Spring 5-2020

Measuring the Onlooker Effect in Information Security Violations

Sahar Farshadkhah

MEASURING THE ONLOOKER EFFECT

IN INFORMATION SECURITY

VIOLATIONS

by

Sahar Farshadkhah, M.S.

A Dissertation Presented in Partial Fulfillment
of the Requirements of the Degree
Doctorate of Business Administration

COLLEGE OF BUSINESS
LOUISIANA TECH UNIVERSITY

May 2020

LOUISIANA TECH UNIVERSITY

GRADUATE SCHOOL

February 27, 2020
Date of dissertation defense

We hereby recommend that the dissertation prepared by

Sahar Farshadkhah, M.S.

entitled **Measuring the Onlooker Effect in Information Security Violations**

be accepted in partial fulfillment of the requirements for the degree of

Doctor of Business Administration, Computer Information Systems Concentration

Dr. Thomas F. Stafford, Supervisor of Dissertation Research

Dr. T. Selwyn Ellis,
Head of Computer Information Systems

Members of the Doctoral Committee:
Dr. Craig Van Slyke
Dr. Bryan Fuller

Approved:

Christopher Martin
Dean of Business

Approved:

Ramu Ramachandran

Ramu Ramachandran
Dean of the Graduate School

ABSTRACT

Todays' organizations need to be ensured that their critical information is secure, not leaked, and inadvertently modified. Despite the awareness of organizations and their investment in implementing an information security management plan, information security breaches still cause financial and reputational costs for organizations. A recent report of the Ponemon Institute for 2019 showed that the global cost and frequency of data breach increased, and negligent insiders are the root cause of most incidents. Many insider threats to cybersecurity are not malicious but are intentional. Specifically, more than 60 percent of reported incidents in 2019 were due to negligent or inadvertent employees or contractors (Ponemon Institute 2020). Many behavioral cybersecurity research projects investigate factors that influence mitigating information security violations, but still, there is a need to have a better understanding of behavioral factors. One of these factors is the perception of being overseen by onlookers who are organization members to whom one's security policy violations are visible, but who are not directly involved in the behavior.

This study examines the onlooker effect through the lens of Sociometer Theory and Affective Events Theory, which were used to investigate the impact of the perception of being overseen in a workplace on an intention to violate information security policies. In addition, this study tests the hypothesis that individuals under this situation experience different negative affective responses. Finally, this research tests the hypothesis that perceived onlooker threat intensifies these relationships by examining its moderating influence.

An experimental vignette study was conducted with the Qualtrics platform with the currently employed population who are aware of information security policies in their organizations to determine responses to treatment conditions. The results suggested that the interaction of the perceived presence of onlookers and perceived onlooker threat results in experiencing negative affective responses such as shame, guilt, fear, and embarrassment. Moreover, the results showed that employees experiencing fear, guilt, or embarrassment are less intended to violate information security policies.

Overall, this research the understanding of the onlooker effect and the essential role of perceived onlooker threat. This study has substantial theoretical and practical implications for information security scholars and practitioners.

APPROVAL FOR SCHOLARLY DISSEMINATION

The author grants to the Prescott Memorial Library of Louisiana Tech University the right to reproduce, by appropriate methods, upon request, any or all portions of this Dissertation. It is understood that “proper request” consists of the agreement, on the part of the requesting party, that said reproduction is for his personal use and that subsequent reproduction will not occur without written approval of the author of this Dissertation. Further, any portions of the Dissertation used in books, papers, and other works must be appropriately referenced to this Dissertation.

Finally, the author of this Dissertation reserves the right to publish freely, in the literature, at any time, any or all portions of this Dissertation.

Author ______________________________

Date ______________________________

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

In today’s digitally-driven market, the effective use of information system is essential for the long-term success of any organization. The increase in the usage of information systems by organizations makes the importance of information security paramount. Todays’ organizations need to be ensured that their critical information is secure, not leaked, and inadvertently modified (D’Arcy and Hovav 2007).

Despite the awareness of organizations about the importance of information security and investing more in defining, deployment and enforcement of information security policies, information security breaches still cause financial and reputational costs for organizations. Security policies refer to “a set of formalized procedures, guidelines, roles and responsibilities to which employees are required to adhere to safeguard and use properly the information and technology resources of their organizations” (Lowry and Moody 2015, p.434). Even in the organizations with information security policies and staff, employees violations of information security policies are mostly because of negligence or ignorance of the information security policies on the part of employees (Vroom and Von Solms 2004).

A recent report of Ponemon Institute for 2018 showed that the global cost of data breach increased and the average total cost in the United States was $7.91 million (Ponemon Institute 2018). Reported security breach incidents were the result of some intentional or unintentional actions by people within the organizations (Hu et al. 2012; Warkentin and Willison 2009). The Global State of Information Security Survey (GSISS) 2018 reported that current employees remain the top source of security incidents while incidents attributed to hackers, competitors and other outsiders have decreased (PwC 2017). Moreover, Ponemon Institute (2018) found that forty-eight percent of data breaches were caused by malicious and criminal attacks and twenty-seven were the results of human errors and negligence. To overcome these insider-based information security breaches, the use of deterrents is widely advocated by both practitioners and scholars (David 2002; Kankanhalli et al. 2003).

Different factors have been identified in order to overcome the information security violations and enhance the effectiveness of information security policies in organizations, such as use of sanctions (Bulgurcu et al. 2010; D’Arcy and Herath 2011; Herath and Rao 2009), fear appeals (Boss et al. 2009; Johnston and Warkentin 2010a), self-efficacy (Boss et al. 2009; Bulgurcu et al. 2010), etc. Despite the advocates of practitioners and researchers on the importance of some of these factors, still there is a lack in understanding the behavioral aspect of information security. One of the potential factors that has not yet been studied is the violator’s perception of being overseen by onlookers in the workplace when contemplating a behavior that violates the information security policies, and the subsequent influence that being seen has on mediating potential violations.

Prior work studied different information security violations. Siponen and Vance (2010) reported that the most frequent information security policy violations include practices such as failing to lock or log out of workstations, writing down personal passwords in visible places, sharing passwords with colleagues or friends, or copying sensitive data to insecure USB devices. This study argues that the perception of the presence of onlooker(s) at the time of violating the information security policy, may result in the adjustment of the violator's behavior. Individuals are vulnerable to the other's perceptions in their groups of association (Cialdini et al. 1976) and this study seeks to examine how this interpersonal approval dynamic can influence adherence of employees to information security policies specifically when their behavior is discernable by others.

1.1 What is the Onlooker Effect?

Flat organizational structures and the modern streamlined design of companies result in workers rarely being in solitary conditions in the workplace. Most workers have colleagues in their vicinity who may play an inadvertent monitoring role in regard to potentially illicit behaviors and actions. These individuals who are available in a situation and are aware of another individual's action but are not personally involved could be considered as "onlookers." The organizational behavior literature has some examples on how onlookers influence employee's behavior (Cialdini et al. 1976; Nicolini et al. 2011; Tyler 2008) and the Information Technology literature also considers the onlooker effect in the context of technology use (Sergeeva et al. 2017). Prior studies in the context of technology usage at work conceptualize the role of onlookers in terms of their inferences, judgments, and reactions to coworker activities which may then trigger users to reflect on the potential consequences to their contra-policy activities and subsequently cause them to adjust their behaviors when in the presence of others (Sergeeva et al. 2017).

The Onlooker Effect refers to the notion that employees care about what their coworkers think of them and their activities. So, the perceived presence of workplace colleagues may play the role of a deterrent at the time of an information security violation. For that reason, the perception of being watched by onlookers may prevent security policy violations and increase compliance with information security policies in the workplace.

To that end, this study considers onlookers as organization members to whom information security violations are visible, but who are not directly involved in the violation. Accordingly, the role of onlookers as the "Onlooker Effect" is specifically conceptualized as "the adjustment in the violator's behavior in response to the perceived presence of onlookers and their inferences, judgments, or reactions."

1.2 Purpose of the research

A rich stream of research has identified numerous predictors for the prevention of information security violations. However, employee violations of IS security will continue to result in financial and reputational harm to organizations. The research generally indicates that company employees are the top source of information security incidents (PwC 2017). In that respect, considering aspects of violator intentions and considering the specific importance of the situational environment in the workplace may result in having a better understanding of the violator's mindset. This, in turn, may help to provide the basis for better information security policies which will serve to prevent information security incidents.

The Onlooker Effect is a normal aspect of human behavior in social workplace situations. The insight that onlookers can influence security violation behaviors on the part of perpetrators emerged from a focus group study of MBA students in an information security course (Farshadkhah and Stafford 2019). In this encounter, it was discerned that perceptions of the presence of others on the part of potential violators might trigger adjustments of behavior by stimulating feelings and affective drivers resulting in behavioral modification.

The potential impact that the knowledge of being seen has on motivations for engaging in sanctioned activities has not been studied in the context of information security. To that end, the purpose of this research is to study the Onlooker Effect and measure its impact on information security violations.

1.3 Significance of the study

Even though organizations invest substantial resources in order to prevent information security violations, the cost of data breaches increases every year (Ponemon Institute 2018). Numerous studies of information security violations agree on the importance of the role of insiders -- widely considered the weakest link in the organizational security chain (Crossler et al. 2013; Dang-Pham et al. 2014; Warkentin and Willison 2009). For that reason, it is important to understand the factors which may prevent employees from engaging in information security policy violations. Given an expanded understanding of the impact of onlookers on security behavior, this study will contribute to the understanding of violator affective states and motivations, and how they may lead to adjustments in violation behavior.

This research not only introduces the Onlooker Effect to the information security literature but it will also extend the understanding of situational factors that can prevent information security violations. The results of this research will also be useful to managers since it will give them a better understanding of how changes in workplace situational factors may help prevent information security violation behaviors by employees.

1.4 Organization of dissertation

In order to achieve the goal of this dissertation research, this study proceeds as follows: Chapter 2 will specifically discuss the theoretical background and introduce a literature review along with providing the conceptual model of this study and proposing hypotheses. The selected methodology and data collection procedures will be described in Chapter 3. Data analysis and results will be presented in Chapter 4, Chapter 5 will offer discussion of results and conclusions, including implications and future research directions.

CHAPTER 2

LITERATURE REVIEW

The purpose of this chapter is to analyze the relationship between the proposed model of Onlooker Effect and the existing empirical and theoretical literature. The primary goal is to build upon existing work in the IS field for supporting theory and methodology. This study is drawn from, and should be considered part of, the behavioral and organizational IS research which incorporate the reference disciplines of management and criminology.

The effects of onlooker influences on employee's behavior have been considered in the organizational behavior. Cialdini et al. (1976) note that individuals try to represent their connections with positive personal influences since they perceive that the observers of these connections will see them in a similar way. This may have a root in a desirability effect in terms of both self-image and social image (Cialdini et al. 1976). Tyler (2008) used the "sociometer model" to discuss the influence of peers and their visibility on the process of monitoring for relational value cues and subsequent behavioral self-regulation.

In consideration that individuals do not use information technology in a vacuum, it is well to consider the influence of social "others" in workplace technology usage situations. Prior studies consider a variety of "others" such as coworkers (Wang et al. 2013) as well as managers (Vieira da Cunha 2013), and factors of influence can include type of technology, sorts of users, and the social context in which technology usage takes place (Sergeeva et al. 2017). Wang et al. (2013) suggested that identification and internalization are two key social influence mechanisms that explain usage of knowledge management systems; they find strong degrees of influence between levels of organizational hierarchy and limited support for peer influence within hierarchy levels.

Vance et al. (2013) presented an approach for reducing access policy violations by using the theory of accountability. They considered the social presence of another as one of the factors that heighten the individual's perception of accountability. Moreover, Guerin (1986) considered mere presence effects as one such condition for social facilitation effects. Social facilitation, in this case, refers to the effects on behavior caused by the presence of other persons excluding those who might directly interfere, compete, or interact. This social facilitation effect may include increased apprehension due to an expectation that the "socially present" person will at in an evaluative role, hence there would be increased effort on the part of those perceiving social present others to make a good self-presentation to the person present, and an increase in conforming to public and private norms due to increased self-attention caused by the presence of the "other" (Guerin 1986). Lastly, it should be mentioned that the perceived presence of others can have an effect even when the others are not visible (Bond and Titus 1983).

2.1 What is *not* an Onlooker Effect?

In the absence of a specific operationalization, the phrase of "Onlooker Effect" may bring different things to mind among different perceivers. This section will define different permutations of several putative onlooker constructs and explain how they might be different from the specific Onlooker Effect that we are discussing in this study.

2.1.1 Subjective Norms

The Theory of Reasoned Action (TRA) and the related Theory of Planned Behavior (TPB) have articulated normative influences on behavior. In this case, subjective norms refer to the social pressure to perform or not perform a behavior (Ajzen 1991). In the context of information security, Bulgurcu et al. (2010, p.529) defined subjective norms as "an employee's perceived social pressure about compliance with the requirements of the information security policies caused by behavioral expectations of such important referents as executives, colleagues, and managers."

One may be tempted to consider the Onlooker Effect in ways similar to accepted meanings of subjective norms, but they are operationally distinct concepts. When applying subjective norms in security research, the notion typically refers to the degree to which employees perceive that other key personnel expect them to comply with information security rules and policies (D'Arcy and Lowry 2019). In contrast, the Onlooker Effect that we are discussing in this study is based the specific awareness of the presence of workplace peers. As previously noted, these onlookers are able to observe coworker actions but do not directly take part in the activity (Sergeeva et al. 2017).

