989)
	ISP Knowledge	How would most of your coworkers characterize you with regard to the level of KNOWLEDGE you have about your organization’s information security policies? How would other employees characterize you with regard to the level of KNOWLEDGE you have about your organization’s information security policies?	(Bloch et al. 1989)

In addition, as the moderation effects proposed in our study (rules-oriented ethical climate and susceptibility to interpersonal influence) have not been tested in the information security literature, our study is more explanatory than confirmatory in nature. Therefore, techniques intended to maximize the variable prediction, rather than goodness of fit, are more suitable (Gefen et al. 2011).

2.5.1. Measurement Validation

The Smart-PLS (version 2.0.M3) software package (Ringle et al. 2005) was used for the estimations. Before testing the hypotheses, we examined the convergent validity, individual item reliability, composite reliability, and discriminant validity to ensure the measurement quality of all principle constructs. We calculated factor and cross-loadings (see Table 2.4), the average variance extracted (AVE) values, the composite reliability, and Cronbach's alpha for each construct (Table 2.3). The AVE values for all constructs were greater than the recommended minimum of 0.50, thereby indicating that the items satisfied the convergent validity. The square root of each construct's AVE was higher than the construct's correlations, with all of the other constructs and factor loading for each item being higher than its cross-loadings on other constructs (at least 0.10). These results indicate the items satisfied the discriminant validity (Hair et al. 2009).

Table 2.3. Reliability, Average Variance Extracted and Construct Correlation Matrix

	AVE	CR	AL	COM	RUL	DB	RB	VC	LG	KN	SII	SNI
COM	0.75	0.94	0.92	**0.87**								
RUL	0.78	0.92	0.86	0.58	**0.88**							
DB	0.73	0.89	0.82	0.35	0.43	**0.86**						
RB	0.89	0.94	0.88	0.44	0.46	0.61	**0.95**					
VC	0.83	0.96	0.95	0.36	0.54	0.32	0.22	**0.91**				
LG	0.72	0.94	0.92	0.68	0.58	0.42	0.44	0.47	**0.85**			
KN	0.83	0.90	0.79	0.21	0.17	0.22	0.14	0.28	0.19	**0.91**		
SII	0.73	0.93	0.91	0.29	0.31	0.31	0.28	0.31	0.38	0.08	**0.85**	
SNI	0.72	0.93	0.90	0.22	0.27	0.29	0.26	0.27	0.29	0.11	0.39	**0.85**

AVE: Average Variance Extracted; CR: Composite Reliability; AL: Cronbach's Alpha; COM: ISP Compliance Behavior; RUL: Rules-oriented ethical Climate; VC: Value Convergence; LG: Legitimacy; DB: Detection of Behavior; RB: Reaction to Behavior; SII: Susceptibility to Informational Influence; SNI: Susceptibility to Normative Influence; KN: ISP Knowledge

Note: The diagonal represents the square root of (AVE) values

The composite reliability (Fornell and Larcker 1981) and Cronbach's alpha scores were calculated to confirm the scale reliability and internal consistency of the constructs. Composite reliability and Cronbach's alpha values of 0.70 are recommended cutoffs (Gefen, D. Straub, et al. 2000; J C Nunnally and Bernstein 1994). As shown in Table 2.3, both values for all constructs were greater than 0.70, indicating that they all had acceptable reliability scores (Podsakoff, MacKenzie, Lee, et al. 2003).

Table 2.4. Factor Loadings And Cross-Loadings

	COM	**RUL**	**DB**	**RB**	**VC**	**LG**	**SII**	**SNI**	**KN**
COM1	**0.92**	0.58	0.32	0.42	0.35	0.66	0.26	0.19	0.22
COM2	**0.71**	0.38	0.24	0.27	0.28	0.45	0.29	0.16	0.21
COM3	**0.86**	0.49	0.31	0.43	0.27	0.57	0.27	0.22	0.24
COM4	**0.93**	0.52	0.33	0.39	0.32	0.62	0.22	0.19	0.11
COM5	**0.90**	0.52	0.32	0.39	0.33	0.63	0.24	0.17	0.14
RUL1	0.49	**0.90**	0.37	0.38	0.48	0.48	0.27	0.26	0.10
RUL2	0.53	**0.86**	0.37	0.44	0.45	0.55	0.23	0.20	0.21
RUL3	0.51	**0.90**	0.39	0.40	0.50	0.50	0.32	0.26	0.13
DB1	0.27	0.35	**0.82**	0.47	0.21	0.33	0.22	0.28	0.18
DB2	0.27	0.30	**0.86**	0.47	0.29	0.32	0.23	0.20	0.16
DB3	0.36	0.43	**0.89**	0.61	0.32	0.43	0.35	0.26	0.21
RB1	0.37	0.40	0.54	**0.94**	0.19	0.38	0.26	0.26	0.12
RB2	0.47	0.47	0.60	**0.95**	0.23	0.45	0.28	0.23	0.15
VC1	0.32	0.50	0.31	0.21	**0.92**	0.44	0.28	0.24	0.25
VC2	0.34	0.44	0.33	0.24	**0.89**	0.46	0.31	0.29	0.27
VC3	0.35	0.49	0.29	0.20	**0.93**	0.45	0.28	0.27	0.29
VC4	0.32	0.54	0.26	0.18	**0.86**	0.38	0.27	0.20	0.21
VC5	0.30	0.47	0.27	0.18	**0.94**	0.43	0.27	0.22	0.22
LG1	0.62	0.48	0.28	0.37	0.42	**0.84**	0.34	0.25	0.17
LG2	0.62	0.50	0.40	0.44	0.42	**0.84**	0.29	0.19	0.17
LG3	0.58	0.51	0.41	0.42	0.44	**0.87**	0.42	0.32	0.16
LG4	0.54	0.48	0.37	0.37	0.41	**0.87**	0.35	0.30	0.18
LG5	0.60	0.52	0.37	0.39	0.38	**0.90**	0.32	0.23	0.13
LG6	0.52	0.44	0.32	0.23	0.34	**0.77**	0.17	0.17	0.17
SII1	0.15	0.25	0.29	0.24	0.25	0.26	**0.82**	0.42	0.08
SII2	0.20	0.27	0.28	0.25	0.27	0.29	**0.85**	0.43	0.11
SII3	0.29	0.22	0.22	0.20	0.22	0.33	**0.87**	0.23	0.04
SII4	0.30	0.27	0.27	0.25	0.28	0.35	**0.85**	0.31	0.05
SII5	0.32	0.30	0.27	0.27	0.30	0.39	**0.88**	0.25	0.08
SNI1	0.18	0.19	0.21	0.23	0.25	0.24	0.34	**0.83**	0.12
SNI2	0.31	0.33	0.30	0.31	0.33	0.36	0.36	**0.86**	0.18
SNI3	0.11	0.20	0.19	0.18	0.16	0.23	0.27	**0.86**	0.06
SNI4	0.12	0.20	0.25	0.14	0.21	0.22	0.34	**0.88**	0.07
SNI5	0.19	0.21	0.26	0.23	0.18	0.17	0.34	**0.80**	0.04
KN1	0.20	0.18	0.19	0.14	0.27	0.17	0.09	0.13	**0.92**
KN2	0.18	0.12	0.20	0.11	0.23	0.17	0.06	0.07	**0.90**

COM: ISP Compliance; RUL: Rules-oriented ethical Climate; DB: Detection of Behavior; RB: Reaction to Behavior; VC: Value Convergence; LG: Legitimacy; SII: Susceptibility to Informational Influence; SNI: Susceptibility to Normative Influence; KN: ISP Knowledge

Using the repeated indicators method (Chin et al. 2003; Lohmöller 1989; Wold 1982), we estimated the second-order formative variables of command-and-control, self-regulatory, and susceptibility to interpersonal influence. First, following a molecular approximation, we constructed first-order latent constructs and related them to their corresponding items. Then, we formed the second-order by the repeated use of the manifest variables of the first-order latent constructs. The paths between the first- and the second-order construct represent the second-order loadings.

Given that multicollinearity may be a problem for measures of formative constructs (Jarvis et al. 2003). It is suggested that formative measures should not have strong correlations, as high multicollinearity can destabilize the construct, and high correlations suggest that multiple measures are tapping into the same dimension of the construct (Jarvis et al. 2003; Petter et al. 2007). In this study, none of the formative constructs suffers from multicollinearity, as all VIFs are lower than 3.3 (Diamantopoulos and Siguaw 2006; Petter et al. 2007).

The common method bias (CMV) could have affected the integrity of the results as both dependent and independent variables were gathered from the same participant. To investigate whether it is a concern, Harman's one-factor test was performed (Podsakoff et al. 2003). The exploratory factor analysis of all the measurement items found eleven factors, which explained 71.51% of the data variance. No single factor explained the majority of the variance—the factor with the largest variance explained 27.43% of the data variance. Thus, we conclude that CMV is not a major threat.

In addition, because of the nature of our study (ISP compliance), there is a possibility that social desirability bias skews the responses toward ISP compliance. Therefore, we examined the relationship between ISP compliance and a short version of the Marlowe–Crowne social desirability scale (Strahan and Gerbasi 1972). The result was significant (*b* = .11; *p* < .05). To mitigate its effect on the result, we controlled for the effect of social desirability bias in our hypothesis testing.

2.5.2. Hypothesis Testing

Figure 2.2 shows the results of the PLS estimation. We controlled for the effects of age, gender, race, tenure, ISP knowledge, company information intensity, IT-related job, type of job, company size, social desirability bias, education, and ISP knowledge. Except for education (*b* = -.15, *p* < .005) and social desirability bias (*b* = .11; *p* < .05), none of the other variables had a significant effect on ISP compliance (all *p*'s > .15). These results indicate that employees with lower education are more likely to comply with the organizational ISP.

H_1 specifies that the command-and-control approach is positively associated with employee ISP compliance. Consistent with **H_1**, the link from command-and-control to ISP compliance was positive and significant (*b* = .17, *t* = 2.42, *p* < .02). **H_2** proposes that the self-regulatory approach is positively associated with employee ISP compliance, and the result supported this hypothesis (*b* = .40, *t* = 5.07, *p* < .001).

To test the moderating effects, we created multiplicative terms by cross-multiplying the items of relevant constructs (Chin et al. 2003). We standardized the items to prevent the potential issues of multicollinearity (Aiken et al. 1991). The PLS test results indicated that rules-oriented ethical climate negatively moderated the effect of command-and-control (*b* = -.14, *t* = 2.59, *p* < .02) and that of self-regulatory approaches (*b* = -.18, *t* = 2.63, *p* < .01) on ISP compliance, thereby supporting **H_3** and **H_4**, respectively. Susceptibility to interpersonal influence was found to negatively moderate the effect of the command-and-control (*b* = -.16, *t* = 3.28, *p* < .001) and that of self-regulatory approaches (b = -.16, t = 2.47, p < .02) on ISP compliance, in support of **H$_5$** and **H$_6$**, respectively. Notably, our proposed model explained 50% of the variance in ISP compliance.

To test the importance of the moderating role of rules-oriented ethical climate and susceptibility to interpersonal influence, we estimated the significance of the difference in variance explained between one model that contains the moderating effects (i.e., the interaction model) and the other that does not have the moderating effects (i.e., the main effects model), using the following F-statistics:

$$F(df_{Interaction} - df_{main}, N - df_{Interaction} - 1) = \frac{\Delta R^2/(df_{Interaction} - df_{main})}{(1 - R^2{}_{Interaction})/(N - df_{Interaction} - 1)}$$

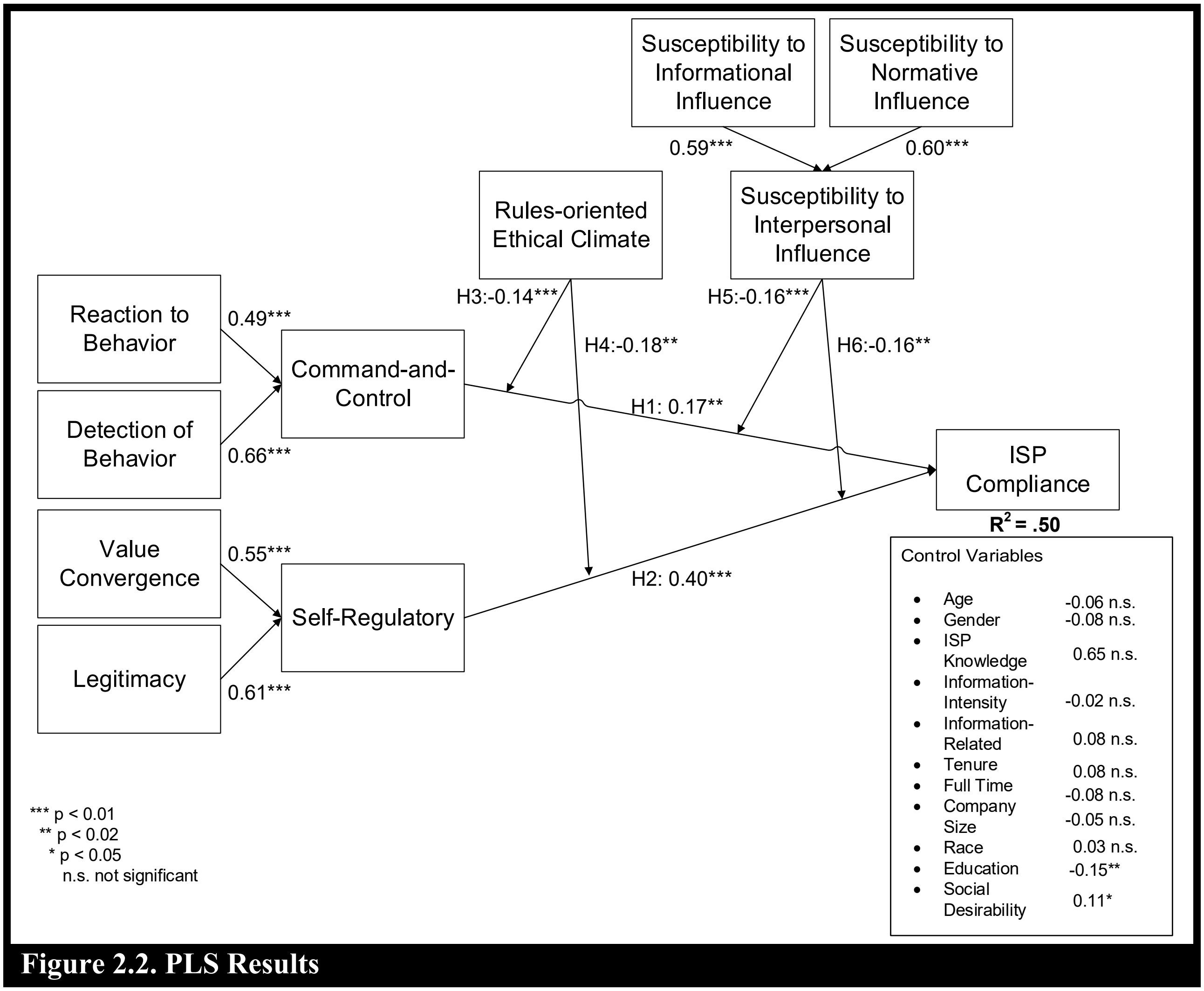


Figure 2.2. PLS Results

For the moderating effect of rules-oriented ethical climate on the relationship between the command-and-control approach and ISP compliance, the *F*-value was 7.93 (*p* < .001). For the moderating effect on the relationship between the self-regulatory approach and ISP compliance, it was 15.32 (*p* < .001). Next, for the moderating effect of susceptibility to interpersonal influence on the relationship between the command-and-control approach and ISP compliance, the *F*-value was 12.63 (*p* < .001). Finally, for the moderating effect of susceptibility to interpersonal influence on the relationship between the self-regulatory approach and ISP compliance, it was 11.57 (*p* < .001). These results provide further support for $\mathbf{H_3}$, $\mathbf{H_4}$, $\mathbf{H_5}$ and $\mathbf{H_6}$. To have a pictorial explanation of the moderating effects, we plotted two regression lines for each independent variable (command-and-control and self-regulatory) on the dependent variable (ISP compliance) when the moderating variables were low (one standard deviation below the mean) and high (one standard deviation above the mean). Figure 2.3 presents the moderating effect of rules-oriented ethical climate, and Figure 2.4 illustrates the moderating role of susceptibility to interpersonal influence. These two figures indicate the effects of command-and-control and self-regulatory approaches on ISP compliance are weaker when these two aspects of social influence are high than low.