2.1.2 Social influence

The Onlooker Effect considered in this study is conceptually different from the idea of social influence. Kelman's (1958) social influence theory specifies that an individual's attitudes, beliefs and behaviors are influenced by referent others through three different processes: compliance, identification, and internalization. Compliance occurs when an individual adopts the induced behavior simply because he/she hopes to achieve specific rewards and/or avoid specific punishment. Identification occurs when an individual accepts influence because it is associated with a desired relationship with another person or reference group. Internalization leads an individual to adopt the induced behavior because it is congruent with his/her value system and, as a result, is intrinsically rewarding.

2.1.3 Bystander effect

The bystander effect is a phenomena in social psychology studies and is yet another which, on its face, seems related to what we consider here as the Onlooker Effect. However, as conceptualized in the literature, the bystander effect refers to the idea that an individual’s likelihood of helping another in distress decreases when passive bystanders are present in a critical situation (Fischer et al. 2011). Prior studies used the terms “bystander” and “onlooker” interchangeably, but in this study the definition of the Onlooker Effect is totally distinct from the notion of social influence that mediate the rendering of aid to those in need of help.

2.1.4 Surveillance

Surveillance is a classic concept from the criminology literature. Different types of surveillance include both informal and formal monitoring strategies (Cozens et al. 2005). Formal surveillance is involved with the production of deterrent threats to potential offender by deploying security personnel or surveillance technologies in their near vicinity. Informal surveillance involves limiting opportunities for a potential crime. There is no research that we are aware of that studies informal surveillance in information security, and Onlooker Effect is conceptually difference from either surveillance strategy because it involves employee oversight that is not specifically organized the firm for surveillance purposes. More importantly, the onlookers we consider here are not directly responsible for security monitoring. They have an effect on security violations, but they do not (as yet) constitute an organizationally deployed deterrent effort.

In summary, there are phenomena and constructs that are conceptually similar to the Onlooker Effect, but yet are operationally distinct. As discussed above, in addition to the operational distinctions between similar concepts, there is no literature in the context of information security considering the Onlooker Effect. Table 2-1 summarizes the distinctions between the Onlooker Effect and conceptually related constructs in order to provide a more compelling differentiation.

Table 2-1: What is not an Onlooker Effect

Construct/ Phenomena	**Definition**	**Reference**
Subjective Norms	The social pressure to perform or not perform the behavior.	(Ajzen 1991)
Social Influence	An individual's attitudes, beliefs and behaviors are influenced by referent others through three different processes: compliance, identification, and internalization.	(Kelman 1958)
Bystander Effect	The phenomenon that an individual's likelihood of helping decreases when passive bystanders are present in a critical situation.	(Fischer et al. 2011)
Surveillance	Close watch kept over someone or something.	Merriam-Webster Dictionary

As discussed in Chapter 1, for the purpose of this study onlookers are specifically as organization members for whom information security violation behavior is visible, but who are not directly involved in the behavior. The practical influence of the Onlooker Effect will be the adjustment in a violator's behavior as a result of perceived onlooker presence and the subsequent adjustment of their inferences, judgments, or reactions. Reviewing the available literature also leads to the supposition that there is a need to incorporate violator affective states resulting from the perceived presence of onlookers, as well. The following section discusses its importance in more details.

2.2 What are affective states?

Affect is a critical factor in human behavioral decision making, and in many different social contexts (Zhang 2013). Affect is principal aspect of being human (Zhang 2013) and it impacts various behaviors (Brief 2001; Forgas and George 2001). Prior studies in social psychology, management, and information systems demonstrate that affect is a strong determinant of individual's cognition and behavior and it has more explanatory power than cognition under certain circumstances (Zhang 2013).

Rational decision calculus may not be the only factor impacting violator behaviors; there are also affective states that could influence decisions (Kaufman 1999; Simpson 2000). Zhang (2013) discussed fundamental concepts of affect in the psychology literature that play a role in the development of the construct in the IS field. Table 2-2 summarizes Zhang's points.

Table 2-2: Basic affective concepts (Zhang 2013, p. 251)

Concept	Definition and Characteristics
Core affect	An intrinsic aspect of consciousness that is mental but not cognitive or reflective. Conceptualized as a neurophysiologic state consciously accessible as simple, non-reflective feelings inside oneself. The specific feeling itself may change from time to time, but a person will always have some feeling (core affect) at any moment. Core affect may have no known causes (mood) or it can be linked to stimuli (such as perceptions of affective quality and emotions). It is a primitive concept and fundamental for all affective events.
Stimulus	That which a person responds to. It is a psychological representation, thus can be real, imagined, fictitious, remembered, anticipated, or in forms of virtual reality.
Mood	Prolonged core affect with no stimulus (simple mood) or with quasi-stimulus. It is often regarded as an affective state without a specific stimulus.
Temperament	A characteristic, habitual inclination, or mode of emotional response.
Emotion	An affective state induced by or attributed to a specific stimulus. Emotions typically arise as reactions to situational events and objects in one's environment that are relevant to the needs, goals, or concerns of an individual. Emotion emphasizes a person’s subjective feeling. The feeling is short-lived, existing only as long as the supporting cognition, perceptions, or other elicitors are active, and vanishing as soon as one is no longer in that condition. An emotional episode depicts the complex process of the emotion in responding to a stimulus.
Attitude	A summative evaluation of a stimulus that may help guide behavior regarding that stimulus; can be considered as either a multidimensional construct comprised of cognitive, affective, and behavioral components, or a two-dimensional construct with instrumental (mostly cognitive) and experiential aspects (mostly affective).

Emotion is one of the most complex affective concepts. Emotion refers to interrelated, synchronized changes in the states of all or most of the five organismic subsystems in response to the evaluation of an external or internal stimulus (Scherer 2005). Emotions generate subjective feelings and motivational states with action tendencies. Zhang (2013) asserts that emotions typically arise in reaction to events in an individual’s environment appraised to be relevant to his/her needs, goals, or concerns. These definitions distinguish emotion from other affective states such as feelings or moods. More precisely, feelings are about a single component of the subjective experience process which integrate the central representation of appraisal-driven response organization in emotions (Scherer 2004, 2005).

The complexity of access to the emotional state of an individual has been discussed in prior studies. The emotional state of a person could be deduced form nonverbal behavior such as facial expressions and physiological indicators; however, the subjective experience of a person during an emotional episode could not be measured through available objective methods (Scherer 2005). Given the difficulty of identifying all dimensions of subjective feelings, which reflect the unique experience of being confronted with a specific situation, there is no way to access this information other than to ask the individual to report on the nature of the experience (Scherer 2004).

There are different affective states which violators may experience as a result of the perceived presence of onlookers. Considering the precise definition of different aspects of affect, in the case of the Onlooker Effect, it is reasonable to suppose that the perceived presence of onlookers will influence the emotions of violators, in turn triggering adjustments in violation behaviors.

2.3 Theoretical Background

This study corporates two theories, Sociometer Theory and Affective Event Theory, in order to study the impact of the onlooker in adjustment of violation behaviors in a workplace. Following sections will discuss these two theories in details.

2.3.1 Sociometer Theory

Acceptance by others is a primary determinant of how people get along in life (Leary 2005). The initial idea for sociometer theory in the early 1990s came from an interest in understanding the emotional and behavioral effects of interpersonal acceptance and rejection. Leary in 1990 began to realize that people wish to be evaluated positively because of their desire to be accepted and to belong to groups.

The principal of sociometer theory is a subjective gauge of the degree to which people perceive that they are relationally-valued and socially-accepted by others. This gauge is related to self-esteem, and it characterizes a "reflection of the individual's assessment of the implications of his or her behavior for social inclusion and exclusion." (Leary 1990, p. 227). Sociometer theory differs from most explanations of self-esteem, considering the positive self-image as the output of a cognitive system that monitors interpersonal acceptance and rejection and which offers a description of people's efforts to maintain a minimum degree of social acceptance (Leary 2012).

Baumeister and Leary (1995) suggested that people not only have a strong motivation toward affiliation and group membership but also wish to be accepted rather than rejected by others. Given the vitality of social acceptance, which arises from a psychological system (here, called the "sociometer"), individuals constantly monitor and craft responses to social cues about their putative self-worth. According to this theory, self-esteem, which is monitor or gauge of relational value, has no inherent value to the individual, per se; he behaviors and motives that *appear* to protect self-esteem actually serve to reinforce an individual's relational value in the eyes of others and to subsequently foster positive feelings (Leary 2005).

Seen through the lens of Sociometer theory, situations and events such as failure, rejection, embarrassment, negative evaluations, criticism, and being outperformed by other people serve to decrease self-esteem -- not only because they damage a person’s private self-image but also because the serve to lower one’s relational value and the probability of acceptance by others (Leary 2012, p. 147).

This study applied the aspect of the sociometer theory that emphasized the goal of maintaining self-esteem in motivating actions. This would result in protection of self-image and enhancement of relational, all of which should increase the likelihood of acceptance (Leary 2005; Leary and Baumeister 2000). Seen this way, the fundamental function of the self-esteem system is to monitor and respond to threats to a person’s relational value (Leary 2012). In other words, the “sociometer “helps people to maintain relationships that are aligned with social support by providing a mechanism that monitors other people’s reactions to their personal self-worth.

Taken together, the underlying assumption of sociometer theory is that people need to form and maintain social relationships and utilize an internal cognitive system to monitor these relationships. The sociometer system monitors a person’s interpersonal relationships and motivates subsequent behaviors that support the maintenance of a sufficient level of acceptance by others. This study using the sociometer theory as a theoretical lens to describe the primary influence of the onlooker effect, where the perceived presence of onlookers and their potential judgments and reactions may result in an adjustment of a potential violator’s security behavior.

Under the theory, when an individual detects a possible threat to his/her social acceptance, a conscious analysis of the situation is triggered to find out whether something related to an individual's own characteristic or behavior precipitated the threat. Sociometer theory suggests that an employee will be motivated to avoid negative responses and will expend effort to protect and maintain the quality of relationships, since a denigration of them would threaten their feeling of belongingness and self-esteem at work. To that end, this study argues that the perceived presence of others and its potential negative consequences may reduce the chance of engaging in behaviors that violate workplace norms and policies and subsequently harm the individual's social relationships and image.

2.3.2 Affective Events Theory (AET)

Affective events theory (AET) is a theory that focuses on the importance of work events and affective experiences at work. AET was introduced by Weiss and Cropanzano (1996) as a theoretical discussion of the structure, causes, and consequences of affective experiences at work.

The main idea of AET is that as workers experience events in the workday, their emotional reaction to those events and the related affective experiences they engender will have a direct influence on behaviors and attitudes. The structure of this psychological experience is essential. People can feel angry, frustrated, or joyful, and this can result in widely varying reactions and behavioral implications (Weiss and Cropanzano 1996).

The macro structure of Affective Event Theory (Weiss and Cropanzano 1996) is shown in Figure 2-1. In this structure, the core of AET is the affective experience. Since affect levels fluctuate over time, the causes of such affect could be considered as endogenous constructs (mood cycles or affective dispositions) or exogenous components (affectively relevant events) based on the problem being addressed. The theory also considers the moderating role of dispositions and emphasizes both the direct and indirect influence of work environments on affective experiences. The consequences of affective experiences could be attitudinal and behavioral. Affective-driven behaviors, then, are the direct results of affective experiences and are not mediated by overall attitudes.

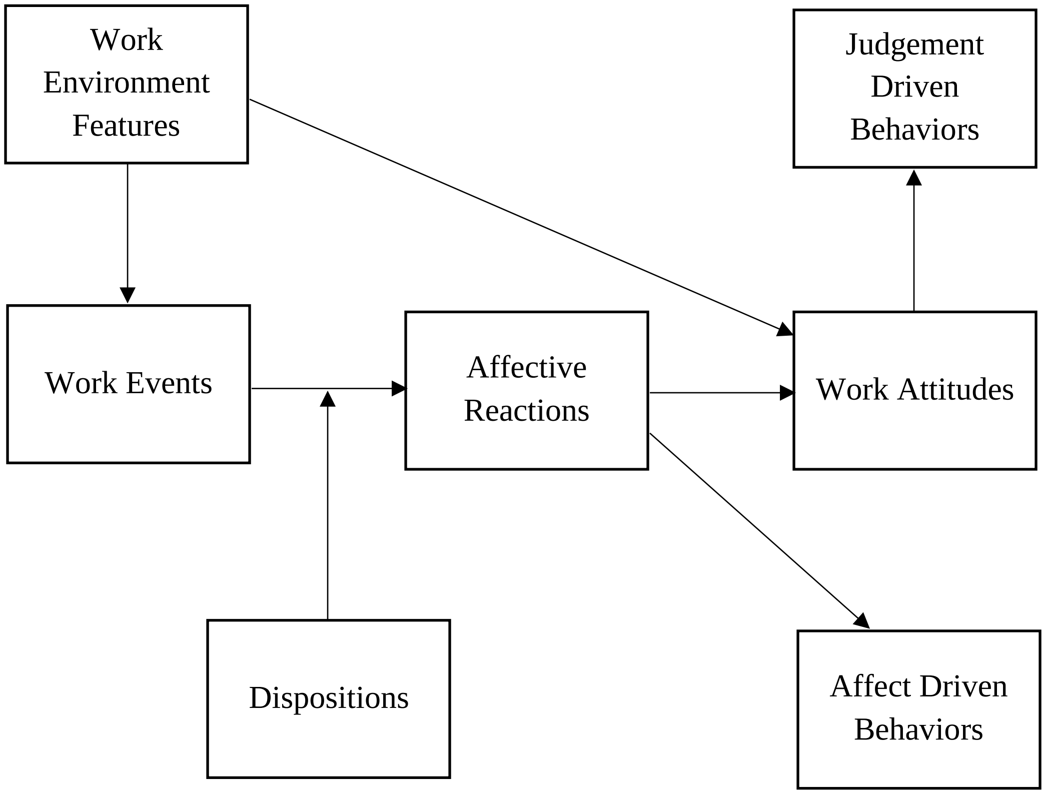


Figure 2-1: Affective Event Theory (Weiss and Cropanzano 1996)

Following the primary emphasis of AET on the role of events as the cause of workplace affective reactions, Weiss and Cropanzano (1996) defined the triggering event as “the idea of change, a change in circumstances, a change in what one is currently experiencing” (p. 31). The perceived presence of onlookers and their ability to see or hear a potential violation behavior is conceptualized as just such an event, based on the conceptualization of Weiss and Cropanzano (1996). They emphasized that work environmental features influence affect primarily by causing affective events to take place, by stimulating recall of such events, or even by causing the worker to imagine such affective events.