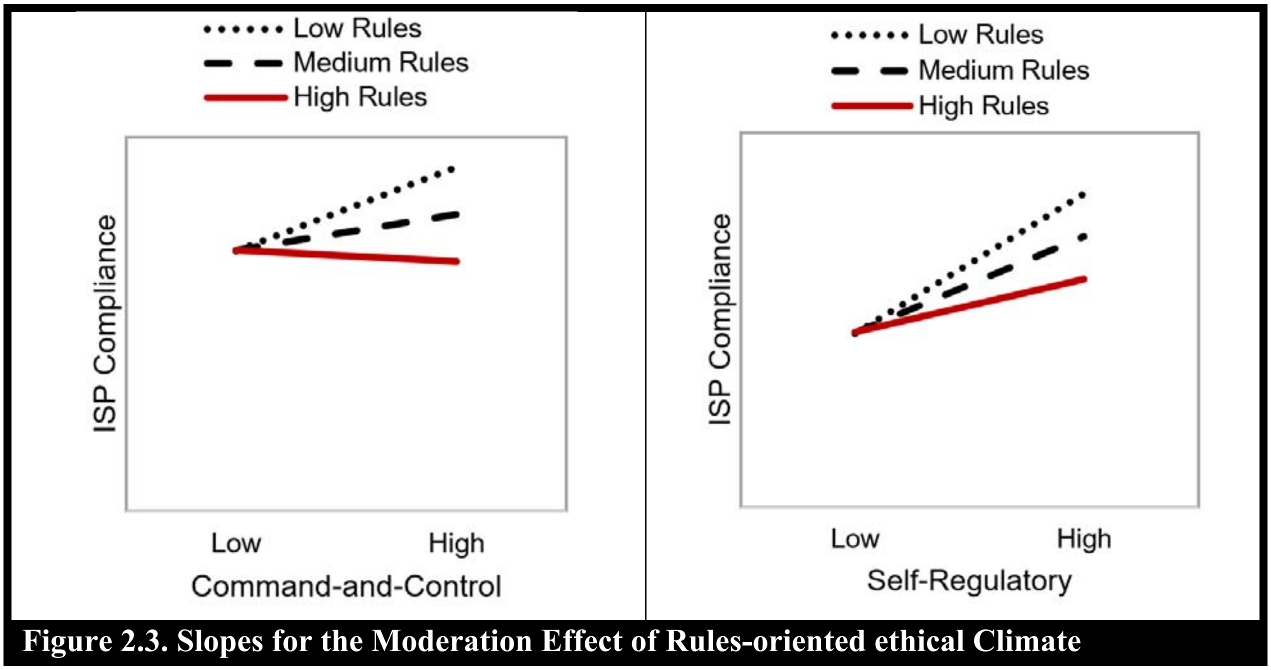


Figure 2.3. Slopes for the Moderation Effect of Rules-oriented ethical Climate

Rules: Rules-oriented ethical climate

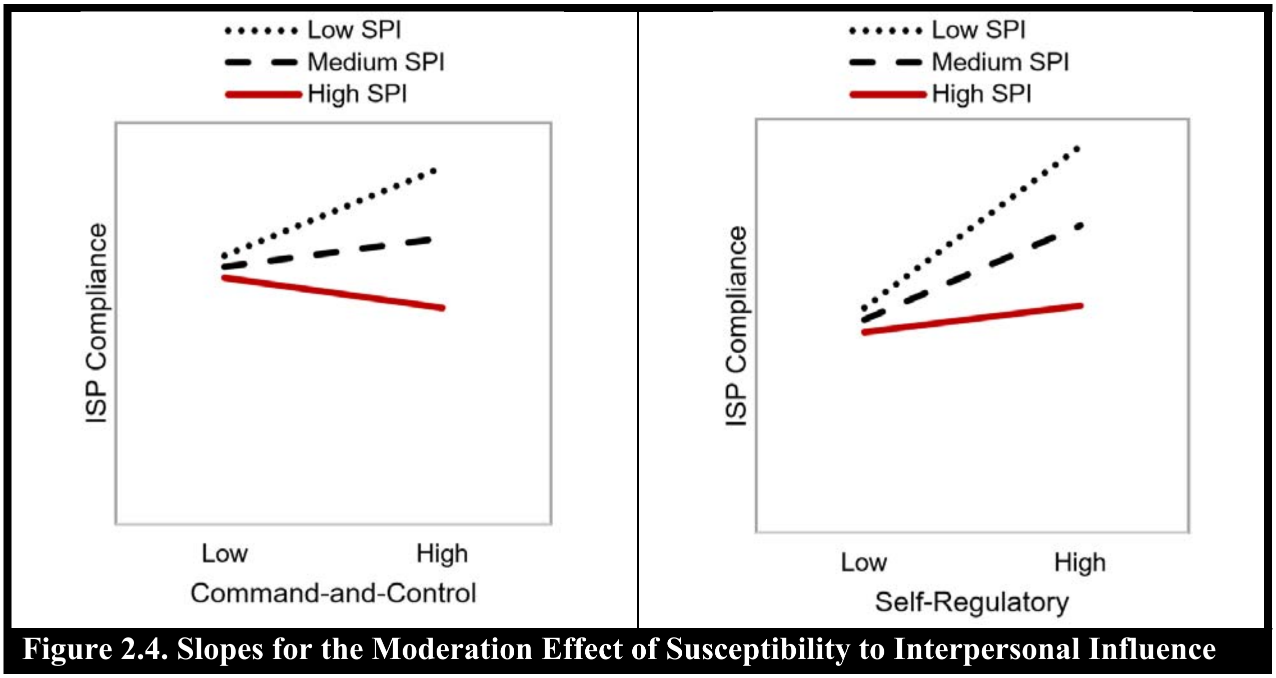


Figure 2.4. Slopes for the Moderation Effect of Susceptibility to Interpersonal Influence

SPI: Susceptibility to Interpersonal Influence

2.6. DISCUSSION

This research note aims at empirically investigating the moderating roles of rules-oriented ethical climate and susceptibility to interpersonal influence in the effects of command-and-control and self-regulation approaches on ISP compliance. Notably, our research is in line with the growing interest in the role of social psychology in understanding the motivation behind employee ISP compliance. We found that employees who perceived strong rule adherence in ethical climate at work were significantly less likely to be influenced by the command-and-control and the self-regulatory approaches. In addition, we found that employee susceptibility to interpersonal influence reduced the effectiveness of both approaches as well.

2.6.1. Contributions to Theory

This research note contributes to information security research in several ways. First, by including two important aspects of social influence as contingent factors in the model, the study advances the understanding of the well-established effects of command-and-control and self-regulatory approaches on ISP compliance. A common strategy used by an organization to enforce ISP compliance relies on the deterrence effect of sanctions. But recent literature suggests mixed findings in terms of its effectiveness (see the reviews by Sommestad et al. 2014 and D'Arcy and Herath 2011). While some studies (Straub and Nance 1990) show that deterrence effectively promotes ISP compliance, other studies report that deterrence does not have effect on ISP compliance (Guo and Yuan 2012; Herath and Rao 2009a; Hu et al. 2011; Han Li et al. 2010; Pahnila et al. 2007; Siponen and Vance 2010; Son 2011; Vance and Siponen 2012). By taking social influence factors into account, our study intends to shed light on the contingency factors that may affect the effectiveness of deterrence, and therefore help reconcile these mixed findings in the literature.

Additionally, along with the command-and-control approaches, researchers and practitioners strive to educate employees with the hope that employees consider ISP to be legitimate and internalize these rules into their own value system. These strategies fall under the self-regulatory approach. While research interest in such approaches is growing (Ifinedo 2014; Li et al. 2014; Myyry et al. 2009; Vance and Siponen 2010), previous studies have not yet considered the effect of social influence on the effectiveness of self-regulatory approaches in motivating ISP compliance. Our study is among the first to provide a framework to examine such effects.

Finally, the information security literature often conceptualizes social influence as opinions of important others (Dugo and Marshall 2007; Guo et al. 2011; Herath and Rao 2009a; Ifinedo 2012) and normative beliefs (Bulgurcu et al. 2010; Herath and Rao 2009b; Pahnila et al. 2007; Siponen et al. 2010). Extending this stream of research, our study enriches the concept by including both rules-oriented ethical climate and individuals' susceptibility to interpersonal influence. As a result, it provides a novel perspective through investigating the effects of social influence at both macro- and micro- levels in the same model. Such a conceptualization and operationalization of social influence provides a foundation for future research looking into the role of social influence in information security compliance.

2.6.2. Implications for Practice

Successful security management without considering situational and individual characteristics is not achievable. Apart from its theoretical contributions, this research note also has several implications for information security practices in organizations. First, our findings suggest that a rules-oriented ethical climate sets up a boundary for the effect of command-and-control and that of self-regulatory on ISP compliance. Based on these insights, organizations should focus on preparing or strengthening a rules-oriented ethical environment as a strategy to avoid the drawbacks associated with the rule-following approaches. To build a stronger ethical climate, managers shall clarify ethical issues and reduce ethical ambiguities (Grojean et al. 2004). In addition, organizations can design campaigns to remind the employees that "successful employees follow the rules" or "adhering to the rules is the expectation".

Organizations may also integrate ethical issues into their career development curriculum and training programs (Baker 1997; Goldstein 1993; Grojean et al. 2004). Furthermore, security managers may also implement programs that aim at using such external stimuli as oral feedback and awareness campaigns to communicate the importance of information security policies to employees and the value the organization places on them.

Our results indicate that susceptibility to interpersonal influence has a powerful impact on the effectiveness of command-and-control and self-regulatory approaches on ISP compliance. As an individual's susceptibility to interpersonal influence is hard to change, organizations could measure such tendencies and use the data to decide employee placement. For instance, employees who are susceptible to interpersonal influences often observe their peers' ISP decisions when they are deciding on ISP-related issues. These employees may be more sensitive to professional opinions and recommendations regarding the best ISP-related practices. Because these employees may find the social aspect of ISP compliance specifically important, an effective strategy is to provide them the possibility of interacting with those who have the highest level of ISP compliance.

2.6.3. Limitations and Future Research

Our study has some limitations that deserve consideration. The first is rooted in its cross-sectional design, which provides the least support for the causal directions proposed in our model. The proposed causality is based on theory and the empirical findings documented in previous research. Furthermore, it may be compelling to investigate the stability of social influence and whether or not a change in it over time influences ISP compliance more. Future research may utilize a longitudinal design to test such ideas. Another limitation is that our constructs are measured based on employee perception. Future research could use objective data to capture the intensity of employee interactions. Specifically, it may be fruitful for future researchers to look separately into employees' interaction with their supervisors and with their teammates.

Chapter Three:

Can Peers Help You Comply with Information Security Policies?

3.1. INTRODUCTION

Peer monitoring—is an informal type of organizational control in which employees who have no formal authority over each other observe their peers' behaviors, recognize when others make a mistake or break the rules, and respond by correcting and reporting the wrongdoers (Dickenson and Mclntyre 1997; Jong et al. 2010; Loughry and Tosi 2008; Marks 2001; Marks and Panzer 2004). Peer monitoring has been proven effective in enhancing employees' performance (Langfrevd 2004; Marks and Panzer 2004). As a whole, this study advances a theory that frames the effect of peer monitoring on ISP compliance.

The first objective of this study is to adapt a peer monitoring approach into the context of information security and investigate its immediate as well as indirect impact on motivating employees to comply with the ISP. When employees do not comply, it is often without the intention to harm the organization or its information assets. These cases are often linked to a lack of adequate training, weak commitment, carelessness, and lack of motivation (Willison and Warkentin 2013). Examples include failing to change a password, to encrypt the sensitive data, or to log off a computer before leaving it (Willison and Warkentin 2013). This study advances the hypothesis that peer monitoring can address the above-mentioned factors associated with employee ISP noncompliance. As it is implied, peer monitoring at a higher level consists of noticing (peer observing) and responding (peer reporting and correcting mechanisms) to peers' actions (Loughry and Tosi 2008). Peer observing refers to group members observing each other to look for any wrongdoing (i.e., ISP noncompliance); peer reporting refers to group members reporting their peers' wrongdoings to higher authorities (i.e., management), while peer correcting refers to group members correcting their peers' wrongdoings (Loughry and Tosi 2008).

Peer monitoring can encourage ISP compliance because it helps organizations convey the message that they have access to more (detailed) information about their employees' behaviors. By increasing the chance of detection as well as frequency of punishment (i.e., perceived deterrence), it discourages ISP noncompliance. This is consistent with previous studies, which have found that peer monitoring mechanisms reduce other undesirable behaviors, including employee theft, social loafing, escalation of commitment and self-interested behavior (Chen and Sandino 2007; Harkins and Petty 1982; Kirby and Davis 1998). Moreover, peer monitoring allows employees to receive guidance on ISP compliance as well as identify opportunities to rectify their mistakes. This leads to a positive preference and attitude toward ISP compliance (i.e., commitment to the ISP) and consequently improves employee ISP compliance. Furthermore, guidance and assistance through peer monitoring may indirectly train employees on accepted ISP behaviors and thus address the lack of proper training. It can also increase information security awareness, which would improve overall ISP compliance. This is crucial as more than one-third of security breaches result from users' careless and ignorant, inadvertent actions (Shey 2016). Consistently, previous studies have indicated that peer monitoring is a capable mechanism to motivate employees to make up for their low performance (Lepine and Dyne 2001) or to conform to group expectations (Sewell 1998), thereby leading to higher group coordination and performance (Langfred 2004; Marks and Panzer 2004).

In brief, assuming that peer monitoring may (1) highlight the importance of ISP compliance for the group and consequently exert psychological pressure on group members to comply with the ISP, (2) enhance the probability of getting caught for ISP noncompliance, and (3) increase the perception that group members are cared for, we set out to test the argument that peer monitoring both directly and indirectly—through increasing commitment to the ISP and perceived deterrence—promotes ISP compliance.

The second objective of this study is to investigate the factors (beside organizational policies) that promote peer monitoring in organizations. In particular, this study investigates the social context that leads group members to engage in (or perceive) peer monitoring. This is important as when not motivated by organizational policies, peer monitoring is a voluntary action—extra-role or organizational prosocial behavior, which can be prompted by social context (i.e., group norms) as opposed to organizational policies (Olson and Maio 2003; Trevino and Victor 1992). It is suggested that social contexts that aligns individual group members' interests and group's interests by holding individual group members responsible for others promote peer monitoring (Trevino and Victor 1992). This study introduces collective responsibility (Lickel et al. 2003) as a group norm that creates a reward structure aligning individual group members' interests with their group interests and thus promotes peer monitoring as an expected (prosocial) behavior (Trevino and Victor 1992).

Collective responsibility, in this context, refers to a group norm in which individual group members are convinced that they may be held responsible for any member's ISP noncompliance (Denson et al. 2006; Lickel et al. 2003; May 1987). It is based on the notion that employees' perception of peer monitoring can emerge from collective sense-making (Weick 1995)—the process by which individuals give meaning to their joint experiences in the group. This study further argues that collective responsibility arises because individual group members may conclude that (1) other members could have prevented ISP noncompliance (i.e., responsibility by omission), or (2) other members have indirectly contributed to ISP noncompliance (i.e., responsibility by commission). In groups that have a sense of collective responsibility, it is expected that members conduct peer monitoring to avoid punishment, as they may be accused of overlooking or encouraging ISP noncompliance. Thus, this study contends that collective responsibility encourages individual group members to conduct peer monitoring. And collective responsibility itself is the product of responsibility by omission and responsibility by commission.

In short, by building upon organizational agency theory, prosocial organizational behavior, and management literature, this study investigates the following propositions: (1) perception of peer monitoring in a group increases employee ISP compliance, (2) this effect is mediated by commitment to the ISP as well as perception of deterrence for ISP noncompliance, (3) the perception of collective responsibility in a group arises from the perception of responsibility by omission and responsibility by commission, and finally, (4) collective responsibility can lead to peer monitoring. We tested the proposed research model using data collected through Qualtrics panel, which comprises 891 valid responses from working professionals. The results indicate the validity of the aforementioned propositions.

This study makes four contributions to the literature. One, it is the first to investigate peer monitoring, its antecedent, and its mechanisms in the context of information security. Two, it adds to general deterrence theory by introducing an effective, informal detection mechanism. This is novel as previous studies using general deterrence theory have consistently ignored such a component. Furthermore, it brings a new, tailored concept of affective commitment to the ISP (as a specific type of organizational commitment) to the context of information security. This can enrich understanding of the concept as previous literature have taken more holistic views by investigating the effect of affective organizational commitment on employee ISP compliance (c.f., Posey et al. 2015). Finally, by examining collective responsibility, it introduces a novel way of capturing the social context (reward structure) that aligns the interests of the group with those of its members. This is important as previous studies have emphasized the positive impact of such a social structure in motivating peer monitoring but not empirically (via measurement items) operationalized it (c.f., Trevino and Victor 1992).

This paper is organized as follows: first, section 2 establishes the theoretical background. Section 3 then develops the hypotheses, section 4 presents the research methodology and results, and section 5 outline the data analysis. Finally, section 6 discusses the potential theoretical contributions, practical implications, limitations, and future possible studies.

3.2. THEORETICAL BACKGROUND

3.2.1. Peer Monitoring

Peer monitoring is a lateral control mechanism that occurs when employees observe their fellow coworkers' behavior and directly react if they conclude the observed behavior is inappropriate (Loughry and Tosi 2008; Welbourne et al. 1995; Welbourne and Ferrante 2008). In the context of this study, it occurs when employees observe their peers' ISP noncompliance and react by correcting their behavior according to the ISP or reporting them to a supervisor or management. Therefore, peer monitoring consists of three distinct behaviors (dimensions), namely peer observing, peer correcting, and peer reporting (Loughry and Tosi 2008) wherein peer monitoring may seem incomplete without each component. In other words, observing ISP noncompliance without responding to it (i.e., reporting or correcting) may be insignificant. Similarly, responding to ISP noncompliance before observing such a behavior may not be realistic. Theoretically, peer monitoring can be conceptualized as a second-order construct consisting of a diverse set of observable phenomena bringing together its disparate actionable facets (Barki et al. 2007; Cenfetelli and Bassellier 2009; Chin and Gopal 1995; Gefen et al. 2000; Mathieson et al. 2001), suggesting a formative nature of peer monitoring (Bagozzi 2011; Podsakoff, MacKenzie, Podsakoff, et al. 2003). Two key perspectives, agency theory and organizational prosocial behavior, can explain the effect of peer monitoring on employee behavior (i.e., ISP compliance).

3.2.1.1 Agency Theory

From the agency theory perspective, peer monitoring can address agency problems of adverse selection (when agents misrepresent their abilities) and moral hazard (when agents act against a principal) by providing the principal better information about agent's abilities and behavior (Arnott and Stiglitz 1991). In this view, peer monitoring is a preferable control method compared to other methods because (1) it is less costly—as employees themselves perform the peer monitoring while doing their work as opposed to approaches that rely on other sources to perform the control function (Fama and Jensen 1983); (2) it captures a broad range of information regarding employee behavior, which is typically difficult for other methods to obtain (Fischer and Hughes 1997). Therefore, from an agency theory perspective, peer monitoring is an efficient control approach (Loughry 2010). Furthermore, according to agency theory, the perception of peer monitoring would enforce acting in line with the group's interest, i.e., discourage poor decisions (Kirby and Davis 1998). Because employees typically understand their peers' tasks and observe their behavior in real time when required, they are the best ones to offer guidance and correction (Fama and Jensen 1983; Holmström 1982; Loughry and Tosi 2008).

3.2.1.2 Prosocial Organizational Behaviors

Acknowledging that organizational policies can promote peer monitoring, this study argues that it can be viewed through the lens of prosocial organizational behavior as a voluntary or extra-role behavior—discretionary behavior not formally requested by the organization (Dozier and Miceli 1985; Dworkin and Baucus 1998; Miceli and Near 1985; Organ 1990; Trevino and Weaver 2001). This framework can help explain the processes and motives (other than organizational policies) behind peer monitoring. Prosocial organizational behaviors refer to actions that benefit other members or the entire organization, such as keeping organizational information assets safe (Brief and Motowidlo 1986; Staw 1984). Often going beyond what is required for the specific role (Brief and Motowidlo 1986; Dornyei 1989), they require spending extra personal time and effort (Brief and Motowidlo 1986; O'Reilly III and Chatman 1986). Five categories have been identified: (1) cooperating with and helping others, (2) protecting the organization, (3) volunteering productive views, (4) self-training, and (5) keeping a positive attitude toward the organization (Barnard 1938; Katz 1964; Seifert 2006).

The peer correcting dimension of peer monitoring can be classified under helping coworkers with job-related matters (Brief and Motowidlo 1986; Smith et al. 1983), i.e., an individual strives to correct ISP noncompliance in another individual. On the other hand, peer observation and reporting can both be classified under protecting the organization (i.e., civic virtue) wherein an employee seeks to protect organizational information assets and the organization and its members by observing and reporting ISP noncompliance to management (Dozier and Miceli 1985; Podsakoff 2000; Smith et al. 1983).

Prosocial organizational behaviors are either functional or dysfunctional. For instance, an employee might help coworkers to do their job more efficiently (i.e., functional) or help them attain personal goals that do conflict with organizational interests (i.e., dysfunctional). In this study, peer monitoring is functional as employees reporting or correcting ISP noncompliance is in line with organizational interests as opposed to going against them (Loughry and Tosi 2008).

3.2.1.3 General Deterrence Theory

Traditional general deterrence theory (GDT) emphasizes formal sanctions and postulates that individuals abstain from committing a crime if they perceive the punishment to be certain, severe, and swift (Gibbs 1975). GDT assumes that individuals are rational, self-interested actors whose behavior is based on the minimization of costs and the maximization of benefits (Becker 1968). Thus, theoretically, one would expect that if a high risk and punishment is associated with committing a crime—the costs of committing it outweigh the benefits—individuals would abstain from the criminal act (Gibbs 1975; Nagin and Pogarsky 2001; Straub 1990; Tittle 1980).

Extending the GDT, Piquero and Tibbetts (1996) additionally incorporated informal sanctions. As such, more recent versions of GDT assumes that individuals consider perceived risks and the costs of both formal and informal sanctions (Pratt et al. 2006). Certainty of detection and severity of punishment are distinct dimensions of GDT (Geerken and Gove 1975; Gibbs 1975). Without both, deterrence is not inclusive—detecting a crime without punishing it defeats the purpose, while punishing a crime that has not been detected is impossible (Geerken and Gove 1975). This suggests that perceived deterrence is a formative construct consisting of perceived certainty of detection and severity of punishment (Bagozzi 2011; Podsakoff, MacKenzie, Podsakoff, et al. 2003).

Monitoring systems have been shown to significantly increase the perception of risk associated with committing an illegal act (e.g., tax evasion) (Alm and McKee 2006; Kinsey 1992; Wenzel 2004). In addition, several studies have demonstrated a positive link between the former systems and perception of punishment severity (Dubin et al. 1990; Grant and Patil 2012; Kinsey 1992). In the context of information security, monitoring of IS misuse (e.g., ISP noncompliance) has been shown to reduce such behaviors (D'Arcy et al. 2009; Parker 1998; Straub and Welke 1998). In particular, D'Arcy et al. (2009) argued that monitoring employees' computer-related activities is a proactive security action that enhances an organization's ability to detect employee ISP noncompliance. Organizations with robust monitoring mechanisms create the perception that the certainty of getting caught and frequency of punishments are high (D'Arcy et al. 2009). In addition, exposing those who have been caught and punished can bolster the effectiveness of monitoring systems in increasing the perception of not only certainty of detection but also severity of punishment (D'Arcy et al. 2009). Finally, having monitoring systems in place signals the importance of ISP compliance as it means resources are being dedicated to them (D'Arcy et al. 2009). Similarly, it is theoretically plausible that peer monitoring would signal the importance of ISP compliance as employees would spend extra time and effort to make sure every member complies.

3.2.1.4. Commitment to the ISP

Commitment, broadly, refers to a mindset that binds an individual to seek for achieving a specific target (Herscovitch and Meyer 2002; Meyer and Herscovitch 2001). More specifically, organizational commitment is an individual's dedication to act in a way that fulfills organizational interests. In the organizational context, the primary outcome of interest of commitment (i.e., organizational commitment) is retention (Mathieu and Zajac 1990), while other outcomes such as job performance is secondary (Herscovitch and Meyer 2002). When considering commitment to various targets such as goals and policies, retention is not the main outcome of interest (as in organizational commitment) (Herscovitch and Meyer 2002). In other words, when outcomes such as ISP compliance is a primary outcome of interest, retention and thus organizational commitment is not generally relevant. Thus, a more tailored conceptualization of organizational commitment to the ISP is more appropriate.

This study argues that a mindset that binds employees to actions regarded as crucial to the success of the ISP can prompt ISP compliance. Given that, similar to Herscovitch and Meyer (2002), it defines affective commitment to the ISP as a mindset that binds employees to a course of action (i.e., compliance) that is required for the success of the ISP. It is theoretically plausible that affective commitment to the ISP can induce ISP compliance as those who believe in the value ISP bring to the organization are likelier to support and thereby comply with it.

Employees in groups with high peer monitoring, an informal control system, may experience peer influence that encourages them to seek goals consistent with the group interests as a result of the desire for their peers to accept them (Stewart et al. 2012). There is also a shared understanding on what constitutes accepted behavior (Loughry 2010; Ouchi 1979). Thus, informal control systems cause members to practice more individual discretion, which means greater commitment (Cravens et al. 2004; Loughry 2010; McGrath 2001; Thompson 1967). In addition, peer monitoring can imply members hold each other in high regard. In such a case, members would likely be more committed to following group-desired behaviors. Social exchange theory (Blau 1964) contends that members with positive attitudes toward the group may behave in a way that benefits the group (Parboteeah et al. 2010).

In general, organizations with higher level of employee commitment benefit from high levels of task completion and performance (Randall, 1987). In particular, such employees often demonstrate compliance with the organization’s rules and decisions (Kim and Mauborgne 1993; O’Reilly III and Chatman 1986). Accordingly, in the context of information security, one can expect that peer monitoring can boost weak affective commitment, which has been identified as one of the main reasons for ISP noncompliance (Willison and Warkentin 2013). Previous studies have confirmed the positive effect of affective organizational commitment on employees’ information security behavior, specifically on employee ISP compliance (Herath and Rao 2009a; Oz 2001; Posey et al. 2015; Stanton et al. 2003). Those with higher affective commitment are more likely to feel that organizational cherished values are similar to theirs, inducing those to act towards organization goals (Meyer et al. 2004; Posey et al. 2015). The reason behind such a relationship is that employees who have such a commitment may feel emotionally attached to their organization or they may emotionally identify with their organization, and as a result have a higher tendency to act in support of their organization decisions and interests (Meyer and Alien 1984; O'Reilly III and Chatman 1986; Posey et al. 2015).

3.2.2. Collective Responsibility

Collective responsibility refers to a concept wherein individual group members are held responsible for another member's misconduct whether they took part or not, because of their social association (e.g., group membership, coworkers) (Hamilton 1978; Lickel et al. 2003; Sanders et al. 1996). In an organizational context, social association is in the form of task groups (i.e. coworkers) (Denson et al. 2006; Lickel 2000; Lickel et al. 2003). The way group members think of ISP noncompliance may affect their perception of collective responsibility. Perception of collective responsibility can be generated when an individual believes other members might indirectly contribute, encourage, or facilitate the blameworthy behavior or when group members fail to prevent this behavior (May 1987). A group member may conclude to be held responsible for the blameworthy behavior conducted by peers if he or she believes that, first, other members perceive that in some capacity he or she indirectly encouraged or helped the condition for such action; Second, if other members perceive that he or she could have prevented the blameworthy actions (e.g., ignoring an instance of ISP noncompliance). The former is called responsibility by commission, while the latter is called responsibility by omissions (Lickel et al. 2003).

An organization may formally implement peer monitoring through its policies. However, employees may not be receptive to such an appeal and thereby ignore the policies (Ferrin et al. 2007). In the same line, previous studies have suggested the creation of a pro-peer monitoring social context—group norms that influences individuals to act prosocially to avoid social sanctions

(Olson and Maio 2003)— as an alternative approach to formal requests (Trevino and Victor 1992). The social context refers to a set of norms and expectations as well as rewards and punishments (reward structure) that influence group members' attitudes and behaviors (Trevino and Victor 1992). Trevino and Victor (1992) have suggested two conditions to promote peer monitoring: (1) the perception that member misconduct threatens the interest of other members, and (2) the perception that other members are also held responsible for member misconduct. This study advances the argument that collective responsibility by structuring a reward system that implies benefiting the group is in individual group members' interests can capture both suggested aspects of social context required for peer monitoring.

Collective responsibility can be considered a form of an organizational prosocial norm[2] as it emphasizes benefiting the group, or collectivism (Olson and Maio 2003). However, a subtle form of egoism (i.e., self-interest) can be traced in collective responsibility and generally in norms such as collectivism. It can be argued that ignoring the needs of the group results in putting the individuals' self-interests at risk in the long run. Thereby, one may opt to benefit the group to maximize his or her own interests (Olson and Maio 2003). Similarly, politicians and social activist often trying to motivate individuals to act prosocially by appealing to their self-interest. For example, they motivate people to adopt environmentally friendly behaviors (e.g., taking public transportation to reduce fuel use) by warning them that their actions may have a negative effect (e.g., global warming and air pollution) on both themselves and their children.

[2] It should be noted that peer monitoring cannot be considered an altruistic behavior. While prosocial organizational behaviors are intended to benefit others, those who behave thusly might do so to benefit themselves. On the contrary, altruistic behaviors requires self-sacrifice and solely benefits someone else (Staub 1978).

In short, peer monitoring can function as a way to avoid the blame in case of ISP noncompliance. Although the motivation may be selfish, it could also be viewed as a prosocial behavior because it benefits the group and its members. Reporting and correcting ISP noncompliance contributes to organizational information security in the long run. In addition, considering that peer monitoring requires extra time and effort, it is not without self-sacrifice (O'Reilly III and Chatman 1986). Finally, this study argues that collective responsibility is an appropriate motive for peer monitoring.

3.3. HYPOTHESIS DEVELOPMENT

3.3.1. Peer monitoring

In the context of this study, peer monitoring is defined as the degree to which an employee perceives group members observing each other for ISP compliance and reporting or correcting those who do not follow the ISP. Peer monitoring can act as an implicit coordination mechanism. It creates an opportunity in which employees provide task-relevant information to their peers (without their request), proactively helps them, keeps track of their activities, and finally encourages them to meet the group expectations (Rico et al. 2008). Therefore, peer monitoring may increase awareness of ISP compliance among group members and consequently directs their attention to such behaviors (Bowen and Ostroff 2004). As a result, it reduces the possible ambiguities regarding the ISP compliance and thus helps members develop a clear common interpretation of appropriate ISP compliance (Bowen and Ostroff 2004; Callister et al. 1999; Cooper and Withey 2009; De Jong et al. 2014). In addition, it exerts psychological pressure on members to adopt group expected behaviors, thereby creating behavioral coordination among the members (Cooper and Withey 2009; De Jong et al. 2014; Meyer et al. 2010). Finally, it may help individual change their behavior in relation to ISP compliance. In fact, research has shown that those who receive constructive feedback about their decisions through monitoring are more willing to change their behavior, whereas those who have not been monitored are more likely to follow their initial decision even when evidence suggest them otherwise (Kirby and Davis 1998). In terms of information security, it can be argued that peer monitoring by expressing the importance of ISP compliance encourages ISP compliance. Accordingly, we hypothesize

H$_1$: *Perceived peer monitoring is positively associated with employee ISP compliance.*

3.3.2. Perceived Deterrence

Perceived deterrence is refers to the perception that the chance of getting caught for ISP noncompliance is high and would result in serious punishments that outweigh the benefits of noncompliance (Geerken and Gove 1975). Though peer monitoring, employees may pass on any information about ISP violations to the designated authorities. Thus, it can decrease ISP noncompliance though different mechanisms. First, it emphasizes negative consequences for any misconduct (Meyer et al. 2010) as well as a higher frequency of punishment from management. In this sense, it increases the perception of punishment through informal sanctions (i.e., peer pressure) and thus motivates employees to act appropriately (i.e., complying with the ISP) (Hollinger and Clark 1983). Second, it creates the threat of becoming observed and report for ISP noncompliance. As such, it increases the perception of a higher probability of getting caught through an informal mechanism (Greenberger et al. 1987; Victor, B., Trevino, L.K. and Shapiro 1993).

H$_{2a}$: *Perceived peer monitoring is positively associated with perceived deterrence.*

Individuals are rational and self-interested actors who may not comply with the ISP if the cost of not following compare to following the ISP is minimized (Becker 1968). Higher perceived deterrence signals that high risk and punishment are associated with ISP noncompliance and thereby encourage compliance. In other word, in an environment with high perceived deterrence costs of ISP noncompliance may outweigh its benefits, and thus encourage employees to refrain from not complying with the ISP (Straub 1990). Accordingly, it is expected that higher perceived deterrence persuades employees that ISP compliance is in their best interests.

H_{2b}: *Perceived deterrence is positively associated with employee ISP compliance.*

Previous literature in information security has confirmed that organizational formal monitoring systems induce ISP compliance by increasing the perception of risk and punishment (D'Arcy et al. 2009). This study advances an argument that such a relationship can also be theoretically extended to peer monitoring as an informal monitoring mechanism. We argue that peer monitoring motivates group members to comply with the ISP by conveying the message that those who do not comply will be detected and sanctioned through both formal and informal channels. Accordingly, we hypothesize that:

H_2: *The effect of peer monitoring on ISP compliance is mediated through perceived deterrence.*

3.3.3. Commitment to the ISP

Peer monitoring can induce members to feel more commitment to group goals, such as ISP compliance. In showing they are willing to spend the extra time and effort to perform peer monitoring, they emphasize the importance of ISP compliance as well as group expectations of the former. In addition, peer monitoring by navigating employees to the right direction regarding the ISP compliance creates an accountability among members for ISP compliance. Furthermore, peer monitoring prevents undesired behaviors and thereby punishment (Loughry 2010). Finally, information sharing and constructive error correction may lead to higher closeness among group members (Collins and Miller 1994). In this way, peer monitoring helps conveys the notion that members care for each other, which leads to stronger feelings of dedication, responsibility, and affinity to group goals (Herscovitch and Meyer 2002; Meyer and Alien 1984; Norris-Watts and Levy 2004; O'Reilly III and Chatman 1986).

H$_{3a}$: *Perceived peer monitoring is positively associated with commitment to the ISP.*

Commitment to the ISP encourages ISP compliance. This is because when peer monitoring perceived by individual group members as an act towards the interests of the group and its members, it may lead them to conclude that it should be reciprocated (Blau 1964; Leung 2008; Osterman 2000). Such a reciprocation can be shown as acting in line with group interests such ISP compliance. Information security literature has confirmed the positive effect of organizational commitment on ISP compliance (c.f., Posey et al. 2015; Stanton et al. 2003). Similarly, this study argues that commitment to the ISP—as a more specific type of organizational commitment that refers to an individual's dedication to ISP compliance for ISP success—motivates ISP compliance.

H$_{3b}$: *Commitment to the ISP is positively associated with employee ISP compliance.*

Altogether, this study argues that peer monitoring, in leading to correcting group members correcting each other's ISP noncompliance, enhances the perception that they care for each other. This in turn would encourage them to promote group interests through ISP compliance. Accordingly, we hypothesize that:

H$_3$: *The effect of peer monitoring on ISP compliance is mediated through individual commitment to ISP.*

3.3.4. Collective responsibility

If ISP noncompliance is not important to the group members—neither hurts or benefits them, it may not be in their interest to respond to it (Miceli and Near 1984; Trevino and Victor 1992). Thus, we propose that a group social context structured by some kind of reward (or punishment) system makes members more likely to perform peer monitoring (McCallum et al.

1985; Trevino and Victor 1992). One example is aligning the interests of individual group members with those the group (Kandel and Lazear 1992; Welbourne et al. 1995).

Extending this to the context of information security, this study introduces collective responsibility as a group structure (a norm of collectivism) that implies members who have no apparent, direct, causal involvement with the ISP noncompliance are held responsible by association. In this way, a norm of collective responsibility would lead to group members being more likely to engage in peer monitoring to ensure no one commits an error; otherwise, everyone becomes responsible. Moreover, it structures a punishment system in addition to eliminating any excuses for not engaging in peer monitoring. Thus, members with a perception of high collective responsibility would conclude that every group member has a responsibility to monitor ISP compliance to protect the group. Accordingly, we hypothesize:

H$_4$: *Collective responsibility is positively associated with peer monitoring.*

3.4.5. Responsibility by omission and responsibility by commission

Establishing collective responsibility can be critical for organizations interested in benefiting from peer monitoring. This study proposes two ways in which individual group members might conclude they may be blamed or held responsible for others' ISP noncompliance (i.e., collective responsibility): One, other members could have prevented ISP noncompliance, and two, other members indirectly encouraged or contributed to it (Lickel 2000). The former is responsibility by omission, whereas the latter is responsibility by commission (Lickel 2000). Either makes individual group members believe they may be accused of being negligent or benefiting from others' ISP noncompliance and thus also be held accountable. Accordingly, we hypothesize that:

H$_5$: *Responsibility by omission is positively associated with collective responsibility.*

H$_6$: *Responsibility by commission is positively associated with collective responsibility.*

Figure 3.1 summarizes these hypotheses and presents the proposed model of peer monitoring.

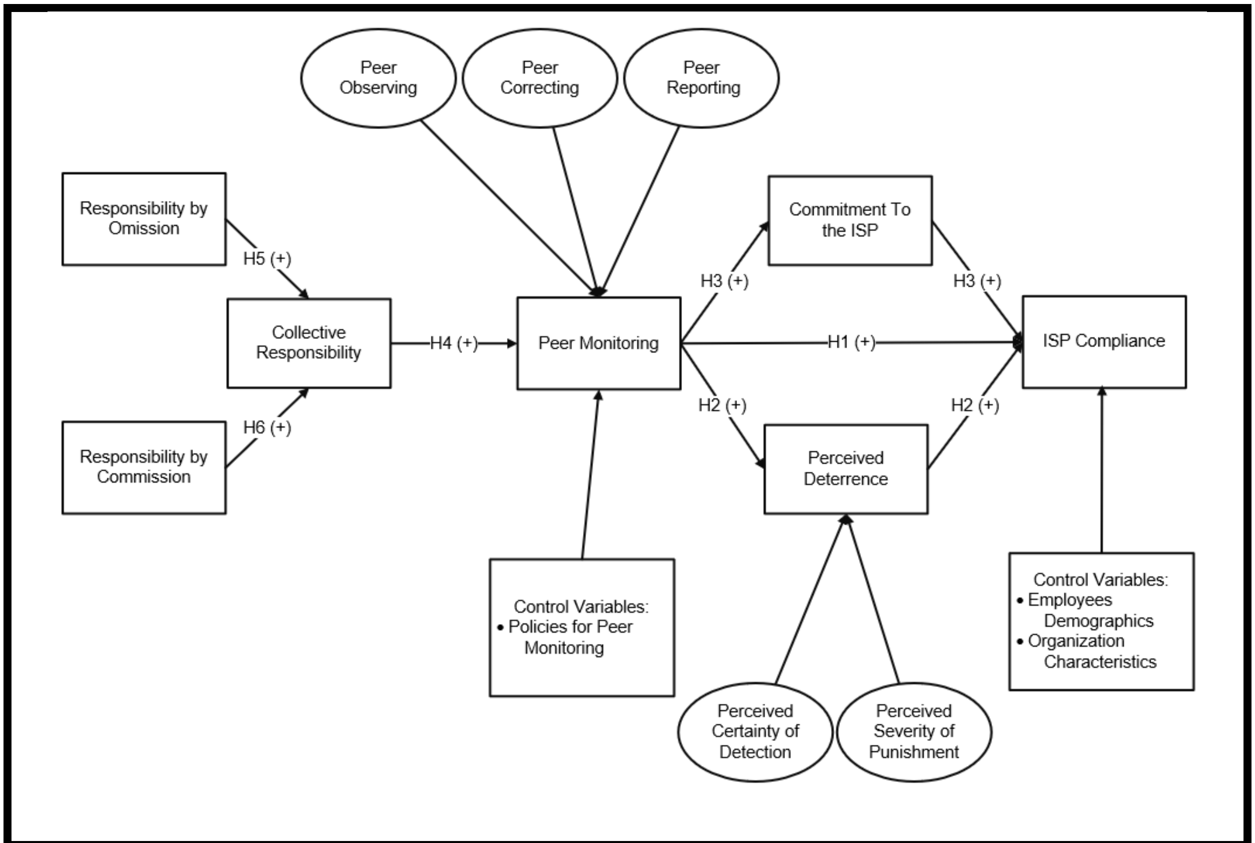


Figure 3.1. Research Model

3.4. RESEARCH METHODOLOGY AND RESULTS

3.4.1. Data Collection

To ensure the external validity of our results, we conducted a survey with participants recruited from Qualtrics panel of U.S. employees. To confirm that we targeted the right respondents, screening questions were put up front, asking participants whether they are holding a full-time job. For those who had a full-time job, we then provided the definition of information security policy with illustrative examples. We then filtered those participants whose organization did not have an ISP in place, or whose job did not require ISP compliance. Finally, we asked participants whether they work in a group such as a team, department, or work unit. We filtered those whose job did not require them to work in a group. A total of 891 valid responses were collected (refer to Table 3.1 for the summary of the sample demographics).