Most emotion theories assume that emotional reactions generally begin with an appraisal of an event (Plutchik 1994). According to Weiss and Cropanzano (1996), emotions and moods are each affective states; however, this study specifically considers emotions as affective responses. Frijda (1993) argues that the general awareness of feelings arises from the knowledge of the pleasantness or unpleasantness of an event, which is why experiencing affect is tied to the appraisal of the event, including the case of both people and things. This event appraisal experience results in an action readiness response in order to deal with events in the environment.

The initial appraisal is related to one’s personal goals and values. Both positive and negative goal-relevant events can occur and result in positive and negative emotional reactions. However, Taylor (1991) found that the effects of positive and negative events are not symmetrical, and negative events trigger stronger psychological responses and reactions. Accordingly, this study emphasizes negative affective responses that employees may experience as a result of the perception of the presence of onlookers and subsequent onlooker threats at the time of forming intentions to violate information security policies. Experiencing negative emotions usually leads to specific coping responses (Lazarus 1991). In this sense, then, the affect-driven behavior is the direct response to the affective experiences (Weiss and Cropanzano 1996), and will result in the adjustment to the contemplated act, resulting in avoidance of a violation of information security policy.

AET has been supported in several studies in the management and organizational behavior literature. Pirola-Merlo et al. (2002) evaluated the role of emotions and the value of AET in studies of leadership and found a linkage between workplace events that provided obstacles to team performance and team leader responses to these events. Fisher (2002) studied the effects of real-time affective reactions at work, and found results consistent with AET, subsequently proposing related causes and effects of positive versus negative affect. Fuller et al. (2003) conducted a time series analysis of events, mood, stress, and satisfaction and found that job attitudes and stress varied in direct response to workplace events. Ashton-James and Ashkanasy (2008) applied AET to strategic management and strategic decision-making, suggesting that workplace events elicit affective responses which influence both the content and process of strategic decision-making.

While the role of emotions in the workplace has been receiving more attention from IS scholars, there are few studies that consider AET in technological contexts. Stam and Stanton (2010) investigated the relations between workplace events, emotions, and technology change by combining regulatory focus theory and affective events theory. They demonstrated that employees’ responses to new technology were related to the emotional experiences surrounding events about the deployment of the new technology. Chea and Luo (2009) applied AET in explaining e-service customer post-adoption behaviors such as continuance intentions, complaint behavior, and recommendations to other customers. Their findings support that consideration that e-service customer retention behaviors were determined by perceived site quality and cognitive appraisal of incident handling.

Decisions have been made by individuals in organizations are not always controlled and based on purely cognitive process. The moods and emotions that individual experience in response to positive and negative workplace events have a significant effect on decision making process (Ashton-James and Ashkanasy 2008). Accordingly, when individuals are in a situation to make decision regards to violate information security in order to make their task done, different organizational characteristics may result in experiencing positive or negative emotions which may lead to alteration in their behavior.

2.4 Research model and hypothesis

Considering the Sociometer Theory and Affective Event Theory as the theoretical lenses, the conceptual model was developed through a synthesis of the literature review. This model contains four broad constructs: affective responses, a response to the perception of the presence of onlookers and onlooker threat (deterrence components) and Violation Intent (behavioral intention to engage in violation behavior). These are discussed individually, below.

2.4.1 Affective Responses

A given behavior can result in a range of different emotions. Emotions influence how information is processed, so they are one of the factors that have a potential to impact the decision-making process. Recent studies have identified the potential importance of emotional states on the way people perceive situations and how they make decisions. Kligyte et al. (2013) discussed that emotions influence how people think about ethical problems and make ethical decisions.

Affective Event Theory proposes that when organizational events occur, people react emotionally to them and the resulting affective experiences have a direct impact on their behaviors and attitudes (Weiss and Cropanzano 1996). To better understand AET, it is essential to know what job events or situations might cause employees to experience specific emotions or what type of emotions should be expected to arise in specific circumstances. Answering these questions helps to predict the consequences of particular behaviors related to affective experience.

An affective event refers to an incident that stimulates appraisal of and emotional reaction to a transitory or ongoing job-related agent, object, or occurrence (Basch and Fisher 1998, p. 3). The events could be intra-organizational, such as stress-related workplace events, elements of the physical workplace environment, work-group characteristics, relationships with leaders, or extra-organizational events including but not limited to economic, legal, political, and inter-organizational negotiation events.

Emotion researchers believe that different types of events cause different emotions (Izard 1991) while individuals will feel the same emotions if their appraisal of a given event is same (Lazarus 1966). Basch and Fisher (1998) developed two event-emotion matrices (for positive and negative emotions) by studying common job-related emotions. Event categories include “acts of colleagues,” “acts of managers,” “task problems,” “making mistakes,” “physical situations,” “lack of goal achievements,” etc. A listing of the various categories of job events for positive and negative emotions, per Basch and Fisher, is shown in Table 2-3.

Table 2-3: Job events for positive and negative emotions (Basch and Fisher 1998)

Categories of Job Events for Positive Emotions Experienced	**Categories of Job Events for Negative Emotions Experienced**
Acts of work colleagues	Acts of work colleagues
Acts of management	Acts of management
Goal achievement	Lack of goal achievement
Receiving recognition	Lack of receiving recognition
Acts of customers	Acts of customers
Involvement in challenging tasks	Task problems
Interacting with customers	Making mistakes
Goal progress	Lack of influence or control
Organizational reputation	Company policies
Disconfirmation of Negative Expectations	External environment
Influence or control	Physical situations
Involvement in decision making	Workload
Involvement in planning	Personal problems
Involvement in problem solving	

This study considers the working position of a given employee and the subsequent likelihood of being overseen by onlookers as an event resulting in the experience of negative emotions, in the case of an employee who has an intention to violate information security policies. Accordingly, “acts of colleagues,” “acts of managers,” “making mistakes,” and “physical situation.” Drawn from the above-mentioned Basch and Fisher list are considered as proxies for the affect-generating event in this study. The definition of these negative job events is demonstrated in Table 2-4.

Table 2-4: Definitions of negative job events

Negative job event	**Definition**
Acts of colleagues	Appraised negative behaviors towards oneself or others by work colleagues.
Acts of management	Appraised negative behaviors towards oneself or others by work managers.
Making mistakes	Minor acts resulting in unintended poor consequences.
Physical situation	Situations appraised as physical threats toward the individual while at work.

Emotions have the potential to initiate ethical decision-making processes and to subsequently influence how people think about ethical problems (Kligyte et al. 2013). For purposes of devising an appropriate emotional reaction stimuli for this study, the Negative Event-Emotion Matrix (Basch and Fisher 1998, p. 10) has been used. Among the different negative emotions categorized in this matrix, embarrassment and fear were the emotions specifically identified as causing the requisite experienced affective response. Embarrassment and fear were caused most frequently by mistakes and unusual physical situations, respectively. Embarrassment and fear affective-generating events are not quite the same as fear appeals, which have been studied widely in information security behavioral research (e.g., Herath and Rao 2009; Johnston and Warkentin 2010b).

In addition to embarrassment and fear, this study also considered shame and guilt as possible experienced affective responses on the part of employees. There is a wide range of research on shame in criminology research (Ahmed et al. 2001; Braithwaite 1989) and in social and clinical psychology (Lewis 1995; Tangney and Dearing 2003). Shame has been discussed in the information security literature as a specific emotional effect that security policy violators might experience (e.g., Siponen et al. 2012; Siponen and Vance 2010). The role of guilt in social behavior regulation and adjustment of the relationship between self and others has also been discussed by emotional theorists (De Rivera 1984; Scheff 1984).

Although one may compare shame to guilt and embarrassment, these emotions are distinct (Bastin et al. 2016; Tangney et al. 1996; Tangney and Tracy 2012; Tracy and Robins 2004). Shame, guilt and embarrassment are each self-conscious emotion and require self-reflection and self-evaluation. These emotions arise when an individual makes an appraisal of failure to live up to an expectation of or to the standards of the social environment (Tangney and Dearing 2003; Tracy and Robins 2004). The nature of these emotions can cause them to have influences in normative ways that benefit others and the organization (Tangney et al. 2007). The significant difference among these emotions is related to the scope of the appraisal. Shame involves a negative evaluation of the self, whereas guilt involves a negative evaluation of one's behavior, and embarrassment involves negative assessment of the social impressions associated with violations of social conventions (Tangney et al. 1996).

Perceived presence of onlookers and fear

Based on the affective events-emotions matrix (Basch and Fisher 1998), job events related to physical situations could result in the experience of fear in the form of a negative event emotion. Fear is an emotion that has been described as an unpleasant state demanding extreme amounts of effort to overcome, and which is associated with profound uncertainty a given situation (Smith and Ellsworth 1985). Fear is characterized by a person's uncertainty about the ability to escape or avoid an unpleasant outcome. Appraisal theories of emotion have identified various appraisals that are consistently associated with fear, such as danger or threat, low certainty, and a sense of situational control (Lerner and Keltner 2001).

Lerner and Keltner (2000) also demonstrated that fear is positively associated with perceived risk. To that end, this study argues that the perception of being watched and having onlookers around is one of the situations that may result in feeling fear by the violator of information security policy. For these reasons, the study considers a scenario in which an employee had the perception of being overseen by an onlooker at the time of a potential information security policy violation; this given scenario implied the maximal level of uncertainty and risk.

H1: The perceived presence of onlookers will result in the experience of fear by security policy violators.

Fear and Intention to violate information security

The specific behavioral manifestation of fear is avoidance or escape (Lerner and Keltner 2001). People in a state of fear also tend to show a reverse action tendency and demonstrate pessimistic situation appraisals (Lerner and Keltner 2000). Fear signals the presence of an environmental threat, and individuals feeling fear engage in more conscious behavioral monitoring while also tending to assess the associated risk negatively (Lerner et al. 2003).

Fear facilitates in-depth cognitive processing and the consideration of alternative perspectives (Kligyte et al. 2013). Janis (1967) pointed out that when individuals experience negative emotional states caused by fear, they will be motivated to take action by engaging in behavior consistent with alleviating the threat and reducing their fear. Extending from these points, in a situation where an organizational member is contemplating the violation of the information security policy, the perception of being watched will result in the experience of fear which will then push the actor into the danger control process. The danger control process can lead to positive outcomes, ultimately resulting in no violation of information security policies.

H2: The feeling of fear arising from the perceived presence of onlookers will negatively influence intentions to violate information security policies.

Perceived presence of onlooker and shame

Organizational Shame has been defined as “a painful emotion that arises when an employee evaluates a threat to the self when he or she has fallen short of an important standard tied to a work-related identity” (Daniels and Robinson 2019, p. 2450). Different situations in the workplace may result in feeling ashamed. The most common situations based on prior studies relate to performance failure, morality, and engaging in socially inappropriate behavior. For an act to result in organizational shame, the employee must have an appraisal that the behavior has negatively deviated from a standard as seen through the eyes of others and which may be socially visible and/or imagined for purposes of subsequent social judgment (Daniels and Robinson 2019). Also, according to the sociometer model, losses of self-esteem which monitor others’ reactions and the possibility of social exclusion are associated with feeling ashamed (Leary et al. 1995).

Shame will be experienced when one has deviated from a standard as seen through the eyes of others while others could be socially visible, imagined, or generalized as a social judgment (Daniels and Robinson 2019). For that reason, shame is included as one of the feelings and affective responses that violators may experience when they perceive that onlookers have seen them perpetrate a violation of information security policy.

H3: The perceived presence of onlookers will cause security policy violators to experience shame.

Shame and Intention to violate information security

Shame has a unique capability to motivate fundamental changes (Lickel et al. 2014); this may result in critical implications for both the employee and the organization (Daniels and Robinson 2019). Prior studies showed that under different circumstances, shame could lead to constructive behaviors, maladaptive behaviors, or even withdrawal (de Hooge et al. 2010). So, it is essential to understand the role of shame in work-related outcomes and ethical behavior (Murphy and Kiffin-Petersen 2017).

Considering deterrence theory as a theoretical lens, prior studies by Braithwaite (1989), Paternoster and Simpson (1993), Siponen et al. (2012), and Siponen and Vance (2010) investigated shame as a deterrent and they advances this particular affective component as part of an extension of the role of formal and informal sanctions in deterrence theory formulations. Informal sanctions include the disapproval of colleagues or friends for a given action (Paternoster and Simpson 1996). In this sense, shame would refer to a feeling that would arise if others knew of one’s socially undesirable actions (Paternoster and Simpson 1996; Siponen et al. 2012; Siponen and Vance 2010). Prior studies demonstrate that shame, a self-imposed sanction (Grasmick and Bursik 1990; Paternoster and Simpson 1996), plays a potent role as a deterrent and that it also has a negative relationship with an individual’s motivation to perform crimes (Grasmick and Bursik 1990; Nagin and Paternoster 1993). In other words, the more significant the perceived threat of shame, the less the expected utility of crime and the lower the likelihood of occurrence. Consistent with studies on corporate crime, Siponen et al. (2012) found a significant negative effect of shame on software piracy, even when formal sanctions had no deterring effect. Taken together, this suggests the deterrent effect of onlooker-generated shame.

H4: The feeling of shame arising from the perceived presence of onlookers negatively influences intentions to violate information security policies.