Table 3.1. Summary of Sample Demographics N=-891

Variable	Content	#	%	Variable	Content	#	%
Gender	Male	267	30.0	Ethnicity	White/Caucasian	740	83.1
	Female	624	70.0		African American	35	3.9
Education	Some or Less Than High School	0	0.0		Hispanic	38	4.3
	High School Graduate	43	4.8		Asian	64	7.2
	Some College	176	19.8		Native American	3	0.3
	College Graduate	435	48.8		Other	11	1.2
	Post-Graduate Education	237	26.6	Age	18-25	81	9.1
Group Size	less than 5 employees	181	20.3		26-35	288	32.3
	5-10 employees	337	37.8		36-45	222	24.9
	10-15 employees	119	13.4		46-55	179	20.1
	15-25 employees	101	11.3		56-65	116	13.0
	25+ employees	153	17.2		66-75	5	0.6
Position	Upper Management	25	2.8	Organization Size	Fewer than 500 employees	147	16.5
	Middle Management	174	19.5		500–999 employees	139	15.6
	Lower Management	164	18.4		1,000–4,999 employees	193	21.7
	Non-management	528	59.3		5,000–10,000 employees	140	15.7
	Information Technology Related	204	22.9		10,000+ employees	272	30.5
	NOT Information Technology Related	687	77.1	Industry	Information Technology	66	7.4
Income	$10,000-$30,000	85	9.5		Financial Services	98	11.0
	$30,000-$50,000	258	29.0		Healthcare	193	21.7
	$50,000-$80,000	268	30.1		Telecommunications	22	2.5
	$80,000-100,000	127	14.3		Retail	85	9.5
	$100,000+	153	17.2		Manufacturing	61	6.8
					Government	110	12.3
					Other	256	28.7

3.4.2. Measures

We adopted pre-existing instruments from prior research and made necessary adaptations to fit them into our research context. All of the key constructs in the model were measured with multiple items. To measure employee ISP compliance we adopted the items from Liang et al. (2013), Tyler and Blader (2005), and Yazdanmehr and Wang (2016). Keeping with our conceptualization of peer monitoring, we adopted direct peer monitoring items from Loughry and Tosi (2008) and De Jong and Elfring (2010). We chose the items applicable to the context of ISP compliance (peer observing, peer correcting, and peer reporting). We then modified their wording to match them with information security context—we replaced the items wording further such that phrases such as "complying with the ISP" or "ISP compliance" for group performance outcomes such as "completes their work on time". We adapted items for responsibility by commission, responsibility by omission, and collective responsibility items from Denson et al. (2006) and Lickel et al. (2003). Originally, these constructs conceptualized to capture the perception of individuals in a case of an incident or a negative act. We considered ISP noncompliance as a negative act and reworded the items accordingly. Items for the certainty of detection and severity of punishment were adopted from Herath and Rao (2009a, 2009b). Items for commitment to ISP were adopted from Herscovitch and Meyer (2002). Original items were designed to capture the commitment to change. We adapted the items to our context and replaced the "change" phrasing with the "ISP" and "ISP compliance". We adopted and changed the items for policies regarding the monitoring from Rothwell and Baldwin (2007). Finally, we adopted items for IT Intensiveness from (Thong and Yap 1995). All the items were measured by 7-point Likert scales. IS faculty members and Ph.D. students experienced in survey-based research examined the measurement items to assure its clarity and content validity (refer to Table 3.2 for the list of items).

Table 3.2. Measurement Items

	Constructs	Items	Source

	ISP Compliance	• How often do you comply with the ISP? • How often do you use the ISP to guide you how to access to and use information assets? • How often do you seek information about the appropriate ISP before acting? • How often do you follow the ISP about how you should use computer or network resources? • How often do you do as the ISP requires?	(Liang et al. 2013; Tyler and Blader 2005)
Peer Monitoring	Peer Observing	• In our group, members watch whether everyone follows the ISP correctly. • In our group, members keep close track of whether everyone complies with the ISP as expected. • In our group, members check whether everyone is following the ISP as expected. • In our group, members closely monitor each other's behavior regarding ISP compliance.	(Jong et al. 2010; Loughry and Tosi 2008)
	Peer Correcting	• In our group, members help correct each other's mistakes related to ISP compliance. • In our group, members assist the ISP wrongdoers to correct their mistakes. • In our group, members correct those who do not correctly follow the ISP. • In our group, members select 'somewhat disagree' please. • In our group, members let ISP wrongdoers know of their mistakes, • In our group, members verbally intervene if someone does not follow the ISP. • In our group, members offer guidance to others regarding the ISP compliance.	
	Peer Reporting	• In our group, members tell a supervisor/manager if there is anyone not complying with the ISP. • In our group, members let a coworker know if there is anyone not complying with the ISP. • In our group, members tell a supervisor/manager if others do not follow the ISP. • In our group, members let a coworker know if others do not follow the ISP.	
	Collective Responsibility	• Each member should feel responsible if others do not comply with the ISP. • The group as a whole should be blamed if some members do not comply with the ISP. • Each member should be blamed if another member does not comply with the ISP. • Other members in addition to the wrongdoer should be held responsible for the wrongdoers' ISP noncompliance.	(Denson et al. 2006; Lickel et al. 2003)
	Responsibility by Commission	• Members in my group directly or indirectly contribute to others' ISP noncompliance. • Members in my group approve others' ISP noncompliance. • Members in my group benefit from others' ISP noncompliance. • Members in my group know about the intention of others who do not comply with the ISP.	
	Responsibility by Omission	• Members in my group are expected to prevent others' ISP noncompliance.. • Members in my group know about the intention of others who do not comply the ISP. • Members in my group have the ability to prevent others' ISP noncompliance. • Members in my group have a responsibility to prevent others' ISP noncompliance if they know the intentions of the wrongdoers.	

	Commitment to ISP	• I believe in the value of the ISP. • Introducing the ISP is a good strategy for this organization. • The ISP serves an important purpose. • The ISP is not necessary (Reversed).	(Herscovitch and Meyer 2002)
Deterrence	Certainty of Detection	• If I do not comply with the ISP, I would probably be caught. • The chance to be caught is high, if I do not follow the ISP • Employees in my organization are properly monitored for ISP noncompliance.	(Herath and Rao 2009a, 2009b)
	Severity of Punishment	• My company disciplines employees if they do not follow the ISP. • If I repeatedly do not comply with the ISP, my company terminates me. • If I were caught not complying with the ISP, I would be severely punished.	
Control Variables			
	Policies for Monitoring	• Does your company maintain a written policy regarding correcting others' ISP noncompliance? • Does your company have a formal policy requiring you to correct ISP noncompliance by other employees? • Does your company maintain a written policy manual regarding reporting ISP noncompliance? • Does your company have a specific policy requiring you to report ISP noncompliance by other employees? • Does your company have a unit of personnel assigned specifically to investigate complaints of ISP noncompliance by employees?	(Rothwell and Baldwin 2007)
	IT Intensiveness	• My company is dependent on up-to-date information technology. • It is very important for my company to have access to reliable, relevant and accurate information technology. • It is very important for my company to access IT systems quickly.	(Thong and Yap 1995)

3.5. DATA ANALYSIS

Structural equation modeling was used to test the model. The proposed model is complex and uses both formative constructs (i.e., peer monitoring and deterrence) and reflective constructs. The component-based partial least squares (PLS) approach was used to validate measurement scales and to test the proposed research model (Gefen et al. 2011). In addition, due to the exploratory nature of proposed model, PLS seemed the well fit (Esposito Vinzi et al. 2010). The SmartPLS software package (version 3.2.6) (Ringle et al. 2015) used for the estimations. The bootstrapping procedures with 2000 resamples were used to estimate the path coefficients weights and their significance.

3.5.1. Measurement Validation

First, we examined the psychometric properties of the latent constructs such as convergent validity, individual item reliability, composite reliability, and discriminant validity to ensure the measurement quality of all these constructs—ISP compliance behavior, peer observing, peer correcting, peer reporting, collective responsibility, responsibility by commission, responsibility by omission, commitment to ISP, certainty of detection, severity of punishment, policies for monitoring, and IT intensiveness (Fornell and Larcker 1981). We calculated the composite reliability and Cronbach's alpha for each construct to examine their measurement reliability; all the measures exceeded the cutoff values of 0.7 (Fornell and Larcker 1981; Nunnally and Bernstein 1994). We calculated the factor loadings, the average variance extracted (AVE) values, the square root of the AVE, and correlation among the latent constructs. All the AVEs were well above 0.5 suggesting each construct captured its intended variance as opposed to error variance. In addition, the square root of the AVE for all constructs was much higher than all other cross-correlations; indicating a convergent validity. All the correlations were well below 0.9 threshold, indicating the distinctiveness of each construct. Finally, all item loadings were highest on their projected constructs, with them higher than 0.70 and significant t-values (refer to table 3.3 and 3.4).

Table 3.3. Factor Loadings

	CB	MO	MC	MR	CR	RC	RO	CI	CD	SP	PM	II
CB1	**0.82**	0.34	0.44	0.41	0.11	-0.19	0.14	0.42	0.43	0.48	0.20	0.20
CB2	**0.70**	0.35	0.36	0.32	0.18	-0.04	0.21	0.33	0.36	0.38	0.22	0.18
CB3	**0.73**	0.52	0.51	0.48	0.28	0.04	0.30	0.37	0.43	0.49	0.33	0.21
CB4	**0.83**	0.37	0.46	0.39	0.14	-0.16	0.17	0.44	0.38	0.45	0.23	0.24
CB5	**0.86**	0.40	0.47	0.44	0.15	-0.20	0.20	0.48	0.47	0.51	0.25	0.21
MO1	0.49	**0.96**	0.63	0.64	0.45	0.09	0.52	0.43	0.47	0.57	0.45	0.23
MO2	0.48	**0.98**	0.62	0.65	0.48	0.11	0.54	0.40	0.47	0.57	0.46	0.22
MO3	0.48	**0.96**	0.64	0.67	0.47	0.09	0.55	0.41	0.48	0.58	0.45	0.22

MO4	0.48	**0.96**	0.60	0.65	0.48	0.12	0.52	0.38	0.47	0.56	0.44	0.21
MC1	0.46	0.53	**0.87**	0.58	0.25	0.01	0.39	0.41	0.41	0.51	0.35	0.20
MC2	0.48	0.54	**0.89**	0.57	0.26	0.00	0.41	0.44	0.40	0.50	0.34	0.19
MC3	0.54	0.61	**0.92**	0.62	0.30	-0.01	0.41	0.49	0.48	0.58	0.41	0.24
MC4	0.52	0.58	**0.90**	0.61	0.27	-0.04	0.41	0.51	0.49	0.56	0.40	0.22
MC5	0.54	0.62	**0.89**	0.66	0.33	0.00	0.43	0.50	0.48	0.58	0.39	0.21
MC6	0.50	0.59	**0.88**	0.61	0.25	-0.03	0.41	0.47	0.48	0.55	0.36	0.22
MR1	0.54	0.67	0.68	**0.89**	0.33	0.00	0.39	0.44	0.53	0.61	0.43	0.19
MR2	0.34	0.48	0.47	**0.81**	0.31	0.06	0.32	0.29	0.36	0.42	0.36	0.13
MR3	0.53	0.65	0.68	**0.91**	0.32	0.00	0.39	0.44	0.53	0.60	0.43	0.19
MR4	0.28	0.44	0.41	**0.77**	0.31	0.09	0.32	0.25	0.31	0.36	0.33	0.12
CR1	0.26	0.46	0.32	0.37	**0.75**	0.21	0.57	0.27	0.24	0.31	0.42	0.15
CR2	0.17	0.40	0.26	0.31	**0.90**	0.28	0.54	0.17	0.17	0.24	0.36	0.12
CR3	0.16	0.41	0.25	0.32	**0.92**	0.33	0.56	0.12	0.18	0.24	0.36	0.08
CR4	0.15	0.40	0.25	0.29	**0.90**	0.32	0.57	0.13	0.18	0.21	0.36	0.09
RC1	-0.07	0.14	0.05	0.10	0.29	**0.82**	0.33	-0.11	0.01	0.00	0.20	-0.04
RC2	-0.19	0.00	-0.10	-0.05	0.21	**0.85**	0.21	-0.26	-0.13	-0.17	0.08	-0.09
RC3	-0.18	0.00	-0.09	-0.02	0.21	**0.82**	0.17	-0.29	-0.14	-0.15	0.03	-0.14
RC4	-0.08	0.16	0.04	0.05	0.33	**0.84**	0.38	-0.14	-0.03	-0.03	0.14	-0.02
RO1	0.26	0.53	0.43	0.42	0.59	0.25	**0.87**	0.25	0.32	0.34	0.44	0.15
RO2	0.16	0.44	0.33	0.32	0.58	0.39	**0.83**	0.12	0.23	0.26	0.35	0.09
RO3	0.18	0.40	0.35	0.29	0.51	0.32	**0.86**	0.20	0.27	0.26	0.36	0.12
RO4	0.27	0.45	0.42	0.38	0.47	0.18	**0.78**	0.33	0.34	0.33	0.43	0.14
CI1	0.49	0.42	0.50	0.43	0.22	-0.15	0.27	**0.88**	0.41	0.47	0.38	0.35
CI2	0.45	0.35	0.46	0.38	0.18	-0.19	0.23	**0.88**	0.35	0.41	0.35	0.36
CI3	0.42	0.33	0.44	0.34	0.15	-0.21	0.23	**0.87**	0.37	0.38	0.30	0.36
CI4	0.37	0.28	0.35	0.28	0.11	-0.20	0.14	**0.69**	0.29	0.31	0.25	0.26
CD1	0.49	0.48	0.51	0.50	0.21	-0.08	0.32	0.42	**0.92**	0.75	0.48	0.27
CD2	0.46	0.41	0.46	0.45	0.17	-0.09	0.31	0.41	**0.91**	0.68	0.44	0.27
CD3	0.48	0.46	0.44	0.49	0.22	-0.04	0.32	0.35	**0.92**	0.70	0.46	0.22
SP1	0.55	0.55	0.59	0.60	0.26	-0.09	0.35	0.46	0.72	**0.94**	0.41	0.26
SP2	0.53	0.53	0.56	0.54	0.27	-0.07	0.32	0.44	0.70	**0.94**	0.41	0.25
SP3	0.56	0.56	0.54	0.53	0.27	-0.08	0.31	0.42	0.73	**0.89**	0.46	0.30
PM1	0.23	0.38	0.31	0.33	0.37	0.16	0.41	0.26	0.36	0.34	**0.82**	0.19
PM2	0.19	0.38	0.33	0.33	0.42	0.22	0.47	0.22	0.33	0.31	**0.81**	0.16
PM3	0.26	0.35	0.34	0.39	0.33	0.08	0.36	0.35	0.44	0.39	**0.85**	0.25
PM4	0.29	0.42	0.40	0.44	0.37	0.09	0.40	0.37	0.47	0.43	**0.88**	0.20
PM5	0.29	0.37	0.32	0.38	0.26	0.04	0.27	0.38	0.45	0.44	**0.70**	0.27
II1	0.26	0.24	0.24	0.21	0.15	-0.06	0.15	0.35	0.29	0.30	0.24	**0.89**
II2	0.21	0.20	0.22	0.16	0.10	-0.06	0.12	0.37	0.23	0.24	0.23	**0.92**
II3	0.23	0.17	0.18	0.14	0.08	-0.08	0.13	0.36	0.23	0.24	0.23	**0.89**

ISP Compliance Behavior; MO: Peer Observing: MC: Peer Correcting; MR: Peer Reporting; CR: Collective Responsibility; RC: Responsibility by Commission; RO: Responsibility by Omission; CI: Commitment to ISP; CD: Certainty of Detection; PM: Policies for Monitoring; SP: Severity of Punishment; II: IT Intensiveness.

Table 3.4. Reliability, Average Variance Extracted and Construct Correlation Matrix

	AVE	CR	AL	CB	MO	MC	MP	CR	RC	RO	CD	CI	PM	SP	II
CB	0.85	0.89	0.63	0.79											
MO	0.98	0.98	0.93	0.50	0.96										
MC	0.95	0.96	0.80	0.57	0.65	0.89									
MP	0.87	0.91	0.72	0.52	0.68	0.68	0.85								
CR	0.89	0.93	0.76	0.21	0.49	0.31	0.37	0.87							
RC	0.86	0.90	0.70	-0.15	0.11	-0.01	0.04	0.32	0.84						
RO	0.85	0.90	0.69	0.26	0.55	0.46	0.43	0.65	0.34	0.83					
CD	0.85	0.90	0.70	0.52	0.42	0.53	0.43	0.20	-0.22	0.26	0.83				
CI	0.91	0.94	0.85	0.59	0.59	0.61	0.61	0.29	-0.09	0.36	0.48	0.92			
PM	0.87	0.91	0.66	0.31	0.47	0.42	0.46	0.43	0.15	0.47	0.39	0.46	0.81		
SP	0.90	0.94	0.84	0.52	0.49	0.51	0.53	0.22	-0.08	0.35	0.43	0.78	0.50	0.92	
II	0.88	0.93	0.81	0.27	0.23	0.24	0.19	0.13	-0.08	0.15	0.40	0.29	0.26	0.28	0.90

AVE: Average Variance Extracted; CR: Composite Reliability; AL: Cronbach's Alpha; CB: ISP Compliance Behavior; MO: Peer Observing: MC: Peer Correcting; MR: Peer Reporting; CR: Collective Responsibility; RC: Responsibility by Commission; RO: Responsibility by Omission; CI: Commitment to ISP; CD: Certainty of Detection; PM: Policies for Monitoring; SP: Severity of Punishment; II: IT Intensiveness.
Note: The diagonal represents the square root of (AVE) values.

Second, we evaluated the formative constructs. Both peer monitoring and perceived deterrence were modeled as second-order formative constructs. Peer monitoring construct was modeled as a second-order construct with three first-order latent sub-constructs (peer observing, peer reporting, and peer correcting), while perceived deterrence was modeled as a second-order construct with two first-order latent sub-constructs (perceived severity of punishment and certainty of detection). The weight from the first-order sub-constructs (peer observing, peer reporting, and peer correcting) to the second-order constructs (peer monitoring) were (b = .36, p < .001; b = .50, p < .001; b = .27, p < .001) respectively, whereas for the first-order sub-constructs (perceived certainty of detection and severity of punishment) to the second-order constructs (deterrence) were (b = .53, p < .001; b = .53, p < .001) respectively. We calculated the variance inflation factor (VIF) to test potential multicollinearity among the sub-constructs. All the VIFs were less than 3.3, suggesting that multicollinearity is not a major concern (Petter et al. 2007) (refer to Table 3.5 and 3.6).

Table 3.5. Correlation Between Sub-constructs of Peer Monitoring

Construct	Coefficients	Sig.	VIF
MO	0.36	.000	2.39
MC	0.50	.000	2.15
MR	0.27	.000	2.34

MO: Peer Observing; MC: Peer Correcting; MR: Peer Reporting.

Table 3.6. Correlation Between Sub-constructs of Deterrence

Construct	Coefficients	Sig.	VIF
CD	0.53	.000	2.51
SP	0.53	.000	2.51

CD: Certainty of Detection; SP: Severity of Punishment;

3.5.2. Testing the Structural Model

3.5.2.1. Control Variables

Previous research on information security has identified additional variables as they have a potential influence on employee ISP compliance, monitoring, commitment to ISP, and perceived deterrence. This study, however, seeks to move beyond these established these predictors. Therefore, we controlled for employees characteristics such as age, gender (Leonard and Cronan 2001; Leonard et al. 2004), and employees' knowledge of ISP, and employees' tenure in their group. Furthermore, we controlled for IT intensiveness of the organization and policies regarding peer monitoring. Table 3.7 list the relevant relationships between control variables and constructs.

The nature of this study makes our results susceptible to potential social desirability bias toward reporting higher ISP compliance, peer monitoring, commitment to ISP, and perceived deterrence. Therefore, we examined the relationship between above-mentioned constructs and a short version of the Marlowe–Crowne social desirability scale (Strahan and Gerbasi 1972). The result for the relationship between social desirability and ISP compliance as well as social desirability and peer monitoring were significant (b= .13, p < .001; b = .14, p < .001 respectively). To mitigate social desirability bias effect on the result, we controlled for it in our hypothesis testing.

The integrity of the results of studies using survey method is susceptible to the common method bias (CMV) as both dependent and independent variables were gathered from the same participant. We employed Harman's one-factor test (Podsakoff, MacKenzie, Lee, et al. 2003) to explore if CMV is a concern. We did an exploratory factor analysis using all the measurement items. We found fifteen factors, all explained 69.94% of the data variance. No single factor explained the majority of the variance. The factor with the largest variance only explained 27.08% of the data variance. Therefore, we conclude that CMV is not a concern.

The link between employees ISP knowledge and all the above-mentioned constructs were statistically significant. The reason behind such a relationship can be that higher knowledge of ISP makes people to (1) understand the importance of ISP and thus comply with it; (2) identify others ISP noncompliance behavior and thus see peer monitoring more feasible and thus engage in such behaviors; (3) realize that ISP is beneficial for both employees and organization and thus commit to it more; and lastly (4) be aware that there are a risk and punishment associated with ISP noncompliance, and therefore perceive higher deterrence.

IT intensiveness is the extent that IT engages in the products, services, processes, and of an organization (Thong 1999; Thong and Yap 1995). The results showed that IT intensiveness had a positive effect on peer monitoring, commitment to the ISP, and perceived deterrence. We postulate that such relationship exists because in companies who are heavily relying on information technology, individual may perceive that ISP is a valuable protection means that benefits employees and the organization; In addition, they may perceive that since group is heavily dependent on information technology, it is in employees self-interest to protect the information by peer monitoring; and finally, due to the emphasis on information technology, they may perceive that ISP noncompliance may be taken seriously by the organization.

Organizational policies for peer monitoring as expected had a significant effect on the perception of peer monitoring in the group. This is reasonable as by these policies organizations directly ask employees to monitor each other’s behavior and in the case of any noncompliance either fix or report such an action. In addition, one may perceive that the organization has established such policies for his or her benefits, increasing his or her commitment to the ISP. Finally, policies regarding peer monitoring, communicate the message that there is an additional monitoring system (in addition to organizational surveillance systems) and thus ISP noncompliance is riskier and is more likely to be punished.

Finally, the results showed that the higher the age of employees, the more they are likely to follow the ISP and the more they may perceive the peer monitoring. One can argue that those who are older may be more experienced and more cautious about their behavior. Thus, they may have higher conscious of peer monitoring and as a result ISP compliance.

Table 3.7. Effects of Control Variables

Control variables	ISP Compliance	Peer Monitoring	Commitment To ISP	Perceived Deterrence
Social Desirability	0.13***	0.14***	0.00 n.a.	-0.01 n.a.
ISP Knowledge	0.11***	0.09***	0.17***	0.07**
IT Intensiveness	-0.02 n.a.	0.08 **	0.24***	0.10***
Tenure in the Group	-0.03 n.a.	0.03 n.a.	0.02 n.a.	-0.06 n.a.
Gender (Male)	-0.03 n.a.	-0.06*	0.00 n.a.	-0.03 n.a.
Age	0.11***	0.06*	0.05 n.a.	0.03 n.a.
Monitoring Policies	-	0.34***	0.11**	0.23***

3.5.2.2. Hypothesis Testing

The PLS path coefficients of the proposed research model are depicted in Figure 3.2 (without showing the control variables presented in Table 3.7). Our proposed model explains 52% variance of employee ISP compliance, 40% variance of peer monitoring, 45% variance of collective responsibility, 40% of commitment to the ISP, and finally 52% of perceived deterrence.

The total effects—sum of the direct and indirect effects—of the independent variables on the dependent variables are presented in Table 3.8.

Our results show that peer monitoring (b = .27, p < .001) has a significant positive impact on employee ISP compliance, supporting H1. To test the mediation effect, we used bootstrapping method as the computing power of the current computers have empowered more accurate statistical mediation testing (Shrout and Bolger 2002).

Table 3.8. Total Effect of the Independent Variables on the Dependent Variables (ISP Compliance)

	ISP Compliance	Commitment To ISP	Perceived Deterrence	Peer Monitoring	Collective Responsibility
Commitment To ISP	0.18***	—	—	—	—
Perceived Deterrence	0.27***	—	—	—	—
Peer Monitoring	0.48***	0.39***	0.53***	—	—
Collective Responsibility	0.11***	0.09***	0.12***	0.23***	—
Responsibility by Omission	0.06***	0.05***	0.06***	0.12***	0.53***
Responsibility by Commission	0.01***	0.01***	0.01***	0.03***	0.12***

We followed the Baron and Kenny method in Hayes (2009) and evaluated three paths. (1) The path between independent variable and mediator, (2) the path from the mediator and dependent, (3) the path from the independent variable to the dependent variable. The results showed that (1) the path between perceived peer monitoring and commitment to the ISP (b = .39, p < .001) as well as perceived peer monitoring and perceived deterrence (b = .52, p < .001) were significant; (2) the path between commitment to the ISP and ISP compliance (b = .18, p < .001) and, perceived deterrence and ISP compliance (b = .27, p < .001) were significant as well; (3) the direct effect between peer monitoring was significant (b = .27, p < .001) as well; (4) the indirect effect of peer monitoring on ISP compliance was statistically significant (b = .21, p < .001); (5) the total effect of peer monitoring on ISP compliance decreased from (b = .48, p < .001) to (b = .27, p < .001) with introducing commitment to the ISP and perceived deterrence; All together indicates that the relationship between peer monitoring and ISP compliance is partially mediated by commitment to the ISP and perceived deterrence (Hayes 2009; MacKinnon 2008; Shrout and Bolger 2002), supporting H2 and H3. Table 3.9 and 3.10 summarize the direct and indirect effect of the independent variables on ISP compliance. The path between collective responsibility and perceived peer monitoring (ɓ = .23, p < .001) was significant, providing support for H4. Finally, the path between responsibility by omission and collective responsibility (ɓ = .53, p < .001) as well as responsibility by commission and ISP compliance (ɓ = .12, p < .001) were significant, supporting H5 and H6.

Table 3.9. Direct Effect of the Independent Variables on the Dependent Variables (ISP Compliance)

	ISP Compliance	Commitment To ISP	Perceived Deterrence	Peer Monitoring	Collective Responsibility
Commitment To ISP	0.18***	—	—	—	—
Perceived Deterrence	0.27***	—	—	—	—
Peer Monitoring	0.27***	0.39***	0.52***	—	—
Collective Responsibility	—	—	—	0.23***	—
Responsibility by Omission	—	—	—	—	0.53***
Responsibility by Commission	—	—	—	—	0.12***

Table 3.10. Indirect Effect of the Independent Variables on the Dependent Variables (ISP Compliance)

	ISP Compliance	Commitment To ISP	Perceived Deterrence	Peer Monitoring	Collective Responsibility
Peer Monitoring	0.21***	—	—	—	—
Collective Responsibility	0.11***	0.09***	0.12***	—	—
Responsibility by Omission	0.06***	0.05***	0.06***	0.12***	—
Responsibility by Commission	0.01***	0.01***	0.01***	0.03***	—

3.5.3. Post Hoc Analysis

3.5.3.1 Investigating peer monitoring

The proposed model gave a holistic view of peer monitoring and its impact on employee ISP compliance. However, it can be inferred from the previous discussions that each dimension of peer monitoring may have a distinct impact on commitment to the ISP and perceived deterrence. Thus, in this section, to gain more insight, we evaluated peer monitoring dimensions independently. The result of the model testing is presented in Figure 3.3. In addition, total effect, indirect effect, and path coefficient of the each dimension of peer monitoring and ISP compliance are reported in Table 3.11.

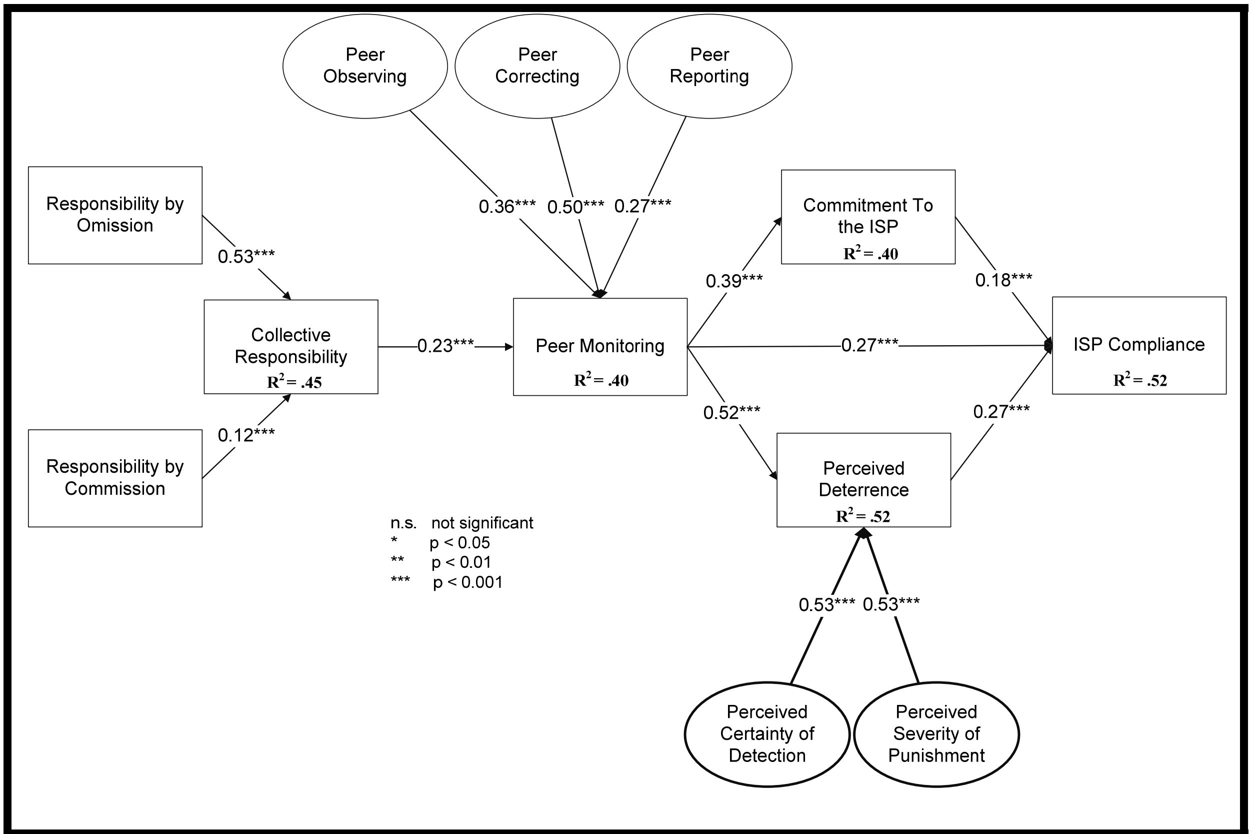


Figure 3.2. Results

The results suggested that the effect of peer reporting on perceived deterrence is stronger (b = .22, p < .001) than on commitment to the ISP (b = .09, p < .05). Theoretically, it is justifiable as peer reporting implies that group members greatly emphasize on information security and thus if they got caught they might be faced with severe punishment (both from management and peers).

In addition, it suggests that aside from organization surveillance systems there is an informal effective surveillance mechanism in the group, enhancing the risk of getting caught.

Peer observing had a significant influence on perceived deterrence (b = .16, p < .001), while its impact on commitment to the ISP was insignificant. This is theatrically plausible as peer observing often conveys the perception that behaviors that once were difficult for formal surveillance systems to identity are now easy and feasible to detect (by peers) (Fischer and Hughes 1997). In this sense, it also signals that there would be the higher frequency of punishments.

Peer correcting had a stronger effect on commitment to the ISP (b = .32, p < .001) than on perceived deterrence (b = .22, p < .001). This is because peer correcting communicates that ISP compliance is an important matter for the group such that members are willing to spend extra time and effort to help other members correct their wrongdoings. This creates the mindset that the success of ISP is in the interest of the group and its members. In addition, peer correcting can express that ISP compliance of group members may not go unnoticed, creating the higher perception of deterrence.

Moreover, the results showed that the effect of peer reporting on ISP compliance is partially mediated (b = .07, p < .001) through both commitment to the ISP and perceived deterrence, while perceived deterrence is a stronger mediator; the effect of peer observing on ISP compliance is partially mediated (b = .05, p < .01) only through perceived deterrence; and finally, the effect of peer monitoring on employee ISP compliance is partially mediated (b = .12, p < .001) by commitment to the ISP and perceived deterrence. Altogether, the results confirm the previous hypothesis (H1, H2, and H3) and validity of the conceptualization of peer monitoring (as a second-order formative construct).

3.5.3.2. Role of benevolent ethical climate

The proposed model in this study did not consider the possible negative effect of peer monitoring. Some studies have suggested it may signal distrust in some cases (Jong and Bunt 2008). In cases when it is perceived as an appropriate act, it might not be considered a sign of distrust (Ferrin et al. 2007; De Jong and Dirks 2012). Individuals tend to interpret a behavior in terms of its causes and that affects how they react (Kelley and Michela 1980). Individuals in their interpretation, evaluate the behaviors against their common expectations (De Jong and Dirks 2012). In the majority of cases, a negative interpretation of peer monitoring arises because individuals did not expect it to occur.

As employees' perception of peer monitoring would vary (De Jong and Dirks 2012) and their immediate social environment (i.e., organizational climate) provide cues to interpret (i.e., social information processing) work-related behaviors and events (Salancik and Pfeffer 1978; Shamir and Lapidot 2003), this study investigates the contextual factors that would peer monitoring seem as an accepted and expected behavior carried out to benefit the group.

To this end, we looked at benevolence organizational climate, in which employees based their decisions on the well-being of others, including their peers or organizations as a unit; in other words, members are willing to help each other (Cullen et al. 2003). This type of climate produces bonds between employees and the organization, thereby motivating more cooperation and cohesiveness (Appelbaum et al. 2005; Cullen et al. 2003). It is characterized by supportiveness, friendliness, mutual personal attraction, positive feelings about tasks, and cooperation (Brief and Motowidlo 1986; Cullen et al. 2003; Wech et al. 1998).

A benevolent organizational climate can shape the perception of peer monitoring in two ways. First, it breeds trust among members (Langfred 2004); thus, the latter may be seen as a positive act to protect the group, rather than a negative act to control members. Second, it encourages employees to look after each other, thereby positioning peer monitoring as an expected act of compassion, rather than a devious act.

We argue that because an organization with a high level of a benevolent climate would emphasize friendship, caring, cohesiveness, and prosocial behaviors (Cullen et al. 2003; Wech et al. 1998), employees are more likely to perceive peer monitoring as a positive behavior and respond favorably. Conversely, in organizations with lower levels of a benevolent climate, employees may interpret peer monitoring as an inappropriate act and thereby react negatively. Thus, in brief, we argue that a high benevolent climate compared to a low one (1) creates a positive attitude toward peer monitoring that leads to more commitment and consequently ISP compliance and (2) encourages peer monitoring. Accordingly, we tested the moderation effect of benevolent organizational climate on the relationship between peer monitoring and ISP compliance. However, the results were not significant (b = .00).

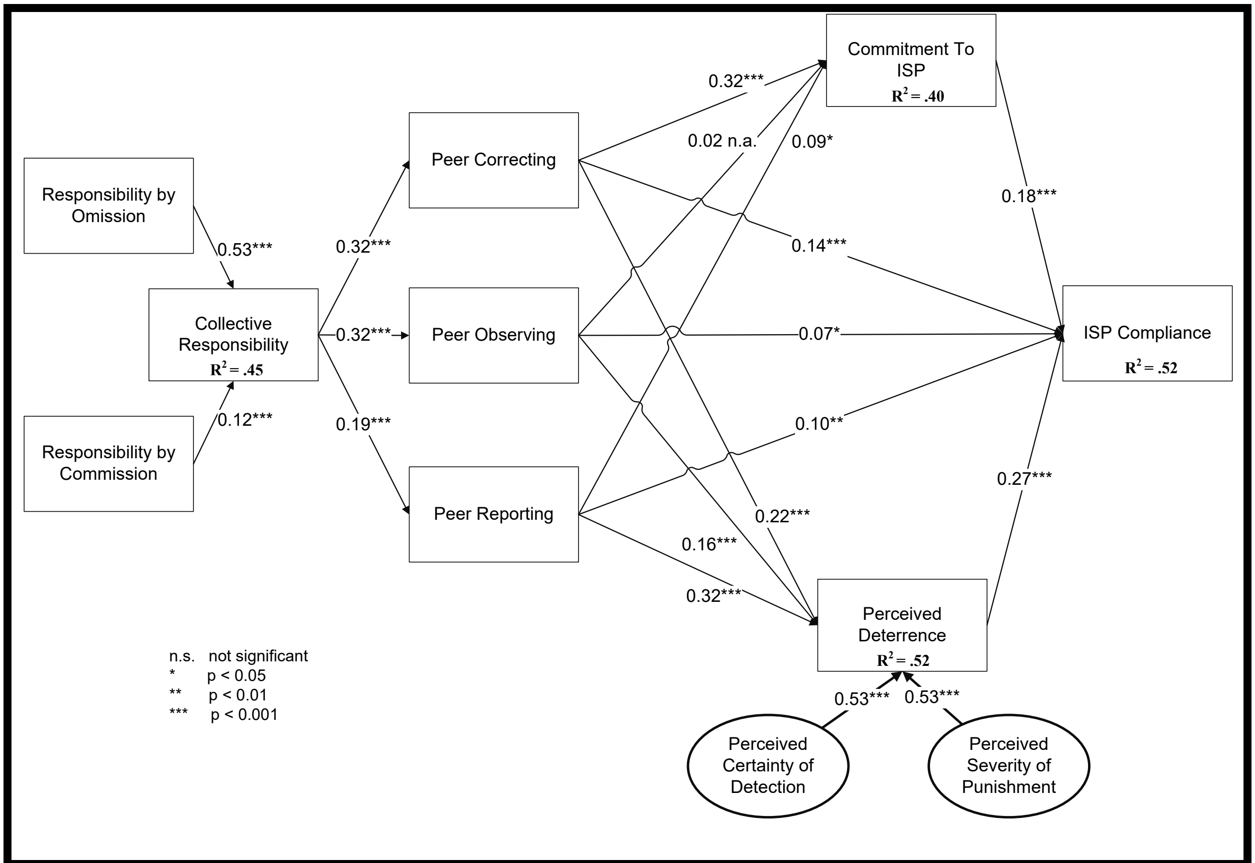


Figure 3.3. Post Hoc Analysis Results

Table 3.11. Total Effect, Indirect Effect, and Path Coefficient of the Peer Monitoring Sub-Constructs on ISP Compliance

	Total Effect	Indirect	Path Coefficient
Peer Reporting	0.17***	0.07***	0.10**
Peer Observing	0.12**	0.05**	0.07*
Peer Correcting	0.26***	0.12***	0.14***

3.6. DISCUSSION

This study aims at theorizing about and empirically testing the role of peer monitoring, its antecedents, and its working mechanisms in light of the growing interest in finding socio-technical approaches that can efficiently motivate ISP compliance.