Perceived presence of onlooker and embarrassment

Embarrassment is one of the common job-related emotions, and one of the emotions in Fisher's (2000) Job Emotion Scale (JES); it also has been considered in the affective events-emotions matrix by Basch and Fisher (1998). Embarrassment is associated directly with “the response [to] the presence of an audience (real or imagined), in which the person worries about their social image as a result of their behavior being directly witnessed” (Bastin et al. 2016, p.456).

While embarrassment arises mostly from making mistakes, the acts of colleagues and of managers have also been known to cause embarrassment (Basch and Fisher 1998). Sabini et al. (2001) demonstrated that people experience embarrassment when they are involved with the violation of conventions and/or others have reason to think that some flaw of theirs has been revealed to others. Accordingly, embarrassment is included in this study as one of the feelings that violators may experience when they perceive that onlookers have observed them perpetrate a violation of information security policy.

H5: The perceived presence of onlookers will result in the experience of embarrassment by security policy violators.

Embarrassment and Intention to violate information security

Embarrassment has been considered as one of the possible socially-imposed sanctions that decreases the expected utility of crime (Grasmick and Bursik 1990). These authors suggest that embarrassment will be experienced by an actor who engages in a particular behavior/action which might lead significant others to lose respect for him/her. Significant others refer to "friends, family, colleagues, employer, etc., whose opinions about an actor are important [to] that actor (p. 840)". The influence of conscience and significant others upon the potential the actor reduces the expected utility of crime.

Embarrassment is associated with sudden and accidental violations of social conventions, resulting in a motivational response that serves to preserve an individual's social reputation. Taken together, this suggests a hypothetical outcome related to the deterrent effect of onlooker-generated embarrassment and implies that feelings of embarrassment related to the perceived presence of onlookers may mitigate the intention to violate information security policies in the workplace.

H6: Feelings of embarrassment by potential security policy violators will negatively influence intentions to violate information security policies.

Perceived presence of onlooker and guilt

Weiner (1985) characterizes guilt as emerging due to actions of individual volition. Guilt refers feelings experienced when an individual recognizes that he/she has violated a social standard or personally relevant moral position (Kugler and Jones 1992). Guilt has been described as the personality dynamic between normal and deviant behavior.

According to the guilt literature, “in general, guilt is said to follow from acts that violate ethical norms, principals of justice … or moral values. Guilt is accompanied by a feeling of personal responsibility” (Wicker et al. 1983, p.26). Moreover, Izard (1977) concluded that “guilt occurs in a situation which one feels personally responsible” (p. 423) while Hoffman (1973) emphasized one’s cognitive capacity to recognize the consequences that his/her actions have for others, and the subsequent choice to control the behavior. Following these points, this study considers the feeling of guilt as what individuals may feel at the time of undertaking violations of information security policies when onlookers may be watching.

H7: The perceived presence of onlookers will result in experience of guilt by security policy violators.

Guilt and intention to violate information security

Guilt has been considered as one of the several innate emotions that prepare and motivate individuals for appropriate behavior (Kugler and Jones 1992). The role of guilt in social behavior regulation and adjustment of the relationship between self and others has been discussed by emotion theorists (De Rivera 1984; Scheff 1984), with Izard (1977) describing the emergence of guilt as interlinked with a sense of responsibility for social behavior.

According to the negative state relief model (NSRM), higher levels of experienced guilt lead to a higher probability of compliance with the requests of others (Cialdini et al. 1973). Also, since feelings of guilt are uncomfortable, people try to predict its occurrence act in ways that avoid inducing it (Boster et al. 2016). Following these points, since opportunities to comply provide a means of reducing or eliminating this negative affect, this study expects that the emergence of guilt may result in the adjustment of behavior based on acceptable standards, serving to prevent potential violations of the information security policy.

H8: Feelings of guilt by potential security policy violators will negatively influence intentions to violate information security policies.

2.4.2 Security deterrent

In general, deterrence is achieved by providing knowledge about what is unacceptable conduct, and then creating a desire to avoid negative consequences through perceived enforcement against unacceptable conduct (Tittle 1980). Considering security policies as an instance of “organizational laws” (Whitman 2004), these policies will prescribe actions and enforcement and consequently serve to deter information security violations. D’Arcy et al. (2009) suggested that the absence of information security policies may result in misunderstanding of acceptable behaviors and the fallacious conclusions that there might be no enforcement or consequences for violation behavior. On the other side, Vroom and von Solms (2004) discussed that even in organizations with information security policies and staff, employees violations of information security policies are happening which is mostly because of employees ignorance or negligence. Extending from that point, having some informal or situational factor may help to improve the effectiveness of information security policies, resulting in mitigating information security violations. This study proposes the perceived presence of onlookers as one of these factors which may reduce the chance of violating information security policies by employees following social facilitation study by Guerin (1986), findings of Vance et al. (2013) about social presence and its effect on heightening employee’s perception of accountability. Accordingly, it is proposed that the perceived presence of onlookers negatively influences intention to violate information security policies.

H9: The perceived presence of onlookers will negatively influence intentions to violate information security policies.

Prior studies in information security and widely-used deterrence theory posit that at the time of deciding to commit a crime, individuals weigh costs and benefits. Individuals will not commit a crime if they believe that the risk of getting caught is high and penalties will apply (Siponen and Vance 2010). This rational calculus besides the impact of the perceived presence of onlooker on the intention to violate information security policies, shed light on the importance of threat that may come with presence of onlooker. This study considers “Perceived Onlooker Threat” to the extent of whether onlooker report the violation behavior or not. It should be considered that the possibility of being reported by onlooker may inflate the effect of the perceived presence of onlooker on mitigating information security violations and in the same way it may have an impact on violator’s affective responses. Extending from these points, it is proposed that the positive relationship between the perceived presence of onlooker and the considered affective responses are moderated by the onlooker threat. Moreover, the direct effect of the perceived presence of onlookers on information security violation intentions is also moderated by the perceived onlooker threat.

H10a-d: The relationship between the perceived presence of onlookers and affective responses (fear, shame, embarrassment, guilt) is moderated by perceived onlooker threat.

H11: The relationship between the perceived presence of onlookers and intention to violate information security policies is moderated by perceived onlooker threat.

The relationships between these constructs is graphically characterized in the conceptual model proposed for the study, which appears in Figure 2-2.

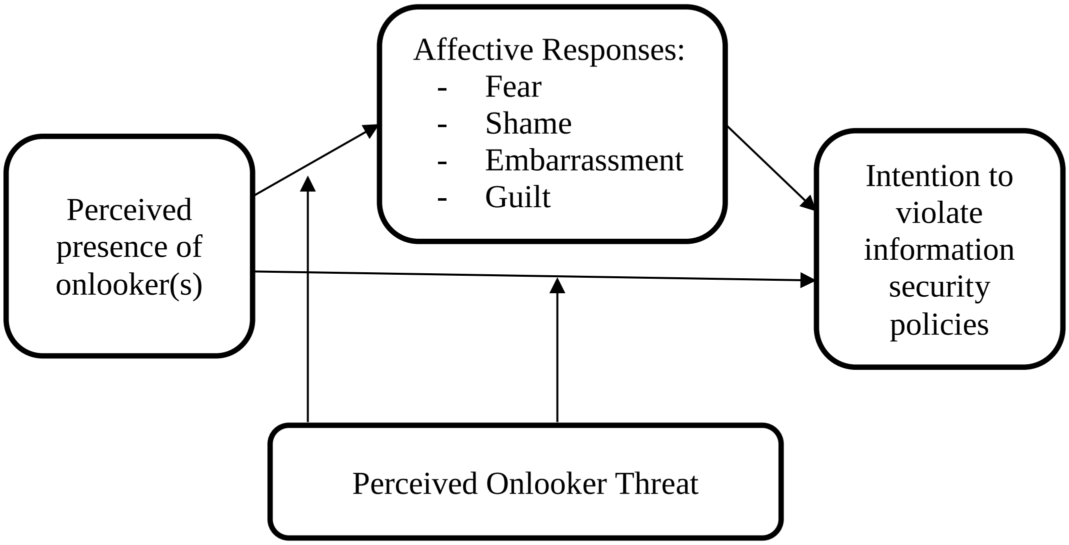

Affective Responses:
- Fear
- Shame
- Embarrassment
- Guilt
Perceived presence of onlooker(s)
Intention to violate information security policies
Perceived Onlooker Threat

Figure 2-2: Proposed Model

CHAPTER 3

RESEARCH METHODOLOGY

In order to test the hypothesized model, an experimental vignette was used to determine subject responses to the treatment conditions. Respondents in this study were recruited using the Qualtrics online survey platform, and instrument development and validation for measurement of the theoretical constructs are discussed in detail below.

The study tested theoretical hypotheses about the Onlooker Effect in information security violation behaviors, as developed in Chapter 2, above. The following hypotheses will be tested:

H1: The perceived presence of onlookers will result in experiencing fear by security policy violators.

H2: The feeling of fear arising from the perceived presence of onlookers will negatively influence intentions to violate information security policies.

H3: The perceived presence of onlookers will cause security policy violators to experience shame.

H4: The feeling of shame arising from the perceived presence of onlookers negatively influences intention to violate information security policies.

H5: The perceived presence of onlookers will result in the experience of embarrassment by security policy violators.

H6: Feelings of embarrassment by potential security policy violators will negatively influence intention to violate information security policies.

H7: The perceived presence of onlookers will result in experience of guilt by security policy violators.

H8: Feelings of guilt by potential security policy violators will negatively influence intentions to violate information security policies.

H9: The perceived presence of onlookers will negatively influence intentions to violate information security policies.

H10a-d: The relationship between the perceived presence of onlookers and affective responses (fear, shame, embarrassment, guilt) is moderated by perceived onlooker threat.

H11: The relationship between the perceived presence of onlookers and intention to violate information security policies is moderated by perceived onlooker threat.

3.1 Methodology

Considering the inherent difficulty of studying actual ethical behaviors, this study assessed the proposed conceptual model using the “hypothetical scenario” method (Weber 1992). Scenario-based methods are a common approach used to assess antisocial and unethical behaviors (Pogarsky 2004; Siponen and Vance 2010). In this approach, descriptive scenarios are used to present subjects with descriptions of realistic situations after which subjects were asked to respond to the scenario with a number of rating scales which measured the dependent variables of interest (e.g., Trevino 1992, pp.127-128). The scenario method has been used in the information security context for studies of information system misuse (D’Arcy et al. 2009), privacy concerns (Malhotra et al. 2004) and security policy violations (Siponen and Vance 2010).

There are several advantages of using this method to study socially undesirable behaviors. Since scenarios describe a “hypothetical other” and their behavior in purely scenario-based terms, subjects will be less likely to conceal their intentions and reactions in response to the manipulation (Trevino 1992). Moreover, scenarios give the researcher an opportunity of providing situational details that are important in operationally characterizing the decision making leading to the violation (Klepper and Nagin 1989).

In this study, scenarios with embedded manipulations were given to the subjects who were then asked to indicate how they would respond, given the conditions in the scenario. The scenarios and instruments were all pretested, and the instruments were also validated, in a pilot study.

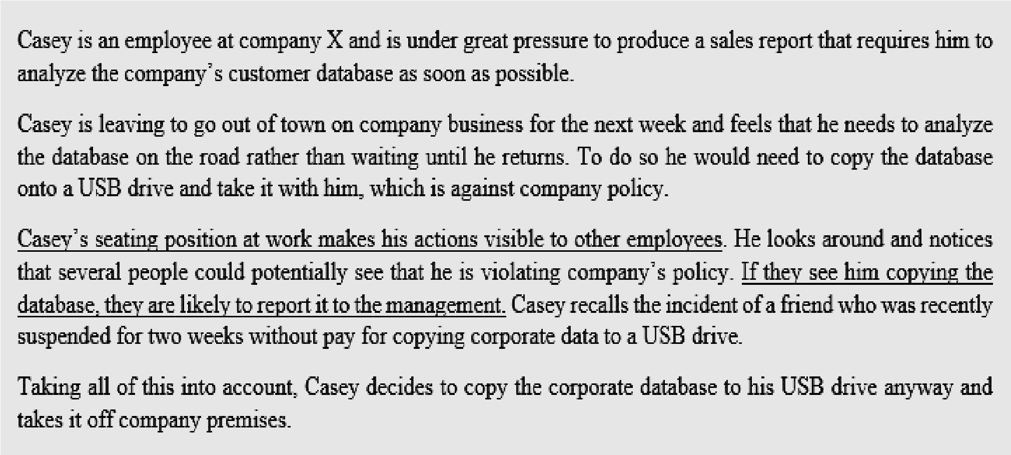
3.2 Experimental design

The goal of the research is to understand the effects of the perceived presence of onlookers (The Onlooker Effect) and the subsequent deterrence effects it might have. Three scenarios were created based on a literature survey of information security violation behaviors, and these are displayed in APPENDIX A. According to Siponen and Vance (2010) copying sensitive data to insecure USB devices is one of the most common security policy violations. With that in mind, in order to use well-constructed and validated scenarios from previous research (Weber 1992), the experimental scenarios were based on the Siponen and Vance (2010) “USB device” security violation exemplar, and were refined and customized through pretesting and pilot testing. The first scenario manipulates both the presence of onlookers and the onlooker threat. The second scenario serves as the experimental control and has no manipulation. The third scenario manipulates only the presence of onlookers. Table 3-1 summarize these experimental conditions.

Table 3-1: Experimental conditions

Experimental condition	**Manipulations**	
	Perceived presence of onlooker	**Perceived onlooker Threat**
Scenario 1	Yes	Yes
Scenario 2	No	No
Scenario 3	Yes	No

These treatments in the experimental conditions were reflected in the three different scenarios (see APPENDIX A). A sample vignette is shown in Figure 3-1.