3.6.1. Contributions to Theory

This study contributes to the information security literature in various ways. First, it suggests that peer monitoring, in offering an efficient detection mechanism to increase the perception of risk and punishment, is a noteworthy solution to ISP noncompliance. This is a significant contribution as employees ignore deterrence messages and do not comply with the ISP in many cases (Straub and Welke 1998; Willison and Warkentin 2009). While previous studies have incorporated informal sanctions with general deterrence (Piquero and Tibbetts 1996), the role of informal monitoring has not been investigated. This study, however, introduces a new complementary component (informal monitoring) to general deterrence theory. This is theoretically reasonable as members who peer monitor can detect behaviors that organizational formal monitoring systems may overlook.

In addition, peer monitoring via peer correcting aims to prevent the ISP noncompliance at the moment of occurrence (Straub 1990). This is especially noteworthy as previous studies focused mainly on solutions to be implemented before ISP noncompliance, which does not necessarily stop ISP noncompliance, only discourages them. However, peer monitoring not only discourages ISP noncompliance but also stops it at the time of happening. Also, this study showed that by providing guidance in the form of immediate feedback to correct ISP noncompliance, peer monitoring increases ISP awareness and addresses the training gap known to be the source of ISP noncompliance (Willison and Warkentin 2009). Finally, such a strategy can enhance the perception that employees are looked after by their peers and the organization, thereby increasing their commitment to the ISP and consequently ISP compliance.

Previous studies have investigated the impact of affective organizational commitment on ISP compliance (c.f., Posey et al. 2015). Employees with affective organizational commitment want to stay at their organizations because their values are aligned with the organizational goals and values (Meyer et al. 1997). This study take a more in-depth look into this phenomenon. We frame affective commitment to the ISP as a specific type that only focuses on ISP success. This is significant as an employee may identify with the organization or believe in its values, but not necessarily the ISP or ISP compliance. Thus, this new concept can be a better fit in the context of information security.

Finally, this study suggests that in an organization not only peer monitoring policies but also a social context in which individual group members can threaten the group and its members' interests can motivate peer monitoring. In this way, members ensure everyone complies with the ISP so that they are not held responsible when someone else does not comply individual group members can threaten the group and its members' interests, (Alchian and Demsetz 1972).This study introduced collective responsibility as a norm that can link individuals' interests to group interests. To the best of our knowledge, this study is the first to introduce this norm to the information security literature.

3.6.2. Practical Implications

By introducing peer monitoring as an alternative mechanism to formal monitoring mechanisms, this study has several implications for practitioners. First, the results suggest that organizations can benefit from using peer monitoring to improve ISP compliance when other mechanisms are not effective. It is a low-cost monitoring mechanism that provides organizations with a better picture of their employees' ISP compliance behavior—surveillance systems typically cannot or have difficulty collecting the type of information garnered by peer monitoring. The extra details can prove helpful in reducing ISP noncompliance opportunities. This is significant as recent reports have indicated that ISP noncompliance can occur in a disguised, repeated fashion, which is difficult and time-consuming to detect by surveillance systems (Cappelli et al. 2012; Verizon 2016). For instance, a hospital computer monitoring system may not detect nor identify a doctor who repeatedly takes a picture of patient's profile with their cell phone (i.e., ISP noncompliance). Moreover, this study suggests that peer monitoring can offer organizations immediate intervention by correcting ISP noncompliance. It can inform and train employees on accepted ISP compliance behaviors as well as motivate them to follow the ISP. This is especially important as the lack of ISP awareness, effective training, and motivation have been identified as primary reasons for ISP noncompliance (Willison and Warkentin 2013).

Second, this study propose collective responsibility as an informal way to encourage peer monitoring. Organizations can benefit from holding all employees responsible for instances of ISP noncompliance; in doing so, it motivates them to perform peer monitoring to prevent ISP noncompliance. This is noteworthy because organizational surveillance practices without collective responsibility in play may not be effective. When employees know it is the organization's job to monitor their peers' ISP compliance, they are more inclined to ignore the ISP noncompliance of their peers (Stewart et al. 2012).

Finally, this study also advances ways that organizations can establish collective responsibility norms. It proposes that organizations indicate individual group members could be held accountable as they either could have prevented or may be benefited from such ISP noncompliance. Security managers can establish such norms by integrating them in the organizational culture.

3.6.3. Limitations and Future Research

This study may have some limitations that may require further consideration. They are rooted in the survey design. The proposed model only explains 52% of variance in employee ISP compliance. Clearly, this study failed to consider other contributing factors, such as individual moral values, that future studies can further investigate. Moreover, despite the Harman test indicated the results do exhibit common method bias, the self-reporting means it is possible that the responses are skewed positively toward ISP compliance. In fact, social desirability was positively associated with ISP compliance, which confirms this concern. Therefore, future studies can employ approaches based on multiple sources. In addition, the cross-sectional design provides minimum support for causation. While our central hypothesis (**H_1**) has been investigated and confirmed in different settings (e.g., employee performance), this study is the first to test such a relationship in the context of ISP compliance. This is important as one may argue that those who comply with the ISP may have a higher perception of peer monitoring. Future studies may use different designs, such cross-lagged, case-study, or experimental, to address this concern.

REFERENCES

Adkins, C. L., and Russell, C. J. 1994. "Judgments of Fit in the Selection Process: the Role of Work Value Congruence," *Personnel Psychology*, (47:3), pp. 605–623.

Agnew, R., and Peters, A. a. R. 1986. "Techniques of Neutralization," *Criminal Justice and Behavior*, (13:1), pp. 81–97.

Aiken, L. S., West, S. G., and Reno, R. R. 1991. *Multiple Regression: Testing and Interpreting Interactions*, Newbury Park, CA: Sage.

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), pp. 653–676.

Alchian, A., and Demsetz, H. 1972. "Production, information costs, and economic organization," *The American economic review*.

Alm, J., and McKee, M. 2006. "Audit certainty, audit productivity, and taxpayer compliance," *National Tax Journal*, (59:4), pp. 801–816.

Anderson, C. L., and Agarwal, R. 2010. "Practicing Safe Computing: a Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly*, (34:3), pp. 613-A15.

Arnott, R., and Stiglitz, J. E. 1991. "Moral Hazard and Nonmarket Institutions: Dysfunctional Crowding Out or Peer Monitoring?," *American Economic Review*, (81:1), pp. 179–190.

Ashkanasy, N. M., Wilderom, C. P., and Peterson, M. F. 2004. *Handbook of Organizational Culture & Climate*.

Bagozzi, R. P. 2011. "Measurement and meaning in information systems and organizational research: Methodological and philosophical foundations," *MIS Quarterly*, (35:1), pp. 261–292.

Baker, N. 1997. "Heightened interest in ethics education reflects employer, employee concerns," *Corporate University Review*.

Bamberg, S., and Schmidt, P. 2003. "Incentives, Morality, Or Habit?: Predicting Students' Car Use for University Routes With the Models of Ajzen, Schwartz, and Triandis," *Environment & Behavior*, (35:2), pp. 264–285.

Banerjee, D., Cronan, T. P. T., and Jones, T. T. W. 1998. "Modeling IT ethics: a study in situational ethics," *MIS Quarterly*, (22:March), pp. 31–60.

Barki, H., Titah, R., and Boffo, C. 2007. "Information system use-related activity: An expanded behavioral conceptualization of individual-level information system use," *Information Systems Research*, (18:2), INFORMS, pp. 173–192.

Barnard, C. I. 1938. "The Functions of the Executive," *Classic readings in organizational behavior*, (15:Book, Whole), p. 181-.

Barnett, J. H., and Karson, M. J. 1989. "Managers, values, and executive decisions: An exploration of the role of gender, career stage, organizational level, function, and the importance of ethics, relationships and results in managerial decision-making," *Journal of Business Ethics*, (8:10), pp. 747–771.

Barnett, T., and Schubert, E. 2002. "Perceptions of the ethical work climate and covenantal relationships," *Journal of Business Ethics*, (36:3), pp. 279–290.

Barnett, T., and Vaicys, C. 2000. "The Moderating Effect of Individuals' Perceptions of Ethical Work Climate on Ethical Judgments and Behavioral Intentions," *Journal of Business Ethics*, (27), pp. 351–362.

Bearden, W. O., and Etzel, M. J. 1982. "Reference group influence on product and brand purchase decisions.," *Journal of Consumer Research*, (9), pp. 183–194.

Bearden, W. O., Netemeyer, R. G., and Teel, J. E. 1989. "Measurement of Consumer Susceptibility to Interpersonal Influence," *Journal of Consumer Research*, (15:4), pp. 473–481.

Becker, G. 1968. "Crime and Punishment: An Economic Approach," in *Essays in the Economics of Crime and Punishment*, (Vol. 76), UMI, pp. 1–54.

Biel, A., and Thøgersen, J. 2007. "Activation of social norms in social dilemmas: A review of the evidence and reflections on the implications for environmental behaviour," *Journal of Economic Psychology*, (28:1), pp. 93–112.

Blau, P. M. 1964. "Exchange and Power in Social Life," in *Exchange and Power in Social Life*, Transaction Publishers New Brunswick, NJ, pp. 1 – 32, 88 – 142.

Bloch, P., Ridgway, N., and Sherrell, D. 1989. "Extending the concept of shopping: An investigation of browsing activity," *Journal of the Academy of Marketing Science*, (17:1), pp. 13–21.

Bobek, D. D., Hageman, A. M., and Kelliher, C. F. 2013. "Analyzing the Role of Social Norms in Tax Compliance Behavior," *Journal of Business Ethics*, (115:3), pp. 451–468.

Bonabeau, E. 2004. "The perils of the imitation age," *Harvard Business Review*, (82:6).

Bowen, D. E., and Ostroff, C. 2004. "Understanding HRM-firm performance linkages: The role of the 'strength' of the HRM system," *Academy of Management Review*, (29:2), pp. 203–221.

Brass, D. J., Butterfield, K. D., and Skaggs, B. C. 1998. "Relationships and unethical behavior: A social network perspective," *Academy of Management Review*, (23:1), pp. 14–31.

Brekke, K. A., Kipperberg, G., and Nyborg, K. 2010. "Social Interaction in Responsibility Ascription : The Case of Household Recycling," *Land Economics*, (86:4), pp. 766–784.

Brief, A. P., and Motowidlo, S. J. 1986. "Prosocial organizational behaviors," *Academy of Management Journal*, (11:4), pp. 710–725.

Buhrmester, M., Kwang, T., and Gosling, S. D. 2011. "Amazon's Mechanical Turk: A New Source of Inexpensive, Yet High-Quality, Data?," *Perspectives on Psychological Science*, (6:1), pp. 3–5.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance:

An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly*, (34:3), pp. 523–548.

Burke, R. J., and Weir, T. 1978. "Organizational climate and informal helping processes in work settings.," *Journal of Management*, (4:2), pp. 91–105.

Burnkrant, and Cousineau, A. 1975. "Informational and normative social influence in buyer behavior," *Journal of Consumer Research*, (2:3), pp. 206–215.

Callister, R. R., Kramer, M. W., and Turban, D. B. 1999. "Feedback seeking following career transitions," *Academy of Management Journal*, (42:4), pp. 429–438.

Cappelli, D. D., Moore, A. A., and Trzeciak, R. R. 2012. *The Cert Guide to Insider Threats: How to prevent, detect, and respond to Information Technology crimes (Theft, Sabotage, Fraud) Addison-Wesley*, (Vol. 1).

Carte, T. A., and Russell, C. J. 2003. "In pursuit of moderation: Nine common errors and their solutions," *MIS Quarterly*, (27:3), pp. 479–501.

Cenfetelli, R. T., and Bassellier, G. 2009. "Interpretation of formative measurement in information systems research," *MIS Quarterly*, (33:4), pp. 689–707.

Chan, M., Woon, I., and Kankanhalli, A. 2005. "Perceptions of Information Security at the Workplace : Linking Information Security Climate to Compliant Behavior," *Journal of Information Privacy and Security*, (1:3), pp. 18–41.

Chen, C. X., and Sandino, T. 2007. "Do Internal Controls Mitigate Employee Theft in Chain Organizations?," *University of Southern California*, University of Southern California.

Chin, W. W. 1998. "The partial least squares approach to structural equation modeling.," *Marcoulides, G.A. (Ed.), Modern Methods for Business Research.*, p. 295–336.

Chin, W. W. 1998. "Issues and Opinion on Structural Equation Modeling.," *MIS Quarterly*, (22:1), p. 1 (doi: Editorial).

Chin, W. W., and Gopal, A. 1995. "Adoption intention in GSS: relative importance of beliefs," *Data Base for Advances in Information Systems*, (26:2–3), ACM, pp. 42–64.

Chin, W. W., and Marcolin, B. 1995. "A holistic approach to construct validation in is research: examples of the interplay between theory and measurement.," *Administrative Sciences Association of Canada – 23rd Conference*, (16:4), pp. 33–43.

Chin, W. W., Marcolin, B. L., and Newsted, P. R. 2003. "A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study," *Information Systems Research*, (14:2), pp. 189–217.

Cialdini, R. B., Kallgren, C. a., and Reno, R. R. 1991. "A Focus Theory of Normative Conduct: A Theoretical Refinement and Reevaluation of the Role of Norms in Human Behavior," *Advances in Experimental Social Psychology*, (24:C), pp. 201–234.

Cialdini, R. B., Reno, R. R., and Kallgren, C. a. 1990. "A focus theory of normative conduct: Recycling the concept of norms to reduce littering in public places.," *Journal of Personality* *and Social Psychology*, (58:6), pp. 1015–1026.

Cialdini, R. B., and Trost, M. R. 1998. "Social influence: Social norms, conformity and compliance.," *The handbook of social psychology, Vols. 1 and 2*, pp. 151–192.

Collins, N. L., and Miller, L. C. 1994. "Self-disclosure and liking," *Psychological bulletin*, (116:3), pp. 457–475.

Cooper, M. D., and Phillips, R. a. 2004. "Exploratory analysis of the safety climate and safety behavior relationship," *Journal of Safety Research*, (35:5), pp. 497–512.

Cooper, W. H., and Withey, M. J. 2009. "The Strong Situation Hypothesis," *Personality and Social Psychology Review*, (13:1), pp. 62–72.

Cornish, D. B., and Clarke, R. V. 1986. "The reasoning criminal: rational choice perspectives on offending," *Criminology*, (25:4), pp. 933–948.

Cravens, D. W., Lassk, F. G., Low, G. S., Marshall, G. W., and Moncrief, W. C. 2004. "Formal and informal management control combinations in sales organizations. The impact on salesperson consequences," *Journal of Business Research*, (57:3), pp. 241–248.

D'Arcy, J., and 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*, (20:6), Nature Publishing Group, pp. 643–658.

D'Arcy, J., and Hovav, A. 2007. "Deterring internal information systems misuse," *Communications of the ACM*, (50:10), pp. 113–117.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Information Systems Research*, (20:1), pp. 79–98.

Denson, T. F., Lickel, B., Curtis, M., Stenstrom, D. M., and Ames, D. R. 2006. "The Roles of Entitativity and Essentiality in Judgments of Collective Responsibility," *Group Processes & Intergroup Relations*, (9:1), pp. 43–61.

Deutsch, M., and Gerard, H. B. 1955. "A study of normative and informational social influences upon individual judgement.," *Journal of abnormal psychology*, (51:3), pp. 629–636.

Diamantopoulos, A., and Siguaw, J. A. 2006. "Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration," *British Journal of Management*, (17:4), pp. 263–282.

Dickenson, T. L., and Mclntyre, R. M. 1997. "A Conceptual Framework for Teamwork Measurement," in *Team performance assessment and measurement: Theory, methods, and applications.*, pp. 19–43.

Dornyei, Z. 1989. "The motivational basis of languagelearningtasks *," *Behavioral science*, (9:2), pp. 131–146.

Dozier, J. B., and Miceli, M. P. 1985. "Potential Predictors of Whistle-Blowing. A Prosocial Behavior Perspective.," *Academy of Management Review*, (10:4), pp. 823–836.

Dubin, J. A., Graetz, M. J., and Wilde, L. L. 1990. “The Effect of Audit Rates on the Federal Individual Income Tax, 1977-1986,” *National Tax Journal*, (43:No.4), pp. 395–409.

Dugo, T. M., and Marshall, T. E. 2007. “The Insider Threat To Organizational Information Security: a Structural Model and Empirical Test,” Auburn University.

Dworkin, T. M., and Baucus, M. S. 1998. “Internal vs. External Whistleblowers: A Comparison of Whistleblowering Processes,” *Journal of Business Ethics*, (17:12), pp. 1281–1298.

Esposito Vinzi, V., Chin, W. W., Henseler, J., and Wang, H. 2010. *Handbook of partial least squares: Concepts, methods and applications*, New York: Springer.

Fama, E. F., and Jensen, M. C. 1983. “Separation of Ownership and Control,” *The Journal of Law and Economics*, (26:2), p. 301.

Faulk, R., and Miller, N. 1992. *A Primer for Soft Modeling*, Akron, OH: University of Akron Press A primer for soft modeling.

Ferrell, O. C., and Gresham, L. G. 1985. “A contingency framework for understanding ethical decision make in marketing,” *Journal of Marketing*, (49:3), pp. 87–96.

Ferrin, D. L., Kim, P. H., Cooper, C. D., and Dirks, K. T. 2007. “Silence speaks volumes: the effectiveness of reticence in comparison to apology and denial for responding to integrity- and competence-based trust violations.,” *The Journal of applied psychology*, (92:4), pp. 893–908.

Fischer, P., and Hughes, J. 1997. “Mutual monitoring and best agency contracts,” *Journal of Institutional and Theoretical Economics (JITE)*, (153), pp. 334–355.

Fornell, C., and Bookstein, F. L. 1982. “Two Structural Equation Models: LISREL and PLS Applied to Consumer Exit-Voice Theory,” *Journal of Marketing Research*, (19:November), pp. 440–452.

Fornell, C., and Larcker, D. F. 1981. “Evaluating Structural Equation Models with Unobservable Variables and Measurement Error.,” *Journal of Marketing Research*, (18:1), pp. 39–50.

Gaertner, K. 1991. *Morality, Rationality, and Efficiency: New Perspectives on Socio-economics M.E. Sharpe, Inc.,* New York.

Geerken, M., and Gove, W. 1975. “Deterrence: Some theoretical considerations,” *Law and Society Review*, (9:3), pp. 497–513.

Gefen, D., Rigdon, E. E., and Straub, D. 2011. “An Update and Extension to SEM Guidelines for Administrative and Social Science Research.,” *MIS Quarterly*, (35:2), pp. iii–xiv.

Gefen, D., Straub, D., and Boudreau, M.-C. 2000. “Structural equation modeling and regression: Guidelines for research practice,” *Communications of AIS*, (4:7), pp. 2–76.

Gefen, D., and Straub, D. W. 2005. “A Practical Guide to Factorial Validity using PLS-GRAPH:Tutorial and Annotated Example,” *Communications of the Association for Information Systems*, (16:1), p. 20.

Gefen, D., Straub, D. W., and Boudreau, M.-C. 2000. “Structural Equation Modeling And

Regression: Guidelines For Research Practice," *Communications of the Association for Information Systems*, (4:7), pp. 1–79.

Gibbs, J. P. 1975. *Crime, Punishment, and Deterrence*, New York: Elsevier.

Goldstein, I. L. 1993. *Training in organizations: Needs assessment, development, and evaluation*, Thomson Brooks/Cole Publishing Co.

Gouldner, A. W. 1957. "Cosmopolitans and Locals: Toward an Analysis of Latent Social Roles.," *Administrative Science Quarterly*, (2:3), pp. 281–306.

Grant, A. M., and Patil, S. V. 2012. "Challenging the norm of self-interest: Minority influence and transitions to helping norms in work units," *Academy of Management Review*, (37:4), Academy of Management, pp. 547–568.

Greenberger, D. B., Miceli, M. P., and Cohen, D. J. 1987. "Oppositionists and group norms: The reciprocal influence of whistle-blowers and co-workers," *Journal of Business Ethics*, (6:7), pp. 527–542.

Grojean, M. W., Resick, C. J., Dickson, M. W., and Smith, D. B. 2004. "Leaders, values, and organizational climate: Examining leadership strategies for establishing an organizational climate regarding ethics," *Journal of Business Ethics*, (55:3), pp. 223–241.

Guo, K. H., and Yuan, Y. 2012. "The effects of multilevel sanctions on information security violations: A mediating model," *Information and Management*, (49:6), Elsevier B.V., pp. 320–326.

Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. 2011. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of Management Information Systems*, (28:2), pp. 203–236.

Hair, J., Black, W., Babin, B., and Anderson, R. 2009. *Multivariate data analysis*, Upper Saddle River, NJ: Prentice Hall.

Hamilton, V. L. 1978. "Who is Responsible? Toward a Social Psychology of Responsibility Attribution," *Social Psychology*, (41:4), pp. 316–328.

Harkins, S. G., and Petty, R. E. 1982. "Effects of Task Difficulty and Task Uniqueness on Social Loafing," *Journal of Personality and Social Psychology*, pp. 1214–1229.

Hayes, A. F. 2009. "Beyond Baron and Kenny: Statistical Mediation Analysis in the New Millennium," *Communication Monographs*, (76:4), pp. 408–420.

Herath, T., and Rao, H. R. 2009a. "Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems*, (18:2), pp. 106–125.

Herath, T., and Rao, H. R. 2009b. "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems*, (47:2), Elsevier B.V., pp. 154–165.

Herscovitch, L., and Meyer, J. P. 2002. "Commitment to organizational change: extension of a three-component model.," *The Journal of applied psychology*, (87:3), pp. 474–487.

Hollinger, R. C., and Clark, J. P. 1982. “Formal and Informal Social Controls of Employee Deviance,” *The Sociological Quarterly*, (23:3), pp. 333–343.

Hollinger, R. C., and Clark, J. P. 1983. “Deterrence in the workplace: perceived certainty, perceived severity, and employee theft.,” *Social forces*, (62:2), pp. 398–418.

Holmström, B. 1982. “Moral hazard in teams,” *The Bell Journal of Economics*, (11:2), pp. 74–91.

Hu, Q., Xu, Z., Dinev, T., and Ling, H. 2011. “Does deterrence work in reducing information security policy abuse by employees?,” *Communications of the ACM*, (54:6), pp. 54–60.

Hunt, S. D., and Vitell, S. 1986. “A General Theory of Marketing Ethics,” *Journal of Macromarketing*, pp. 5–16.

Ifinedo, P. 2012. “Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory,” *Computers and Security*, (31:1), Elsevier Ltd, pp. 83–95.

Ifinedo, P. 2014. “Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition,” *Information and Management*, (51:1), Elsevier B.V., pp. 69–79.

Jaramillo, F., Mulki, J. P., and Solomon, P. 2006. “the Role of Ethical Climate on Salesperson’S Role Stress, Job Attitudes, Turnover Intention, and Job Performance.,” *Journal of Personal Selling & Sales Management*, (26:3), pp. 271–282.

Jarvis, C. B., MacKenzie, S. B., and 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), pp. 199–218.

Johnston, A. C., and Warkentin, M. 2010. “Fear Appeals and Information Security Behaviors: an Empirical Study,” *MIS Quarterly*, (34:3), pp. 549-A4.

Jones, G. 1984. “Task Visibility, Free Riding, and Shirking: Explaining the Effects of Structure and Technology on Employee Behavior.,” *Academy of Management Review*, (9:4), pp. 684–695.

Jong, B. A. D. E. 2010. “How Does Trust Affect the Performance of Ongoing Teams ? the Mediating Role of Reflexivity , Monitoring , and Effort,” *The Academy of Management Journal*, (53:3), pp. 535–549.

Jong, B. A. D. E., De Jong, B. a., and Elfring, T. 2010. “How Does Trust Affect the Performance of Ongoing Teams ? the Mediating Role of Reflexivity , Monitoring , and Effort,” *The Academy of Management Journal*, (53:3), pp. 535–549.

De Jong, B. A., Bijlsma-Frankema, K. M., and Cardinal, L. B. 2014. “Stronger Than the Sum of Its Parts? The Performance Implications of Peer Control Combinations in Teams,” *Organization Science*, (25:6), pp. 1703–1721.

De Jong, B. A., and Dirks, K. T. 2012. “Beyond Shared Perceptions of Trust and Monitoring in Teams: Implications of Asymmetry and Dissensus,” *Journal of Applied Psychology*, (97:2), pp. 391–406.

Jong, B. De, and Bunt, G. Van De. 2008. "Heed , a missing link between trust , monitoring and performance in knowledge intensive teams," *The International Journal of Human Resource Management*, (19:1), pp. 19–40.

Kahan, J. P. 1974. "Rationality, the Prisoner's Dilemma, and Population," *Journal of Social Issues*, (30:4), pp. 189–210.

Kandel, E., and Lazear, E. P. 1992. "Peer Pressure and Partnerships," *Journal of Political Economy*, (100:4), pp. 801–817.

Karahanna, E., Straub, D., and Chervany, N. 1999. "Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs," *MIS quarterly*, (23:2), pp. 183–213.

Katz, D. 1964. "The motivational basis of organizational behavior," *Behavioral Science*, (9:2), pp. 131–146.

Kelley, H. H., and Michela, J. L. 1980. "Attribution theory and research," *Annual Review of Psychology*, (31:1), pp. 457–501.

Kelman, H. C. 1958. "Compliance, identification, and internalization three processes of attitude change," *Journal of Conflict Resolution*, (2:1), pp. 51–60.

Kelman, H. C. 1961. "Processes of Opinion Change," *The Public Opinion Quarterly*, (25:1), pp. 57–78.

Kelman, H. C. 1974. "Further thoughts on the 5 processes of compliance, identification, and internalization," *Perspectives on Social Power*, pp. 125–171.

Kerr, N. L. 1995. "Norms in social dilemmas," *Social Dilemmas. Perspectives on Individuals and Groups*, pp. 31–47.

Kim, W. C., and Mauborgne, R. A. 1993. "Procedural Justice, Attitudes, and Subsidiary Top Management Compliance With Multinationals' Corporate Strategic Decisions.," *Academy of Management Journal*, (36:3), pp. 502–526.

Kinsey, K. 1992. "Effects of IRS Enforcement: An Analysis of Survey Data," in *Why People Pay Taxes*, Ann Arbor: University of Michigan Press, pp. 259–285.

Kirby, S. L., and Davis, M. a. 1998. "A study of escalating commitment in principal-agent relationships: Effects of monitoring and personal responsibility.," *Journal of Applied Psychology*, (83:2), pp. 206–217.

Kirsch, L. J. 1996. "The Management of Complex Tasks in Organizations : Controlling the Systems Development Process," *Organization Science*, (7:1), pp. 1–21.

Klöckner, C. A., and Blöbaum, A. 2010. "A comprehensive action determination model: Toward a broader understanding of ecological behaviour using the example of travel mode choice," *Journal of Environmental Psychology*, (30:4), Elsevier Ltd, pp. 574–586.

Klöckner, C. A., and Matthies, E. 2004. "How habits interfere with norm-directed behaviour: A normative decision-making model for travel mode choice," *Journal of Environmental Psychology*, (24:3), pp. 319–327.

Kohlberg, L. 1981. *The philosophy of moral developmet: Moral stages and the ideal of justice*, San Francisco: Harper and Row.

Kramer, R. M., and Messick, D. M. 1996. "Ethical cognition and the framing of organizatinal dilemmas: Decision makers as intuitive lowyers," in *Codes of conduct: Behavioural research into business ethics*, New York: Russell Sage, pp. 59–85.

Kranz, J. J., and Haeussinger, F. J. 2014. "Why Deterrence is not Enough: The Role of Endogenous Motivations on Employees' Information Security Behavior," *International Conference on Information Systems 2014 Proceedings*.

Kuran, T. 1997. *Private truths, public lies: The social consequences of preference falsification*, Harvard University Press.

Langfred, C. W. 2004. "Too much of a good thing? Negative effects of high trust and individual autonomy in self-managing teams," *Academy of Management Journal*, (47:3), pp. 385–399.

Lee, S. M., Lee, S.-G., and Yoo, S. 2004. "An integrative model of computer abuse based on social control and general deterrence theories," *Information & Management*, (41:6), pp. 707–718.

Leonard, L. N., and Cronan, T. P. 2001. "Illegal, Inappropriate, and Unethical Behavior in an Information Technology Context: A Study to Explain Influences," *Journal of the Association for Information Systems*, (1:1), p. Article 12; 1-31.

Leonard, L. N. K., Cronan, T. P., and Kreie, J. 2004. "What influences IT ethical behavior intentions - Planned behavior, reasoned action, perceived importance, or individual characteristics?," *Information and Management*, (42:1), pp. 143–158.

Lepine, J. A., and Dyne, L. V. 2001. "Peer Responses To Low Performers: an Attributional Model of Helping in the Context of Groups," *Academy of Managment Review*, (26:1), pp. 67–84.

Leung, A. S. M. A. 2008. "Matching ethical work climate to in-role and extra-role behaviors in a collectivist work setting," *Journal of Business Ethics*, (79:1–2), pp. 43–55.

Li, H., Sarathy, R., and Zhang, J. 2010. "Understanding compliance with internet use policy: An integrative model based on command-and-control and self-regulatory approaches," in *International Conference on Information Systems 2010 Proceedings*, p. 181.

Li, H., Sarathy, R., Zhang, J., and Luo, X. 2014. "Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance," *Information Systems Journal*, (24:6), pp. 479–502.

Li, H., Zhang, J., and Sarathy, R. 2010. "Understanding compliance with internet use policy from the perspective of rational choice theory," *Decision Support Systems*, (48:4), pp. 635–645.

Liang, H., Xue, Y., and Wu, L. 2013. "Ensuring Employees' IT Compliance: Carrot or Stick?," *Information Systems Research*, (24:2), pp. 279–294.

Lickel, B. 2000. "Perceptions of Interdependence and Judgments of Collective Responsibility," University of California Santa Barbara.

Lickel, B., Schmader, T., and Hamilton, D. L. 2003. "A case of collective responsibility: who else was to blame for the Columbine high school shootings?," *Personality and social psychology* *bulletin*, (29:2), pp. 194–204.

Liu, C. Z., Zafar, H., and Au, Y. a. 2014. “Rethinking FS-ISAC: An IT Security Information Sharing Network Model for the Financial Services Sector,” *Communications of the Association for Information Systems*, (34), p. Article 2.

Lohmöller, J.-B. 1989. *Latent variable path modeling with partial least squares*, Heidelberg: Physica-Verlag.

Loughry, M. L. 2010. “Peer control in organizations,” in *Organizational control*, New York: Cambridge University Press, pp. 324–362.

Loughry, M. L., and Tosi, H. L. 2008. “Performance Implications of Peer Monitoring,” *Organization Science*, (19:6), pp. 876–890.

MacKinnon, D. P. 2008. *Introduction to statistical mediation analysis*, Routledge.

Malhotra, Y., Galletta, D. F., and Kirsch, L. J. 2008. “How Endogenous Motivations Influence User Intentions: Beyond the Dichotomy of Extrinsic and Intrinsic User Motivations,” *Journal of Management Information Systems*, (25:1), pp. 267–300.

Marks, M. A. 2001. “A Temporally Based Framework and Taxonomy of Team Processes,” *The Academy of Management Review*, (26:3), pp. 356–376.

Marks, M. A., and Panzer, F. J. 2004. “The Influence of Team Monitoring on Team Processes and Performance,” *Human Performance*, (17:1), pp. 25–41.

Mathieson, K., Peacock, E., and Chin, W. W. 2001. “Extending the technology acceptance model: the influence of perceived user resources,” *Data Base for Advances in Information Systems*, (32:3), ACM, pp. 86–112.

Mathieu, J. E., and Zajac, D. M. 1990. “A review and meta-analysis of the antecedents, correlates, and consequences of organizational commitment.,” *Psychological Bulletin*, (108:2), pp. 171–194.

May, L. 1987. *The Morality of Groups*, Notre Dame: Notre Dame Press.

McCallum, D. M., Harring, K., Gilmore, R., Drenan, S., Chase, J. P., Insko, C. A., and Thibaut, J. 1985. “Competition and cooperation between groups and between individuals,” *Journal of Experimental Social Psychology*, (21:4), pp. 301–320.

McGrath, R. G. 2001. “Exploratory learning, innovative capacity, and managerial oversight,” *Academy of Management Journal*, (44:1), pp. 118–131.

McKay, P. F., Avery, D. R., and Morris, M. a. 2009. “A tale of two climates: Diversity climate from subordinates’ and managers’ perspectives and their role in store unit sales performance,” *Personnel Psychology*, (62:4), pp. 767–791.

McNeely, B. L., and Meglino, B. M. 1994. “The Role of Dispositional and Situational Antecedents in Prosocial Organizational Behavior: An Examination of the Intended Beneficiaries of Prosocial Behavior,” *Journal of Applied Psychology*, (79:6), pp. 836–844.

Messick, D. M. 1999. “Alternative logics for decision making in social settings,” *Journal of*

Economic Behavior & Organization, (39:1), pp. 11–28.

Meyer, J. P. A., Allen, N. J. and, and Jean, N. 1997. *Commitment in the workplace*, Sage Publications.

Meyer, J. P., and Alien, N. J. 1984. “Testing the ‘side-bet theory’ of organizational commitment: Some methodological considerations,” *Journal of Applied Psychology*, (69:3), pp. 372–378.

Meyer, J. P., and Alien, N. J. 1991. “A three-component conceptualization of organizational commitment,” *Human Resource Management Review*, (1:1), pp. 61–89.

Meyer, J. P., Becker, T. E., and Vandenberghe, C. 2004. “Employee commitment and motivation: a conceptual analysis and integrative model.,” *The Journal of Applied Psychology*, (89:6), pp. 991–1007.

Meyer, J. P., and Herscovitch, L. 2001. “Commitment in the workplace: Toward a general model,” *Human Resource Management Review*, (11:3), pp. 299–326.

Meyer, R. D., Dalal, R. S., and Hermida, R. 2010. “A Review and synthesis of situational strength in the organizational sciences,” *Journal of Management*, (36:1), pp. 121–140.

Miceli, M. P., and Near, J. P. 1984. “The relationships among beliefs, organizational position, and whistle-blowing status: A discriminant analysis,” *Academy of Manaogement Journal*, (27:4), pp. 687–705.

Miceli, M. P., and Near, J. P. 1985. “Characteristics of Organizational Climate and Perceived Wrongdoing Associated With Whistle-Blowing Decisions,” *Personnel Psychology*, (38:3), pp. 525–544.

Mischel, W. 1977. “The interaction of person and situation,” *Personality at the cross-roads: Current issues in interactional psychology*, pp. 333–352.

Mourali, M., Laroche, M., and Pons, F. 2005. “Antecedents of Consumer Relative Preference for Interpersonal Information Sources in Pre-Purchase Search,” *Journal of Consumer Behaviour*, (4:5), pp. 307–318.

Mourali, M., and Yang, Z. 2013. “The Dual Role of Power in Resisting Social Influence,” *Journal of Consumer Research*, (40:3), pp. 539–554.

Mowday, R. T. 1998. “Reflections on the study and relevance of organizational commitment,” *Human Resource Management Review*, (8:4), pp. 387–401.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and 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), Nature Publishing Group, pp. 126–139.

Nagin, D. S., and Pogarsky, G. 2001. “Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence,” *Criminology*, (39:4), Wiley Online Library, pp. 865–892.

Norris-Watts, C., and Levy, P. E. 2004. “The mediating role of affective commitment in the relation of the feedback environment to work outcomes,” *Journal of Vocational Behavior*, (65:3), pp. 351–365.

Nunnally, J. C., and Bernstein, I. 1994. *Psychometric Theory*, (Vol. 3), McGraw-Hill, New York.

Nunnally, J. C., and Bernstein, I. H. 1994. *Psychometric Theory, 3rd edn*, McGraw-Hill, New York.

O'Reilly III, C., and Chatman, J. 1986. "Organizational commitment and psychological attachment: the effects of compliance, identification, and internalization on prosocial behavior," *Journal of Applied Psychology*, (71:3), pp. 492–499.

Olson, J. M., and Maio, G. R. 2003. *Attitudes in Social Behavior Handbook of Psychology, Volume V: Personality and Social Psychology*, (Vol. 5).

Opp, K.-D. 1982. "The evolutionary emergence of norms.," *British Journal of Social Psychology*, (21:2), pp. 139–149.

Organ, D. W. 1990. "Motivational Basis of Organizational Citizenship Behavior," *Research in Organizational Behavior*, (12:1), pp. 43–72.

Osterhus, T. L. 1997. "Pro-social consumer influence strategies: When and how do they work?," *Journal of Marketing*, (61:4), pp. 16–29.

Osterman, P. 2000. "Work reorganization in an era of restructuring: Trends in diffusion and effects on employee welfare," *Industrial and Labor Relations Review*, pp. 179–196.