Casey is an employee at company X and is under great pressure to produce a sales report that requires him to analyze the company's customer database as soon as possible.

Casey is leaving to go out of town on company business for the next week and feels that he needs to analyze the database on the road rather than waiting until he returns. To do so he would need to copy the database onto a USB drive and take it with him, which is against company policy.

Casey's seating position at work makes his actions visible to other employees. He looks around and notices that several people could potentially see that he is violating company's policy. If they see him copying the database, they are likely to report it to the management. Casey recalls the incident of a friend who was recently suspended for two weeks without pay for copying corporate data to a USB drive.

Taking all of this into account, Casey decides to copy the corporate database to his USB drive anyway and takes it off company premises.

Figure 3-1: Sample vignette

The perceived presence of onlookers was manipulated as follows. When the perception of presence of onlooker was present as part of the scenario, the following words are included:

> *Casey's seating position at work makes his actions visible to other employees. He looks around and notices that several people could potentially see that he is violating company's policy.*

When the perceived presence of onlookers is not included in the manipulation, these words were included:

> *Casey looks around and because of his sitting position, he is confident nobody would be able to see that he is violating company's policy.*

In the manipulation for the perceived onlooker threat, the following words are included:

> *If they see him copying the database, they are likely to report it to the management.*

And, when the onlooker threat was not manipulated, the following words were included:

> *He is confident they won't report him, even if they do see him.*

3.3 Survey instrument

Following the presentation of the scenario, subjects completed an online questionnaire. Most of the items for the instrument were adapted from previously validated scales identified in the literature review.

The dependent variable, intention to violate information security policy, was measured using a three-item scale from D'Arcy et al. (2009) and Cheng et al. (2013). The items wording have been slightly modified to fit the scenario. In order to assess feeling of fear, taking guidance from Block and Keller (1995), Gleicher and Petty's (1992) five-item fear scale was used. For assessing state of shame and guilt, the ten-item SSGS scale of Marschall et al. (1994), was used. A felt state of embarrassment was measured in line with Tracy et al. (2007), who recommended the use of Mosher and White's (1981) three-item inventory, covering feeling embarrassed, feeling self-conscious, and blushing. Given that the perceived presence of an onlooker and the perceived onlooker threat (manipulation checks) have not been previously identified or measured, measures were developed specifically for this study using a focus group of scholars and doctoral students in management, marketing, and CIS.

A single-item measure that asked subjects to rate how realistic they perceived the treatment scenario to be was also included. This measure ranged from 0 (not believable) to 10 (100% believable). Demographic and control variables were included and collected information on gender, age, industry, educational level, organizational tenure, etc. A seven-point Likert response scale, using anchor text for all seven levels, was used for all measures. All instruments items and related questionnaire items are displayed in APPENDIX B.

3.4 Pretest and pilot test

3.4.1 Pretests

The scenarios were refined through three rounds of pretesting. The first round consisted of a review of the draft scenarios by a three-member panel of IS and management scholars for accuracy and realism. Revisions to the scenarios were made following this review. Then, the revised scenarios along with manipulation check questions and scenario realism question were administered to a sample of 43 undergraduate students. The results of the manipulation check showed a small-to-medium effect size. Following one more panel review by three doctoral students and two IS professors, further revisions were then undertaken. Subsequently, a second round of pretesting with a sample of 82 undergraduate students was conducted. The results showed a large effect size for the perceived presence of onlookers (the first manipulation) and a medium-to-large effect size for perceived onlooker threat (the second manipulation).

After refining the scenarios and ensuring the effectiveness of the manipulations, a final round of pretesting was conducted with a panel of 20 doctoral student using an online version of instrument. This final pretest was undertaken to ensure no unanticipated difficulties with the instrumentation before conducting the pilot study. Panel members were asked to determine the time taken to complete the survey and to provide any other feedback regarding the survey in terms of usability, flow, organization, and overall look and feel. The feedback and suggestions were applied in one final revision of the procedure.

Based on pretesting results and revisions, the final instrument for the experimental vignette began with an information sheet, a request for agreement to participate, filtration questions, and a randomly assigned scenario (1 of the 3 experimental conditions). The scales for the constructs were then presented, which also included a marker variable and demographic questions.

3.4.2 Pilot test

The purposes of the pilot study were to make a final check on the quality of the experiment, to identify any issues with the instrument, and to conduct confirmatory factor analysis (CFA) in order to check for any potential internal validity issues before performing the actual study.

The subjects for the pilot study were recruited from the pool of business undergraduate students at a large university in the United States. Students were recruited by professors' announcements via email or in person; the undergraduate faculty in the college were asked to announce the survey to their classes and encourage participation.

The online survey began with a subject information sheet, which guided subsequent actions in the process. On this initial page, student subjects were able to voluntarily agree (or not) to participate. The pilot study included 325 participants, resulting in 268 usable responses. Manipulation checks were conducted, and SmartPLS 2.0 was used for analyzing the pilot data. Results showed that all constructs have AVE values of 0.685 or higher, which is considerably above the critical value of 0.5 (Hair et al. 2017). In addition, all Cronbach’s alpha (ranging from 0.847 to 0.932) and composite reliability values (ranging from 0.902 to 0.956) are well above the critical threshold of 0.70 recommended by Hair et al. (2017). Moreover, the loadings of the items were all higher than the recommended threshold (ranging from 0.724 to 0.946), so the conditions of convergent validity have been met. The constructs also evidenced good discriminant validity because the square root of AVE of each construct was larger than the correlations of each individual construct with the remaining constructs in the model. Based on these pilot results, the survey can be presumed as a valid instrument for further use.

3.5 Main Study Subjects

An anonymous online survey was placed with the Qualtrics data collection site, in order to collect main study data. The Qualtrics organization provided subject recruitment services for subsequent data collection. After participating subjects confirmed their acceptance of the study parameters via a consent form, they were directed to the online instrument that contained one of the three randomly assigned treatment scenarios and the survey questionnaire.

Rigid screening techniques employed by the Qualtrics organization have been applied to ensure that the sample appropriately represents the organizational context of the study. This study targeted currently employed professionals in the U.S. who used computers as an aspect of their jobs and who operated under an organizational information security policy (ISP) of which that they were aware. Each of the three experimental scenarios was targeted to a minimum of two hundred and thirty subjects and a total of 690 usable questionnaires were collected in the process. These were subsequently used to examine the research questions.

CHAPTER 4

DATA ANALYSIS

In order to test the proposed model, an experimental vignette was conducted using a Qualtrics online panel. Mackenzie (2001) argued that structural equation modeling (SEM) has the potential to fundamentally improve experimental research, especially in examining variables like beliefs, emotions and attitudes. The other advantages of using SEM could be its extreme flexibility and ability to conduct rigorous tests of the hypothesized effects of manipulations. This study was intended to follow Mackenzie (2001) and analyze the data using CB-SEM.

After data collection and preliminary analyses, assessment of normality showed that every variable departed significantly from normality according to the critical ratio criterion; the multivariate kurtosis value also indicates severe non-normality (values exceeding ten), as it is shown in Table 4-1. Owing to the severity of non-normality in the sample distribution, using specific estimation methods in covariance analysis was untenable since they are not robust to non-normal data. For that reason, analysis was subsequently conducted with partial least squares structural equation modeling (PLS-SEM), in line with the recommendation of Lowry and Gaskin (2014).

Table 4-1: Assessment of normality

Variable	skew	c.r.	kurtosis	c.r.
Fear1	-1.275	-13.675	1.645	8.821
Fear2	-1.671	-17.915	3.654	19.592
Fear3	-1.308	-14.032	1.687	9.046
Fear4	-0.456	-4.889	-0.641	-3.436
Fear5	-1.52	-16.3	3.049	16.35
Embarrassment1	-1.039	-11.142	0.414	2.218
Embarrassment2	-1.379	-14.786	1.956	10.49
Embarrassment3	-0.303	-3.254	-0.668	-3.584
Shame1	-0.708	-7.593	-0.497	-2.665
Shame2	-0.746	-7.998	-0.422	-2.265
Shame3	-0.876	-9.39	-0.015	-0.078
Shame4	-0.641	-6.876	-0.477	-2.556
Shame5	-0.156	-1.675	-0.829	-4.446
Guilt1	-1.428	-15.316	1.951	10.464
Guilt2	-1.728	-18.532	3.666	19.658
Guilt3	-1.277	-13.697	1.091	5.849
Guilt4	-0.937	-10.043	0.262	1.405
Guilt5	-1.348	-14.457	1.801	9.654
Int.Vio.1	1.756	18.83	1.832	9.825
Int.Vio.2	1.525	16.351	1.245	6.677
Int.Vio.3	1.708	18.312	1.866	10.006
PPO1	-0.988	-10.59	-0.468	-2.511
PPO2	-0.93	-9.968	-0.605	-3.244
Multivariate			258.867	96.242

Lowry and Gaskin (2014) suggest that PLS-SEM is useful in the case of non-normal distributions but also note that abnormal data distributions can still affect the results, albeit to a lesser extent. Even so, an additional benefit is that PLS-SEM is considered particularly useful for exploratory research (Gefen et al. 2011), because it permits the examination of models which include interaction effects (Ringle et al. 2012). Since the proffered model contemplates interactions, PLS-SEM was subsequently undertaken for analysis.

In summary, this study was conducted with experimental vignette methodology with the specific objective of exploring the onlooker effect in an information security context and evaluating the developed model with generalizability in mind. Subjects responded to one of three randomly-administrated treatment scenarios followed by a questionnaire on the Qualtrics platform. A total of 690 usable responses was then submitted to analysis in PLS-SEM.

4.1 Descriptive statistics

The sample frame for the study consists of individuals in the U.S., currently employed by organization which operate under an information security policy, of which they are aware. Table 4-2 displays sample demographic information.

For scenario realism, the average reported scenario realism score was 8.66 out of 10, thus the presented scenarios were fairly realistic.

Table 4-2: Demographic analysis

Subjects (n=690)							
Gender	Male	311	45%	**Position**	Senior Manager	90	13.04%
	Female	379	55%		Middle Manager	174	25.22%
Education	High School	116	16.81%		Technical	65	9.42%
	Two-year College	161	23.33%		Professional Staff	195	28.26%
	Bachelor’s	264	38.26%		Administrative	97	14.06%
	Master’s Degree	116	16.81%		Other	69	10.00%
	Doctoral Degree	19	2.75%	**Industry**	Manufacturing	71	10.29%
	Other	14	2.03%		Finance	58	8.41%
Company Size (Number of Employees)	Less than 100	123	17.83%		IT	100	14.49%
	100-449	155	22.46%		Healthcare	88	12.75%
	500-999	106	15.36%		Education	77	11.16%
	1000-2499	85	12.32%		Retail	78	11.30%
	2500-9999	108	15.65%		Other	218	31.59%
	More than 9999	113	16.38%				
		Mean				**Mean**	
Age		42.57		**Computer Use at Work (hrs/day)**		6.54	
Work Experience (Years)		20.71		**Computer Knowledge (1-7)**		5.46	
Org. Tenure (Years)		9.29					

4.2 Measurement model

Two variables were manipulated through the experimental scenarios: perceived presence of onlookers, and perceived onlooker threat. Manipulation checks were conducted to ensure successful manipulations.

SmartPLS 3.2.8 was used for analyzing data, employing bootstrapping with 5000 re-samples, per Hair et al. (2017). Bootstrapping was employed in order facilitate the evaluation significance of model path estimates. The SmartPLS measurement model statistics include assessments of reliability, convergent validity, discriminant validity and common method variance. In fitting the model, composite reliabilities (ranging from 0.852 to 0.968) and Cronbach's alpha (ranging from 0.754 to 0.950) were all higher than the recommended threshold of 0.70 (e.g., Hair et al. 2017). In addition, all reflectively measured constructs demonstrated AVE values of 0.662 or higher, which is considerably above the critical value of 0.5 (e.g., Hair et al. 2017). These values support the conclusion of measurement instrument validity and reliability (see Table 4-3).

Table 4-3: Construct reliability and validity

Construct	**Composite Reliability**	**Cronbach's Alpha**	**Average Variance Extracted (AVE)**
Embarr.	0.852	0.754	0.662
Fear	0.926	0.900	0.717
Guilt	0.932	0.908	0.733
Shame	0.919	0.891	0.695
PPO	0.950	0.896	0.906
POT	0.930	0.850	0.869
Int. Vio.	0.968	0.950	0.909

PPO= Perceived Presence of Onlooker, POT= Perceived Onlooker Threat, Int.Vio.= Intention to violate.

In measurements model validation via PLS, convergent validity is demonstrated when measurement items load significantly on their specified constructs (Lowry and Gaskin 2014). Such significance is evaluated on an indicator-by-indicator basis, and evidence of significance for a given indicator-on-contract loading is provided when t-values of Outer Model Loadings for each respective measurement indicator are above 1.96 ($\alpha = 0.05$). This condition was met in all instances, and, as demonstrated in Table

4-4, provide good evidence of convergent validity for the set of measurement indicators and their respective constructs.