Ouchi, W. 1979. "A conceptual framework for the design of organizational control mechanisms," in *Readings in Accounting for Management Control*, Springer, pp. 63–82.

Oz, E. 2001. "Organizational commitment and ethical behavior: An empirical study of information system professionals," *Journal of Business Ethics*, (34:2), pp. 137–142.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior towards IS Security Policy Compliance," in *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, p. 1561.

Paolacci, G., Chandler, J., and Ipeirotis, P. 2010. "Running experiments on amazon mechanical turk," *Judgment and Decision making*, (5:5), pp. 411–419.

Parboteeah, K. P., Chen, H. C., Lin, Y.-T., Chen, I.-H., Lee, A. Y.-P., and Chung, A. 2010. "Establishing Organizational Ethical Climates: How Do Managerial Practices Work?," *Journal of Business Ethics*, (97:4), pp. 599–611.

Park, C., and Lessig, V. 1977. "Students and housewives: Differences in susceptibility to reference group influence," *Journal of Consumer Research*, (4:2), pp. 102–110.

Parker, D. B. 1998. *Fighting Computer Crime: A New Framework for Protecting Information*, John Wiley & Sons, Inc.

Paternoster, R., and Simpson, S. 1996. "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime," *Law and Society Review*, (30:3), pp. 549–584.

Perugini, M., Gallucci, M., Presaghi, F., and Ercolani, A. P. 2003. "The Personal Norm of Reciprocity," *European Journal of Personality*, (17:4), pp. 251–283.

Petter, S., Straub, D., and Rai, A. 2007. "Specifying formative constructs in information systems research," *MIS Quarterly*, (31:4), pp. 623–656.

Pillutla, M. M., and Chen, X.-P. 1999. "Social Norms and Cooperation in Social Dilemmas: The Effects of Context and Feedback," *Organizational Behavior and Human Decision Processes*, (78:2), pp. 81–103.

Piquero, A., and Tibbetts, S. 1996. "Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: Toward a more complete model of rational offending," *Justice Quarterly*, (13:3), pp. 481–510.

Podsakoff, P. M. 2000. "Organizational Citizenship Behaviors: A Critical Review of the Theoretical and Empirical Literature and Suggestions for Future Research," *Journal of Management*, (26:3), pp. 513–563.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. "Common method biases in behavioral research: a critical review of the literature and recommended remedies.," *The Journal of applied psychology*, (88:5), American Psychological Association, pp. 879–903.

Podsakoff, P. M., MacKenzie, S. B., Podsakoff, N. P., and Lee, J. Y. 2003. "The mismeasure of man(agement) and its implications for leadership research," *Leadership Quarterly*, pp. 615–656.

Poll, H. 2015. "VORMETRIC INSIDER Trends and Future Directions in Data Security.,"

Posey, C., and Roberts, T. 2013. "Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors," *MIS quarterly*, (37:4), pp. 1189–1210.

Posey, C., Roberts, T. L., and Lowry, P. B. 2015. "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets," *Journal of Management Information Systems*, (57:November), pp. 338–349.

Posner, B. Z. B. 1992. "Person-Organization Values Congruence: No Support for Individual Differences as a Moderating Influence," *Human Relations*, (45:4), pp. 351–361.

Pratt, T., Cullen, F., and Blevins, K. 2006. "The empirical status of deterrence theory: A meta-analysis," in *Taking Stock: The Status of Criminological Theory*, New Brunswick, NJ: Transaction Publishers.

PwC. 2015. "Managing cyber risks in an interconnected world.,"

Rand, D. G. 2012. "The promise of Mechanical Turk: How online labor markets can help theorists run behavioral experiments," *Journal of Theoretical Biology*, (299), Elsevier, pp. 172–179.

Rashotte, L. 2007. "Social influence," *The blackwell encyclopedia of social psychology*, (9), pp. 562–563.

Reichers, A., and Schneider, B. 1990. "Climate and culture: An evolution of constructs," *Organizational climate and culture*, pp. 5–39.

Reno, R. R., Cialdini, R. B., and Kallgren, C. a. 1993. "The transsituational influence of social norms.," *Journal of Personality and Social Psychology*, (64:1), pp. 104–112.

Rico, R., Sánchez-Manzanares, M., Gil, F., and Gibson, C. 2008. “Team implicit coordination processes: A team knowledge–based approach,” *Academy of Management Review*, (33:1), pp. 163–184.

Ringle, C., Wende, S., and Becker, J. 2015. “SmartPLS 3,” *SmartPLS GmbH, http://www. smartpls. com*.

Ringle, C., Wende, S., and Will, S. 2005. “SmartPLS 2.0 (M3) Beta, Hamburg.,”

Robinson, P. H., and Darley, J. M. 1995. “Justice, liability, and blame: Community views and the criminal law,” Boulder, CO: Westview Press.

Rothwell, G. R., and Baldwin, J. N. 2007. “Whistle-Blowing and the Code of Silence in Police Agencies: Policy and Structural Predictors,” *Crime & Delinquency*, (53:4), pp. 605–632.

Salancik, G. R., and Pfeffer, J. 1978. “A social information processing approach to job attitudes and task design.,” *Administrative science quarterly*, (23:2), pp. 224–53.

Sanders, J., Hamilton, V. L., Denisovsky, G., Kato, N., Kawai, M., Kozyreva, P., Kubo, T., Matskovsky, M., Nishimura, H., and Tokoro, K. 1996. “Distributing responsibility for wrongdoing inside corporate hierarchies: Public judgments in three societies,” *Law and Social Inquiry-Journal of the American Bar Foundation*, (21), pp. 815–855.

Schneider, B. 1975. “Organizational Climates: An essay,” *Personnel Psychology*, (28), pp. 447–479.

Schwartz, S. H. 1968. “Awareness of Consequences and the Influence of Moral Norms on Interpersonal Behavior,” *Sociometry*, (31:4), pp. 355–369.

Schwartz, S. H. 1973. “Normative explanations of helping behavior: A critique, proposal, and empirical test,” *Journal of Experimental Social Psychology*, (9:4), pp. 349–364.

Schwartz, S. H. 1977. “Normative Influences on Altruism,” *Advances in Experimental Social Psychology*, (10:C), pp. 221–279.

Schwartz, S. H., and Howard, J. a. 1981. “A Normative Decision Making Model of Altruism,” *Altruism and helping behaviour: Social, Personality and Developmental Perspectives*, pp. 189–211.

Schwartz, S. H., and Howard, J. J. a. 1980. “Explanations of the Moderating Effect of Responsibility Denial on the Personal Norm-Behavior Relationship,” *Social Psychology Quarterly*, (43:4), p. 441.

Seifert, D. L. 2006. “The influence of organizational justice on the perceived likelihood of whistle-blowing,” *Washington State University*, Washington State University.

Sewell, G. 1998. “The Discipline of Teams: The Control of Team-Based Industrial Work through Electronic and Peer Surveillance,” *Administrative Science Quarterly*, (43:2), pp. 397–428.

Sheeran, P., and Orbell, S. 1999. “Augmenting the Theory of Planned Behavior: Roles for Anticipated Regret and Descriptive Norms,” *Journal of Applied Social Psychology*, pp. 2107–2142.

Shey, H. 2016. “Understand The State Of Data Security And Privacy: 2015 To 2016,” *Forrester*.

Shin, Y. 2012. “CEO Ethical Leadership, Ethical Climate, Climate Strength, and Collective Organizational Citizenship Behavior,” *Journal of Business Ethics*, (108:3), pp. 299–313.

Shrout, P. E., and Bolger, N. 2002. “Mediation in experimental and nonexperimental studies: new procedures and recommendations,” *Psychological methods*, (7:4), p. 422.

Siponen, M., Pahnila, S., and Mahmood, A. 2006. “Factors influencing protection motivation and IS security policy a compliance,” *2006 Innovations in Information Technology, IIT Dubai, United Arab Emirates,* p. 5.

Siponen, M. T., Pahnila, S., and Mahmood, M. A. 2010. “Compliance with Information Security Policies : An Empirical Investigation,” *IEEE Computer Society*, pp. 64–71.

Siponen, M., and Vance, A. 2010. “Neutralization: new insights into the problem of employee information systems security policy violations,” *MIS Quarterly*, (34:3), pp. 487-A12.

Siponen, and T., M. 2000. “A conceptual foundation for organizational information security awareness,” *Information Management & Computer Security*, (8:1), pp. 31–41.

Smith, C. A., Organ, D. W., and Near, J. P. 1983. “Organizational Citizenship Behavior: Its Nature and Antecedents,” *Journal of Applied Psychology*, (68:4), pp. 653–663.

Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. 2014. “Variables influencing information security policy compliance: A systematic review of quantitative studies,” *Information Management & Computer Security*, (22:1), pp. 42–75.

Son, J.-Y. 2011. “Out of fear or desire? Toward a better understanding of employees’ motivation to follow IS security policies,” *Information & Management*, (48:7), pp. 296–302.

Stanton, J. M., Stam, K. R., Guzman, I., and Caledra, C. 2003. “Examining the linkage between organizational commitment and information security,” *SMC’03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme - System Security and Assurance (Cat. No.03CH37483)*, (3), Ieee, pp. 2501–2506.

Staub, E. 1972. “Instigation to Goodness: The Role of Social Norms and Interpersonal Influence,” *Journal of Social Issues*, (28:3), pp. 131–150.

Staub, E. 1978. *Positive social behavior and morality Academic Press*, (Vol. 1).

Staw, B. M. 1984. “Organizational Behavior: A Review and Reformulation of the Field’s Outcome Variables,” *Annual review of psychology*, (35:1), pp. 627–666.

Steg, L., and de Groot, J. 2010. “Explaining prosocial intentions: testing causal relationships in the norm activation model.,” *The British journal of social psychology*, (49:Pt 4), pp. 725–743.

Stern, P. C., Dietz, T., Abel, T., Guagnano, G. a., and Kalof, L. 1999. “A value-belief-norm theory of support for social movements: The case of environmentalism,” *Human Ecology Review*, (6:2), pp. 81–97.

Stewart, G. L., Courtright, S. H., and Barrick, M. R. 2012. “Peer-based control in self-managing teams: Linking rational and normative influence with individual and group performance.,” *Journal of Applied Psychology*, (97:2), pp. 435–447.

Strahan, R., and Gerbasi, K. C. 1972. “Short, homogeneous versions of the Marlowe-Crowne Social Desirability Scale,” *Journal of Clinical Psychology*, (28:2), pp. 191–193.

Straub, D. W. 1989. “Validating instruments in MIS research,” *MIS Quarterly*, (13:2), pp. 147–169.

Straub, D. W. 1990. “Effective IS security: An empirical study,” *Information Systems Research*, (1:3), pp. 255–276.

Straub, D. W. J., and Nance, W. D. 1990. “Discovering and Disciplining Computer Abuse in Organizations: A Field Study,” *MIS Quarterly*, (14:March), pp. 45–60.

Straub, D. W., and Welke, R. J. 1998. “Coping With Systems Risk: Security Planning Models for Management Decision Making,” *MIS Quarterly*, (22:4), pp. 441–469.

Sunstein, C. R. 1996. “Social Norms and Social Roles,” *Columbia Law Review*, (96:4), pp. 903–968.

Sutherland, E., Cressey, D., and Luckenbill, D. 1992. *Principles of criminology*, Rowman & Littlefield.

Sutinen, J. G., and Kuperan, K. 1999. “A Socio-Economic Theory of Regulatory Compliance,” *International Journal of Social Economics*, (2:3), pp. 174–193.

Tenbrunsel, A. E., and Messick, D. M. 1999. “Sanctioning Systems, Decision Frames, and Cooperation,” *Administrative Science Quarterly*, (44:4), pp. 684–707.

Thibaut, J., and Kelley, H. 1959. *The social psychology of groups.*, Oxford: John Wiley The social psychology of groups.

Thøgersen, J. 1999. “The ethical consumer. Moral norms and packaging choice,” *Journal of Consumer Policy*, (22:4), pp. 439–460.

Thomas, T. P. 2013. “The Effect of Personal Values , Organizational Values , and Person-Organization Fit on Ethical Behaviors and Organizational Commitment Outcomes among Substance Abuse Counselors : A Preliminary Investigation,” University of Iowa.

Thompson, J. 1967. *Organizations in action: Social science bases of administrative theory*, New York: McGraw-Hill.

Thompson, R. L., Higgins, C. H., and Howell, J. M. 1991. “Personal Computing: Towards a Conceptual Model of Utilization,” *MIS Quarterly*, (15:1), pp. 125–143.

Thong, J. 1999. “An integrated model of information systems adoption in small businesses,” *Journal of Management Information Systems*, (15:4), pp. 187–214.

Thong, J., and Yap, C. 1995. “CEO Characteristics, Organizational Characteristics and Information Technology Adoption in Small Businesses,” *Omega*, (23:4), pp. 429–442.

Tittle, C. R. 1980. *Sanctions and Social Deviance: The Question of Deterrence*.

Torgler, B. 2002. “Speaking to theorists and searching for facts : tax morale,” *Journal of Economic*

Surveys, (16:5), pp. 657–683.

Trevino, L. K. 1986. “Ethical Decision Making in Organizations: A Person-Situation Interactionist Model.,” *Academy of Management Review*, (11:3), pp. 601–617.

Trevino, L. K., and Victor, B. 1992. “Peer reporting of unethical behavior: A social context perspective.,” *Academy of Management Journal*, (35:1), pp. 38–64.

Trevino, L. K., and Weaver, G. R. 2001. “Organizational justice and ethics program‘ follow-through’: influences on employees´ harmful and helpful behavior,” *Business Ethics Quarterly*, (11:4), pp. 651–671.

Tyler, T. R. 1990. *Why People Obey the Law*, New Haven: Yale University Press.

Tyler, T. R. 2006. “Psychological perspectives on legitimacy and legitimation.,” *Annual review of psychology*, (57), pp. 375–400.

Tyler, T. R. 2009. “Self-Regulatory Approaches to White-Collar Crime: The Importance of Legitimacy and Procedural Justice,” in *The Criminology of White-Collar Crime*, New York, NY: Springer, pp. 195–217.

Tyler, T. R., and Blader, S. L. 2005. “Can Businesses Effectively Regulate Employee Conduct? the Antecedents of Rule Following in Work Settings.,” *Academy of Management Journal*, (48:6), pp. 1143–1158.

Vance, A., and Siponen, M. 2010. “Why do employees violate is security policies? insights from multiple theoretical perspectives,” University of Oulu.

Vance, A., Siponen, M., and Pahnila, S. 2012. “Motivating IS security compliance: Insights from Habit and Protection Motivation Theory,” *Information and Management*, (49:3–4), Elsevier B.V., pp. 190–198.

Vance, A., and Siponen, M. T. 2012. “IS Security Policy Violations,” *Journal of Organizational and End User Computing*, (24:1), pp. 21–41.

Vandenbergh, M. P. 2005. “Order Without Social Norms: How Personal Norm Activation Can Protect the Environment,” *Northwestern University Law Review*, (99:3), pp. 1101–1166.

Verizon. 2016. “2016 Data Breach Investigations Report,” *Verizon Business Journal*.

Victor, B., Trevino, L.K. and Shapiro, D. L. 1993. “Whistle Blowing of Unethical Behaviour: The Influence of Justice Evaluations and Social Context Factor,” *Journal of Business Ethics*, (12), pp. 253–63.

Victor, B., and Cullen, J. B. 1988. “The organizational bases of ethical work climates,” *Administrative Science Quarterly*, (33:1), pp. 101–125.

Victor, B., Cullen, J. B., Quarterly, A. S., and Global, I. 1988. “The organizational bases of ethical work climates,” *Administrative Science Quarterly*, (33:1), pp. 101–125.

Viswanath Venkatesh , Michael G . Morris , Gordon B . Davis, F. D. . D., Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. “User acceptance of information technology: Toward a unified view,” *MIS Quarterly*, (27:3), pp. 425–478.

Wang, J., Gupta, M., and Rao, H. R. 2015. "Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications," *MIS Quarterly*, (39:1), pp. 91-U491.

Wang, J., Yang, Z., and Bhattacharjee, S. 2011. "Same Coin, Different Sides: Differential Impact of Social Learning on Two Facets of Music Piracy," *Journal of Management Information Systems*, (28:3), pp. 343–384.

Weick, K. 1995. *Sensemaking in organizations*, Newbury Park, CA: Sage.

Welbourne, T. M., Balkin, D. B., and Gomez-Mejia, L. R. 1995. "Gainsharing and Mutual Monitoring: a Combined Agency-Organizational Justice Interpretation.," *Academy of Management Journal*, (38:3), pp. 881–899.

Welbourne, T. M., and Ferrante, C. J. 2008. "To Monitor or Not to Monitor: A Study of Individual Outcomes From Monitoring One's Peers Under Gainsharing and Merit Pay," *Group & Organization Management*, (33), pp. 139–162.

Wenzel, M. 2004. "The social side of sanctions: personal and social norms as moderators of deterrence.," *Law and human behavior*, (28:5), pp. 547–67.

Willison, R., and Warkentin, M. 2009. "Motivations for employee computer crime: Understanding and addressing workplace disgruntlement through the application of organisational justice," *IFIP TC 8 International Workshop on Information Systems Security Research*, (1), pp. 127–144.

Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: an Expanded View of Employee Computer Abuse," *Mis Quarterly*, (37:1), pp. 1–20.

Wold, H. 1982. "Soft modelling: the basic design and some extensions," in *Systems Under Indirect Observation: Causality, Structure and Prediction, Part II*, (K.G. Jöres.), Amesterdam: North Holland, pp. 1–53.

Woon, I. M. Y., Tan, G. W., and Low, R. T. 2005. "A protection motivation theory approach to home wireless security," *Twenty-Sixth International Conference on Information Systems*, pp. 367–380.

Wrong, D. H. 1961. "The Oversocialized Conception of Man in Modern Sociology," *American Sociological Review*, (26:2), pp. 183–193.

Wu, Y., Guynes, C., and Windsor, J. 2012. "Security Awareness Programs," *Review of Business Information Systems*, (16:4), pp. 165–168.

Wyld, D. C., and Jones, C. A. 1997. "The Importance of Context: The Ethical Work Climate Construct and Models of Ethical Decision Making -- An Agenda for Research," *Journal of Business Ethics*, (16:4), pp. 465–472.

Yang, Z., and Laroche, M. 2011. "Parental responsiveness and adolescent susceptibility to peer influence: A cross-cultural investigation," *Journal of Business Research*, (64:9), pp. 979–987.

Yang, Z., Schaninger, C. M., and Laroche, M. 2013. "Demarketing teen tobacco and alcohol use: Negative peer influence and longitudinal roles of parenting and self-esteem," *Journal of*

Business Research, (66:4), pp. 559–567.

Yang, Z., Wang, J., and Mourali, M. 2015. “Effect of peer influence on unauthorized music downloading and sharing: The moderating role of self-construal,” *Journal of Business Research*, (68:3), pp. 516–525.

Yazdanmehr, A., and Wang, J. 2016. “Employees’ information security policy compliance: A norm activation perspective,” *Decision Support Systems*, (92), pp. 36–46.

Zhao, X., and Xue, L. 2009. “A Framework of Using Captive Insurance to Streamline IT Control and Compliance Management,” *Journal of Information Privacy & Security*, (5:3), p. 27.