Table 4-4: Measurement model results

Indicators	Loadings	Mean	S.D.	t Statistics
Embarrassment1	0.906	0.904	0.013	71.221
Embarrassment2	0.862	0.859	0.021	41.508
Embarrassment3	0.649	0.652	0.051	12.669
Fear1	0.816	0.817	0.026	31.130
Fear2	0.911	0.910	0.009	96.248
Fear3	0.903	0.903	0.011	81.316
Fear4	0.708	0.708	0.025	28.555
Fear5	0.879	0.878	0.012	74.426
Guilt1	0.879	0.879	0.013	65.713
Guilt2	0.849	0.849	0.016	53.202
Guilt3	0.856	0.856	0.021	41.265
Guilt4	0.787	0.786	0.024	32.530
Guilt5	0.906	0.906	0.011	83.668
PPO1	0.971	0.967	0.043	22.719
PPO2	0.928	0.925	0.056	16.551
POT1	0.930	0.930	0.014	67.191
POT2	0.935	0.935	0.013	72.176
Shame1	0.780	0.780	0.025	31.439
Shame2	0.858	0.857	0.015	57.024
Shame3	0.831	0.830	0.017	48.625
Shame4	0.905	0.905	0.009	98.460
Shame5	0.788	0.787	0.021	36.816
Int.Vio.1	0.953	0.953	0.008	124.721
Int.Vio.2	0.962	0.962	0.006	174.289
Int.Vio.3	0.946	0.946	0.010	94.532

PPO= Perceived Presence of Onlooker, POT= Perceived Onlooker Threat, Int.Vio.= Intention to violate.

In demonstrating evidence of discriminant validity, this study utilizes two established techniques: confirming that the all the loadings of the measurement items on their assigned constructs is larger than any other loadings (Gefen and Straub 2005, p. 93), and confirming that the square root of the average variance extracted (AVE) of each latent construct is larger than the correlation with other constructs. Evidence of these two qualities is provided in Table 4-5.

Table 4-5: Construct correlations and AVE

	Embarr.	**Fear**	**Guilt**	**Shame**	**PPO**	**POT**	**Int. to Vio.**
Embarr.	**0.813**						
Fear	0.697	**0.847**					
Guilt	0.741	0.739	**0.856**				
Shame	0.704	0.584	0.687	**0.834**			
PPO	0.097	0.081	0.087	0.094	**0.950**		
POT	0.161	0.123	0.156	0.184	0.616	**0.933**	
Int. Vio.	-0.327	-0.436	-0.500	-0.357	-0.003	-0.037	**0.954**

*Bold numbers are the square root of AVE.

PPO = Perceived Presence of Onlooker, POT = Perceived Onlooker Threat, Int.Vio. = Intention to violate.

In order to control common method variance (CMV), the procedures advocated by Podsakoff et al. (2003) were employed. This included steps such as protecting respondent anonymity, reducing evaluation apprehension, and improving scale items. Since the endogenous variables of the model were collected at the same time and with the same instrument as the exogenous variable, the potential effect of common method variance was tested in order to establish that such variance did not distort the data collection process.

Harman’s single factor test was undertaken, initially. It examined the unrotated factor analysis solution to determine the number of factors that are necessary to explain the majority of variance in the model. Based on the result of this factor analysis, the largest eigenvalue explained about 40% of the variance, suggesting that the majority of variance is not accounted for by just one general factor. To that end, and common method variance is considered unlikely.

Secondly, the correlation matrix of the constructs was examined in order to determine if any of the construct-to-construct correlations were above .90 -- which is generally considered indicative of the presence of common method variance (Lowry and Gaskin 2014; Pavlou et al. 2007). The correlation matrix, which is shown in Table 4-5, does not indicate highly correlated factors. Hence, further support for the lack of common method variance is provided. Lastly, this study used a partial correlation technique with a marker variable proxy (referred as "the marker variable technique"), for detection of common method variance (Lindell and Whitney 2001; Podsakoff et al. 2003). In this approach, researchers correlate the data of the primary model variables to the marker variable and if the correlations are high, then common method variance likely exists. For purposes of market variable analysis, a three-item scale for "outdoor activity" (which is theoretically unrelated to the other constructs) was included in the questionnaire. Marker variable analysis results showed that outdoor activity (the marker variable) is not highly correlated with the other constructs of the model, thus providing even further evidence of the lack of common method variance.

4.3 Structural model

The structural model was explored in SmartPLS to determine the significance and strength of each of the hypothesized effects. However, before assessing the proposed hypotheses, the effects of the manipulations were examined. The manipulations for the perceived presence of onlooker and perceived onlooker threat had the expected effects in their respective manipulation checks; both paths were positive and statistically significant (t-values of 34.387 and 17.826, respectively; α = 0.05).

Evidence of the manipulation check in hand, the hypothesized effects of the model were assessed. The model hypothesized that the relationship between the perceived presence of onlookers and four specific affective responses (fear, shame, guilt, and embarrassment) would be positively moderated by the perception of perceived onlooker threat. In other words, that the presence of onlookers would result in stronger affective responses if a perceived onlooker threat was perceived. Such moderator relationships are tested statistically by checking for interaction effects among independent variables. For this purpose, two models were specified: one for the interaction model and one for the baseline theoretical model.

In subsequent testing, the interaction of perceived onlooker threat and the perceived presence of an onlooker was significantly correlated to all four of affective responses. Considering the interaction term in the model dramatically increases the beta coefficient of the path between perceived presence of onlooker and each of the four affective responses. This resulted in significance for four paths. The comparison of baseline and interaction model is shown in Table 4-6, and is represented graphically in Figure 4-1 and Figure 4-2.

As shown in Table 4-6, R^2, the explained variance for fear increased, from 0.015 to 0.067. Explained variance for shame increased from 0.035 to 0.063, explained variance for embarrassment increased from 0.026 to 0.052, and explained variance for guilt increased from 0.025 to 0.071. The interaction, which was significant, demonstrated an effect size of $f^2 = 0.053$ for fear, $f^2 = 0.029$ for shame, $f^2 = 0.027$ for embarrassment, and $f^2 = 0.047$ for guilt. This represented a modest interaction effect, however these small interaction effects are meaningful here since the resulting beta changes are meaningful, as well (e.g., Chin et al. 2003).

Table 4-6: Model comparison

	Baseline Model					Interaction Model				
	Fear	Shame	Embarr.	Guilt	Int.Vio.	Fear	Shame	Embarr.	Guilt	Int.Vio.
R^2	0.015	0.035	0.026	0.025	0.307	0.067	0.063	0.052	0.071	0.274
ΔR^2						0.052	0.028	0.026	0.046	-0.033
f^2						0.053	0.029	0.027	0.047	-0.048
Effect size						small	small	small	small	-

f^2= [R^2 (interaction model) – R^2 (baseline model)]/ [1- R^2 (baseline model)]
Effect sizes small (.02), medium (.15), large (.35); (Cohen 1988)
Embarr. = Embarrassment, Int.Vio. = Intention to violate.

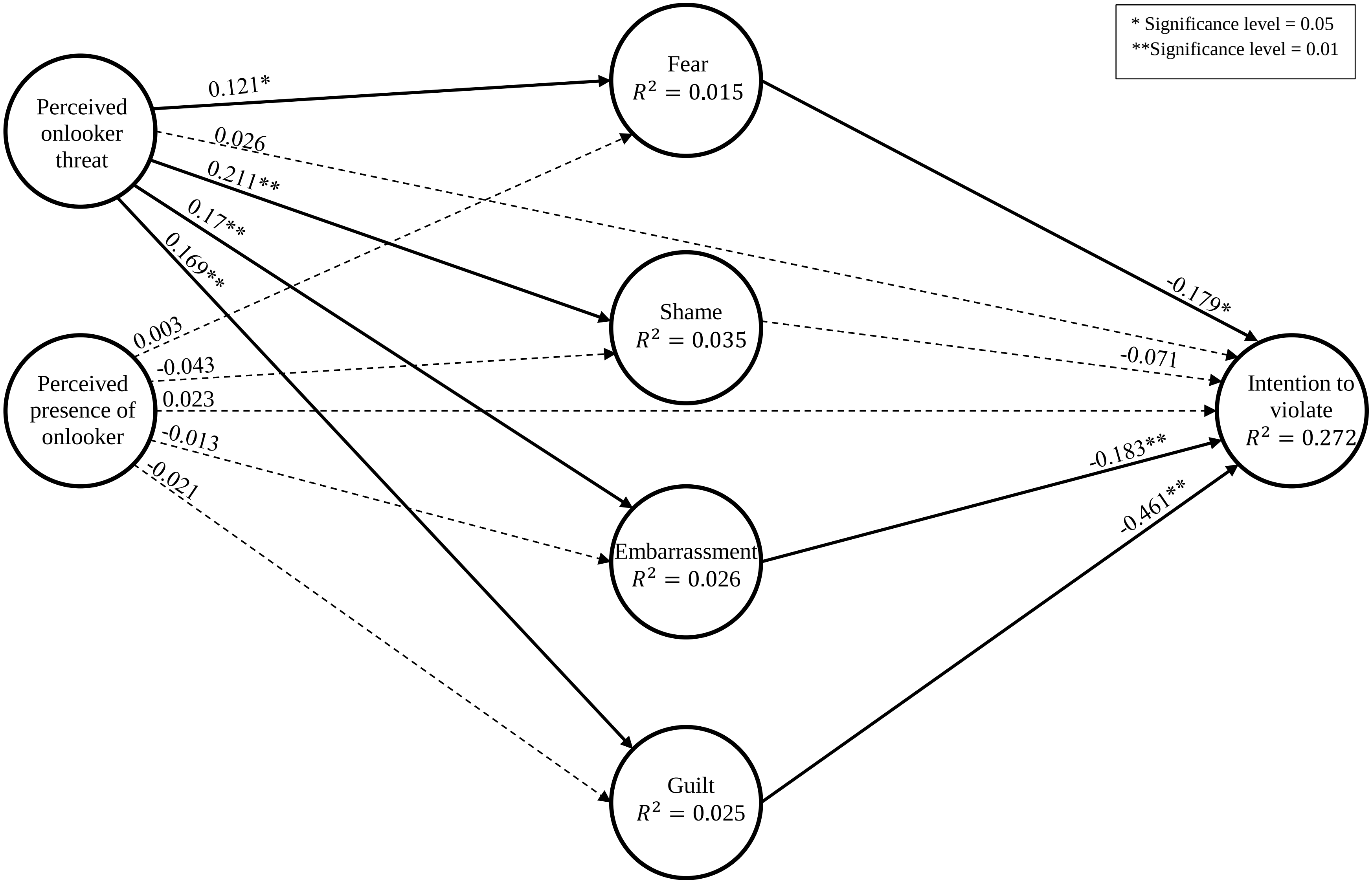

* Significance level = 0.05
**Significance level = 0.01
Perceived onlooker threat
Perceived presence of onlooker
Fear $R^2 = 0.015$
Shame $R^2 = 0.035$
Embarrassment $R^2 = 0.026$
Guilt $R^2 = 0.025$
Intention to violate $R^2 = 0.272$
0.121*
0.026
0.211**
0.17**
0.169**
0.003
-0.043
0.023
-0.013
-0.021
-0.179*
-0.071
-0.183**
-0.461**

Figure 4-1: The baseline model

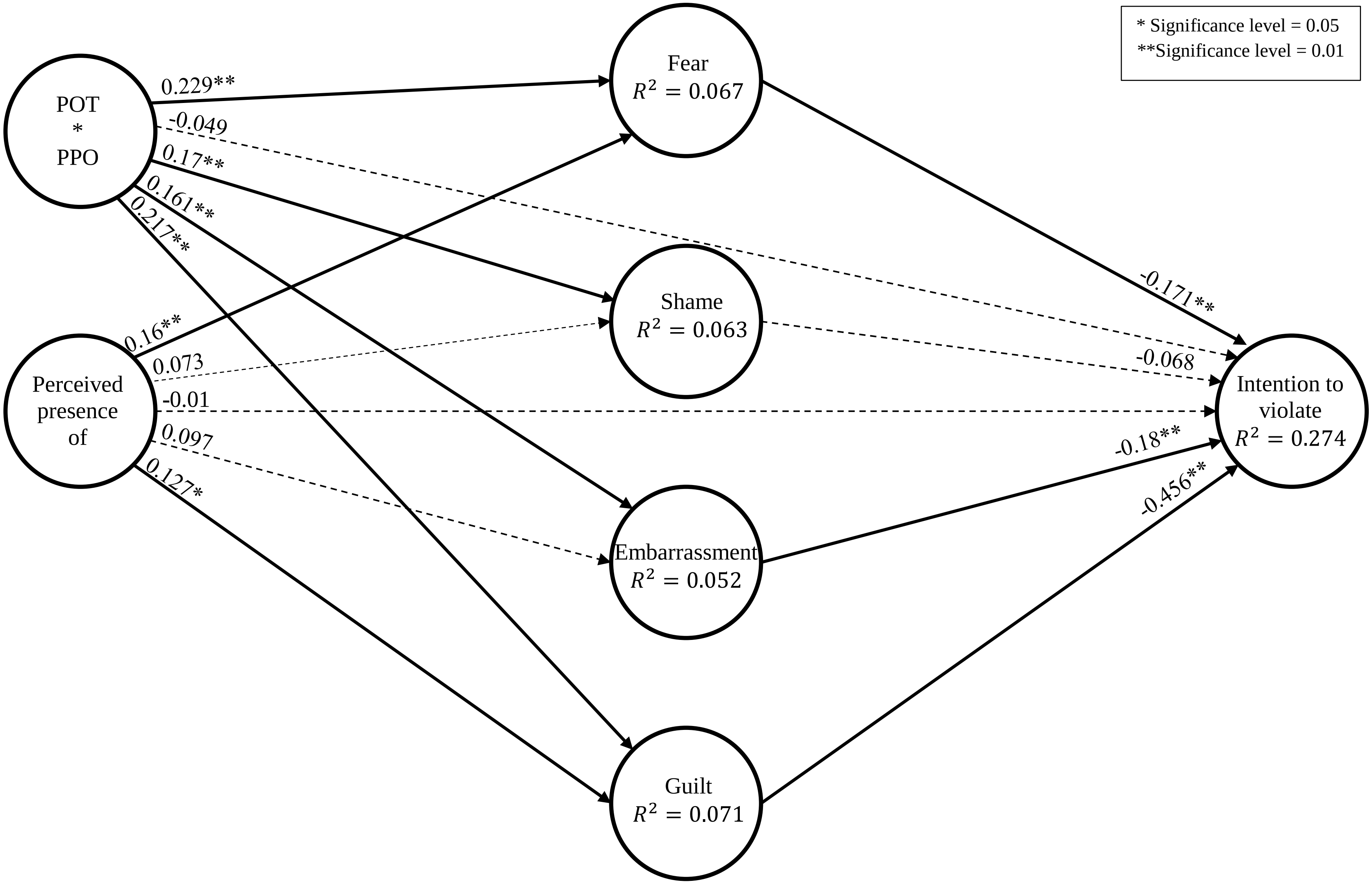
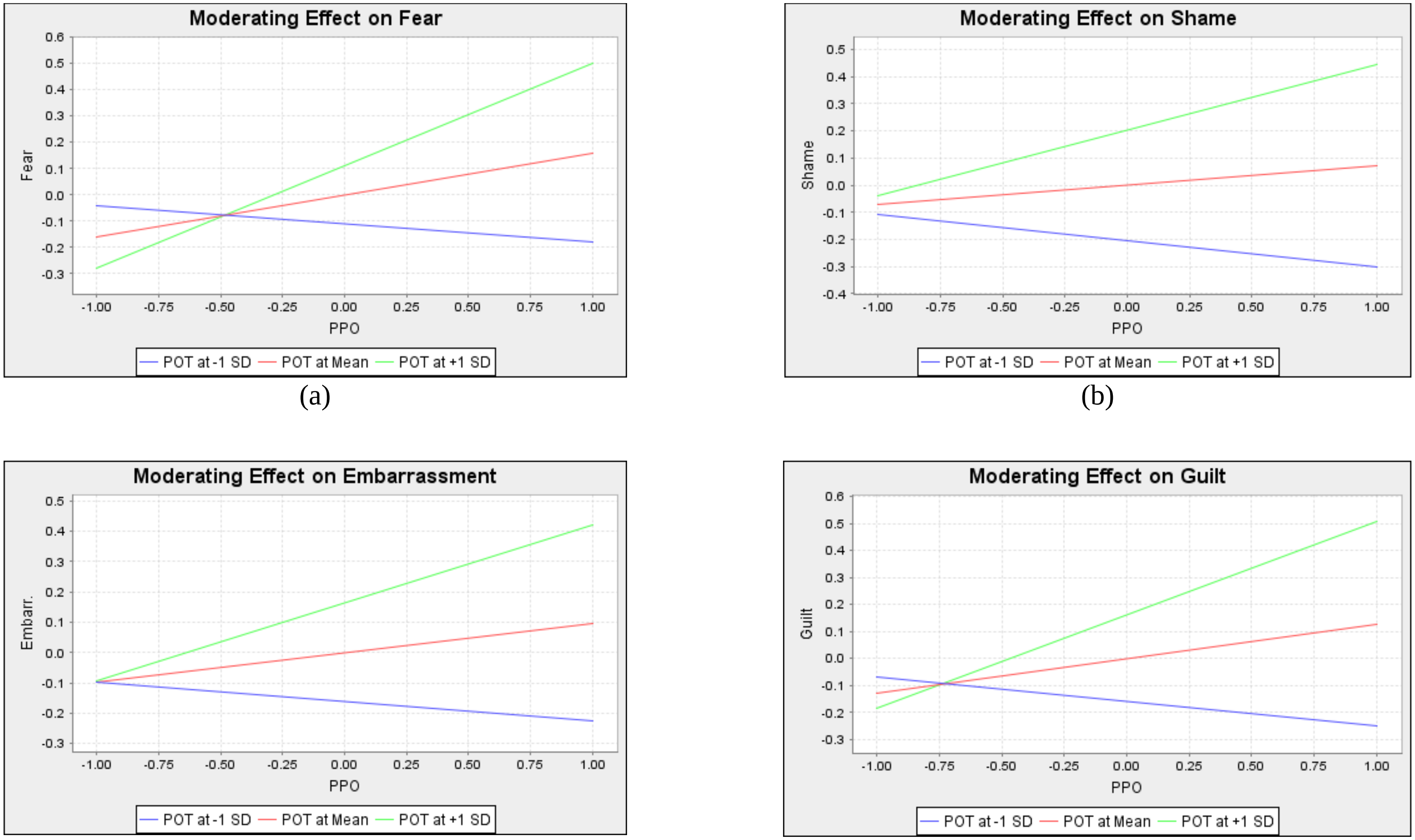


Figure 4-2: The interaction model

4.4 Simple slope analysis

In order to have better understanding of the interaction effects, a simple slope analysis was conducted each interaction effect in the model. The results of this analysis process are shown in Figure 4-3. In each of graphs in this figure, generally the red line shows the regular effect and not considering the moderator role. The blue line shows the effect of perceived onlooker threats at negative one standard deviation from the mean, and the green line shows the effects of this moderator at positive one standard deviation from the mean. By comparing the green line and the red line in each part of this figure, it is evident that the stronger perceptions of onlooker threats serve to strengthen the positive effect of perceived presence of onlooker in each of affective responses.

Moreover, the proposed relationships between four affective responses and intention to violate information security policy were all significant at $\alpha = 0.05$ except for shame. The direct impact of the perceived presence of onlookers on intention to violate the information security policy was not supported with the data, nor did interaction analysis with the perceived onlooker threat result in a significant relationship. It is noted that the relationships with the control variables such as gender, organizational tenure, computer use were not statistically significant. The results of this specific analysis are summarized in Table 4-7.



(a)

(b)

(c)

(d)

Figure 4-3: Simple slope analysis results

Table 4-7: Summary of proposed relationships

Hypotheses	Path coefficient	t statistic	p-value	status
H1: PPO → Fear	0.160	2.767**	0.006	Supported
H2: Fear → Int.Vio.	-0.171	2.317*	0.021	Supported
H3: PPO → Shame	0.073	1.160	0.246	Not supported
H4: Shame → Int. Vio.	-0.068	1.179	0.239	Not supported
H5: PPO → Embarr.	0.097	1.786	0.075	Not supported
H6: Embarr. → Int. Vio.	-0.180	3.179**	0.002	Supported
H7: PPO → Guilt	0.127	2.052*	0.041	Supported
H8: Guilt → Int.Vio.	-0.456	6.658**	0.000	Supported
H9: PPO → Int. Vio.	-0.010	0.219	0.827	Not supported
H10a: POT moderates H1	0.229	5.841**	0.000	Supported
H10b: POT moderates H3	0.170	4.074**	0.000	Supported
H10c: POT moderates H5	0.161	3.932**	0.000	Supported
H10d: POT moderates H7	0.217	5.079**	0.000	Supported
H11: POT moderates H9	-0.049	1.624	0.105	Not supported

* Significance level = 0.05

**Significance level = 0.01

CHAPTER 5

DISCUSSION AND CONCLUSIONS

In the current threat environment, organizations rely on information security more extensively than ever which is why research on information security is so important. Researchers concur that employees are the weakest link in an organization's information security management chain. Numerous studies on the matter have identified a range of different predictors for the intention to violate information security policies and these have resulted in a variety of prescriptions mitigating information security policy violations in the workplace. Never the less, the latest report of Ponemon Institute shows that twenty-seven percent of data breaches are the result of human errors and negligence (Ponemon Institute 2018). This means that in some cases employees do not have malicious intent and that they simply wish to "get the job done" even if it requires violations of organizational information security policies. Even so, the threat from intentional violations of security policy is even higher and studies such as this inform the process of protecting against that hazard.

Taken together, there is still a need to undertake research about the varying behavioral factors involved in employees' decision-making processes when they consider violations of information security policies. This research examined the combined impact of the perceived presence of onlooker and perceived onlooker threat on the intention to violate information security policies, as influenced by different affective responses by employees. As such, the intention was to answer the following research questions:

1. Does the perceived presence of onlookers significantly reduce the intention to violate information security policy in a workplace?
2. Does the perceived presence of onlookers result in the experience of negative affective responses such as fear, shame, guilt, and embarrassment by employees who intend to violate information security policies?
3. Does the experience of affective responses such as fear, shame, guilt, and embarrassment reduce the intention to violate information security policies?
4. Does perceived onlooker threat significantly inflate the impact of perceived presence of onlookers on subsequent intentions to violate information security policies in the workplace?
5. Does perceived onlooker threat result in experiencing stronger affective responses such as fear, shame, guilt, and embarrassment at the time of violating information security policies?

Using Sociometer Theory and Affective Events Theory as theoretical lenses, a model of onlooker effects was developed which proposes that the perceived presence of onlookers results in the experience of negative affective responses such as fear, shame, guilt, and embarrassment, which in turn mitigates intentions to violate information security policies in the workplace. This affective effects in this model were theorized to be strengthened by the presence of a perceived onlooker threat. To test the model, this study used a hypothetical scenario-based method utilizing 690 respondents. The experimental sample consisted of a heterogeneous population from a variety of organizations, positions, and organizational tenure levels.

The results show that the perceived presence of onlookers, on its own, does not significantly impact the intention to violate information security policy in the workplace. Even the interaction of the perceived presence of onlookers and perceived onlooker threat does not directly impact in statistically significant fashion subsequent intentions to violate information security policies. Moreover, the main effect of perceived presence of onlookers also do not significantly impact affective responses. But the perceived onlooker threat does play an important role in subsequent behaviors, and the interaction between perceived onlooker threat and perceived presence of onlookers significantly increases felt experience of all four of affective response among respondents. Consequently, experiencing guilt, fear, and embarrassment negatively impact the intention to violate information security policies.

Simply put, in the event that an employee intends to violate information security policies the perception that someone may hear or see the violation will not mitigate this intention, though it is important who the onlooker is. If the employee has some perception that the onlooker will report the violation (availability of perceived onlooker threat), he/she will experience negative affective responses such as fear, guilt, and embarrassment resulting in mitigation of intention to violate information security policy. Even so, the experience of shame by a potential violator of an information security policy does not significantly reduce the intention to violate, based on the results of this study.

This is consistent with the findings of some studies in information security literature, such as Siponen and Vance (2010), where they found that shame does not have a significant effect on intention to violate security policies when employees invoke neutralization techniques that aid in the rationalization of the guilt, self-blame and shame that may arise in the act. Interestingly, another study by Siponen et al. (2012) found that shame did have a significant effect on intention to commit software piracy, even when neutralization techniques did have a significant impact.

Considering these points as background, as a final analytical step this study tested the hypothesized model with only shame included as the affective response variable, and the results indicate that in this case shame does have a significant and negative impact on intentions to violate information security policies (path coefficient = -0.342, $p \leq 0.000$). The study concludes, then, that the presence of other affective responses such as guilt, fear, and embarrassment likely render the impact of shame as non-significant. This does not mean, however, that there is no relationship between feeling shame and the reduction of intentions to violate information security policies; future studies should consider shame as one of the key influences mitigating against the commitment of workplace security policy violations.

5.1 Theoretical contributions

This study provides a number of theoretical contributions to information security research. First, it is one of the first known attempts to empirically investigate the Onlooker Effect on intentions to violate information security policies. Second, it extends the theoretical foundation of information security research by introducing

Sociometer Theory and Affective Events Theory. Finally, it provides empirical validation through experimental results.

5.2 Practical contributions

This study provides a number of important practical contributions. It provides important insights to managers, suggesting that small changes in situational factors might mitigate the intention of employees to violate information security policies. It also provides practitioners with empirical evidence of the potential impact of the perceived presence of onlookers on reducing intentions to violate information security policies in circumstances where violators perceive the threat of being seen is credible and that an onlooker may report violations that are observed. To be more precise, the results of this study show that the presence of an onlooker around who may report violations of security policies in the workplace will increase negative feelings such as guilt, fear, and embarrassment, hence resulting in reduced intentions to commit security violations. To that end, this study increases practitioner awareness of the importance of an organization’s physical structure and workplace layout especially in departments and sections in which employees deal with sensitive data. More importantly, the results here indicate how small changes in physical workplace arrangements may mitigate information security violations.

5.3 Limitations

As with any study, limitations exist. This study used the scenario-based experimental method which means that respondents read written scenarios and then answered the questionnaire. Although this study conducted pretests and pilot testing to ensure the realism of the scenarios, and to determine that they were and conveying the intended specific situational factors to the respondents, there may well still be differences between the scenarios devised for the study and real-life workplace experiences. Lastly, as in any study that uses a questionnaire for data collection, there is always a potential inherent bias from the self-report process with respondents.

5.4 Future research

This study defines the perceived onlooker threat as the possibility of observed violations of information security policies being reported by onlookers in the workplace. Future research should investigate other possible aspects of the onlooker effect such as the onlooker's identity and organizational position and their relation to the violator, if any. Moreover, it is quite likely that onlookers who are known to be members of the organizational information security team will instantiate quite different responses in perpetrators than would onlookers considered to be normal workplace colleagues.

Future research could also address organizational factors that may moderate the relationship between the perceived presence of onlookers and subsequent affective responses; one such factor might be the organization's perceived security climate. Prior studies (e.g. Goo et al. 2014) indicate that the information security climate in organizations may help employees to understand the importance of information security management and their roles in its successful implementation and, subsequently increase their feeling of responsibility to observe the firm's information security policies.

Future studies could also address a variety of individual differences that may inflate or deflate the impact of the perceived presence of onlookers on subsequent affective responses and related intentions to violate information security policies. Prior studies (e.g. D’Arcy and Lowry 2019) have considered Positive Affectivity (PA) and Negative Affectivity (NA) as general moods that affect rational decision making and employees’ attitude, and such factors may bear upon the degree to which onlooker effects operate or not.

Future research could also consider the role of self-esteem in the onlooker effect phenomena. Based on Sociometer Theory, self-esteem is part of a psychological system that monitors the social environment for and individual’s acceptance or rejection by others. The degree to which an individual feels rejected may influence maladaptive organizational behavior, whereas highly accepted individuals may well be less likely to perpetrate security violations. Fear of negative evaluations also could be a factor that plays a role in the onlooker effect phenomena; reactions to onlookers might be impacted by the likelihood of negative evaluations, if seen in violation of policy.

This study measures onlooker effects using hypothetical scenarios and self-report questionnaires. Future research may consider studying the Onlooker Effect in real organizational settings where the impact of being observed in a violation of security policy can be evaluated via observational methods.

Finally, future research could address the Onlooker Effect in the context of its influence on curbing truly malicious security violation behavior, instead of the casual violation envisioned in the manipulations used here.

APPENDIX A – SCENARIOS

Scenario 1- Perceived presence of onlookers, Perceived onlooker threat

Casey is an employee at company X and is under great pressure to produce a sales report that requires him to analyze the company's customer database as soon as possible.

Casey is leaving to go out of town on company business for the next week and feels that he needs to analyze the database on the road rather than waiting until he returns. To do so he would need to copy the database onto a USB drive and take it with him, which is against company policy.

Casey's seating position at work makes his actions visible to other employees. He looks around and notices that several people could potentially see that he is violating company's policy. If they see him copying the database, they are likely to report it to the management. Casey recalls the incident of a friend who was recently suspended for two weeks without pay for copying corporate data to a USB drive.

Taking all of this into account, Casey decides to copy the corporate database to his USB drive anyway and takes it off company premises.

Scenario 2- Control group- No perceived presence of onlookers, No perceived onlooker threat

Casey is an employee at company X and is under great pressure to produce a sales report that requires him to analyze the company's customer database as soon as possible.

Casey is leaving to go out of town on company business for the next week and feels that he needs to analyze the database on the road rather than waiting until he returns. To do so he would need to copy the database onto a USB drive and take it with him, which is against company policy.

Casey looks around and because of his sitting position, he is confident nobody would be able to see that he is violating company's policy. Moreover, he doesn't know of anybody of being punished for reported copying corporate data to a USB drive.

Taking all of this into account, Casey decides to copy the corporate database to his USB drive anyway and takes it off company premises.

Scenario 3- Perceived presence of onlookers, No perceived onlooker threat

Casey is an employee at company X and is under great pressure to produce a sales report that requires him to analyze the company's customer database as soon as possible.

Casey is leaving to go out of town on company business for the next week and feels that he needs to analyze the database on the road rather than waiting until he returns. To do so he would need to copy the database onto a USB drive and take it with him, which is against company policy.

Casey's seating position at work makes his actions visible to other employees. He looks around and notices that several people could potentially see that he is violating company’s policy. However, he is confident they won’t report him even if they do see him.

Taking all of this into account, Casey decides to copy the corporate database to his USB drive anyway and takes it off company premises.

APPENDIX B – QUESTIONNAIRE

Construct	ID	Item	Reference
Intention to Violate	V1	If you were Casey, what is the likelihood that you would have copied the corporate database to your portable USB drive?	Cheng et al. 2013; D'Arcy et al. 2009
	V2	I could see myself copying the corporate database to my portable USB drive if I was in Casey's situation.	D'Arcy et al. 2009
	V3	If I was in this situation, I would also copy the corporate database to a portable USB drive.	Cheng et al. 2013
State of Shame	S1	If I was Casey, I would want to sink into the floor and disappear.	Marschall et al. 1994
	S2	If I was Casey, I would feel small.	
	S3	If I was Casey, I would feel like I am a bad person.	
	S4	If I was Casey, I would feel humiliated, disgraced.	
	S5	If I was Casey, I would feel worthless, powerless.	
State of Guilt	G1	If I was Casey, I would feel remorse, regret.	Marschall et al. 1994
	G2	If I was Casey, I would feel tension about something I have done.	
	G3	If I was Casey, I couldn't stop thinking about something bad I have done.	
	G4	If I was Casey, I would feel like apologizing, confessing.	
	G5	If I was Casey, I would feel bad about something I have done.	
State of Embarrassment	E1	If I was Casey, I was feeling embarrassed.	Mosher and White 1981
	E2	If I was Casey, I was feeling self-conscious.	
	E3	If I was Casey, I was feeling blushing.	
State of Fear	F1	If I was Casey, I was feeling fearful.	Gleicher and Petty 1992
	F2	If I was Casey, I was feeling nervous.	
	F3	If I was Casey, I was feeling scared.	
	F4	If I was Casey, I was feeling nauseated.	

	F5	If I was Casey, I was feeling uncomfortable.	
Perceived Presence of Onlooker	PPO1	Referring to the above scenario, someone could see Casey at the time of copying data to a USB drive.	Developed for this study
	PPO2	Referring to the above scenario, Casey's seating position makes other employees able to see what he was doing.	
Perceived Onlooker Threat	POT1	Referring to the above scenario, someone would report Casey's violation behavior.	Developed for this study
	POT2	Referring to the above scenario, there were people around Casey who were likely to report his seen violation behavior.	
Scenario Realism: (1-10 scale) How realistic do you think the scenario you were just presented with is?			
Demographic questions: 1. What is your gender? 2. How old are you (in years)? 3. Please select one that best describe your ethnicity. 4. What is the highest level of education you have completed? 5. What is your employment status? 6. If you are employed, what is your company size? (Number of employees) 7. Which item best described your position in the company? 8. Which Industry your company belongs to? 9. How many years of work experience you have? 10. How many years have you worked for your current employer? 11. Could your current position and job duties be considered as an "IT Professional" position? (Yes/No) 12. Are you currently involved with implementing information security management plan in the organization? (Yes/No) 13. If yes, please describe one of your recent related job duties. 14. On average, how many hours per day do you use a computer at work (or for work)? 15. how you evaluate your computer knowledge status?(give us a number between 1-7) 16. Please describe one information security requirement in their organization.			

BIBLIOGRAPHY

Ahmed, E., Harris, N., Braithwaite, J., and Braithwaite, V. 2001. *Shame Management Through Reintegration*, Cambridge University Press.

Ajzen, I. 1991. “The Theory of Planned Behavior,” *Organizational Behavior and Human Decision Processes* (50:2), pp. 179–211.

Ashton-James, C. E., and Ashkanasy, N. M. 2008. “Affective Events Theory: A Strategic Perspective,” in *Emotions, Ethics, and Decision-Making*, Emerald Group Publishing Limited, pp. 1–34.

Basch, J., and Fisher, C. D. 1998. “Affective Events - Emotions Matrix: A Classification of Work Events and Associated Emotions,” *School of Business Discussion Papers* (65), p. 23.

Bastin, C., Harrison, B. J., Davey, C. G., Moll, J., and Whittle, S. 2016. “Feelings of Shame, Embarrassment and Guilt and Their Neural Correlates: A Systematic Review,” *Neuroscience & Biobehavioral Reviews* (71), pp. 455–471. (https://doi.org/10.1016/j.neubiorev.2016.09.019).

Baumeister, R. F., and Leary, M. R. 1995. “The Need to Belong: Desire for Interpersonal Attachments as a Fundamental Human Motivation,” *Psychological Bulletin* (117:3), p. 33.

Block, L. G., and Keller, P. A. 1995. “When to Accentuate the Negative: The Effects of Perceived Efficacy and Message Framing on Intentions to Perform a Health-Related Behavior,” *Journal of Marketing Research (JMR)* (32:2), pp. 192–203. (https://doi.org/10.2307/3152047).

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. “If Someone Is Watching, I’ll Do What I’m Asked: Mandatoriness, Control, and Information Security,” *European Journal of Information Systems* (18:2), pp. 151–164. (https://doi.org/10.1057/ejis.2009.8).

Boster, F. J., Cruz, S., Manata, B., DeAngelis, B. N., and Zhuang, J. 2016. “A Meta-Analytic Review of the Effect of Guilt on Compliance,” *Social Influence* (11:1), pp. 54–67. (https://doi.org/10.1080/15534510.2016.1142892).

Braithwaite, J. 1989. *Crime, Shame and Reintegration*, Cambridge University Press.

Brief, A. P. 2001. “Organizational Behavior and the Study of Affect: Keep Your Eyes on the Organization,” *Organizational Behavior and Human Decision Processes* (86:1), pp. 131–139. (https://doi.org/10.1006/obhd.2001.2975).

Bulgurcu, Cavusoglu, and Benbasat. 2010. “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness,” *MIS Quarterly* (34:3), p. 523. (https://doi.org/10.2307/25750690).

Chea, S., and Luo, M. M. 2009. “EService Customer Retention: An Affective Events Theory Perspective,” in *AMCIS 2009 Proceedings*, p. 12.

Cheng, L., Li, Y., Li, W., Holm, E., and Zhai, Q. 2013. “Understanding the Violation of IS Security Policy in Organizations: An Integrated Model Based on Social Control and Deterrence Theory,” *Computers & Security* (39), pp. 447–459. (https://doi.org/10.1016/j.cose.2013.09.009).

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. (https://doi.org/10.1287/isre.14.2.189.16018).

Cialdini, R. B., Borden, R. J., Thorne, A., Walker, M. R., Freeman, S., and Sloan, L. R. 1976. “Basking in Reflected Glory: Three (Football) Field Studies,” *Journal of Personality and Social Psychology* (34:3), pp. 366–375.

Cialdini, R. B., Darby, B. L., and Vincent, J. E. 1973. “Transgression and Altruism: A Case for Hedonism,” *Journal of Experimental Social Psychology* (9:6), pp. 502–516. (https://doi.org/10.1016/0022-1031(73)90031-0).

Cohen, J. 1988. *Statistical Power Analysis for the Behavioral Sciences*, (2nd edition.), Hillsdale, New Jersey: Lawrence Erlbaum Associates.

Cozens, P. M., Saville, G., and Hillier, D. 2005. “Crime Prevention through Environmental Design (CPTED): A Review and Modern Bibliography,” *Property Management* (23:5), pp. 328–356.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. “Future Directions for Behavioral Information Security Research,” *Computers & Security* (32), pp. 90–101. (https://doi.org/10.1016/j.cose.2012.09.010).

Dang-Pham, D., Pittayachawan, S., and Bruno, V. 2014. *Towards a Complete Understanding of Information Security Misbehaviours: A Proposal for Future Research with Social Network Approach*, ACIS.

Daniels, M. A., and Robinson, S. L. 2019. “The Shame of It All: A Review of Shame in Organizational Life,” *Journal of Management* (45:6), pp. 2448–2473. (https://doi.org/10.1177/0149206318817604).

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), pp. 643–658. (https://doi.org/10.1057/ejis.2011.23).

D’Arcy, J., and Hovav, A. 2007. “Deterring Internal Information Systems Misuse,” *Communications of the ACM* (50:10), pp. 113–117. (https://doi.org/10.1145/1290958.1290971).

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.

D’Arcy, J., and Lowry, P. B. 2019. “Cognitive-affective Drivers of Employees’ Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study,” *Information Systems Journal* (29:1), pp. 43–69. (https://doi.org/10.1111/isj.12173).

David, J. 2002. “Policy Enforcement in the Workplace,” *Computers & Security* (21:6), pp. 506–513.

De Rivera, J. 1984. “The Structure of Emotional Relationships,” *Review of Personality & Social Psychology* (5), pp. 116–145.

Farshadkhah, S., and Stafford, T. 2019. “The Role of ‘Eyes of Others’ in Security Violation Prevention: Measures and Constructs,” in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, p. 9.

Fischer, P., Krueger, J. I., Greitemeyer, T., Vogrincic, C., Kastenmüller, A., Frey, D., Heene, M., Wicher, M., and Kainbacher, M. 2011. “The Bystander-Effect: A Meta-Analytic Review on Bystander Intervention in Dangerous and Non-Dangerous Emergencies.,” *Psychological Bulletin* (137:4), pp. 517–537. (https://doi.org/10.1037/a0023304).

Fisher, C. D. 2000. “Mood and Emotions While Working: Missing Pieces of Job Satisfaction?,” *Journal of Organizational Behavior* (21), pp. 185–0202.

Fisher, C. D. 2002. “Antecedents and Consequences of Real-Time Affective Reactions at Work,” *Motivation and Emotion*, p. 30.

Forgas, J. P., and George, J. M. 2001. “Affective Influences on Judgments and Behavior in Organizations: An Information Processing Perspective,” *Organizational Behavior and Human Decision Processes* (86:1), pp. 3–34. (https://doi.org/10.1006/obhd.2001.2971).

Frijda, N. H. 1993. “Moods, Emotion Episodes, and Emotions,” in *Handbook of Emotions*, New York, NY, US: Guilford Press, pp. 381–403.

Fuller, J. A., Stanton, J. M., Fisher, G. G., Spitzmüller, C., Russell, S. S., and Smith, P. C. 2003. “A Lengthy Look at the Daily Grind: Time Series Analysis of Events, Mood, Stress, and Satisfaction.,” *Journal of Applied Psychology* (88:6), pp. 1019–1033. (https://doi.org/10.1037/0021-9010.88.6.1019).

Gefen, D., Rigdon, E. E., and Straub, D. 2011. “Editor’s Comments: An Update and Extension to SEM Guidelines for Administrative and Social Science Research,” *MIS Quarterly* (35:2), iii–xiv. (https://doi.org/10.2307/23044042).

Gefen, D., and Straub, D. 2005. “A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example,” *Communications of the AIS*, pp. 91–109.

Gleicher, F., and Petty, R. E. 1992. *Expectations of Reassurance Influence the Nature of Fear-Stimulated Attitude Change☆*. (https://doi.org/10.1016/0022-1031(92)90033-G).

Goo, J., Yim, M., and Kim, D. J. 2014. “A Path to Successful Management of Employee Security Compliance: An Empirical Study of Information Security Climate,” *IEEE Transactions on Professional Communication* (57:4), pp. 286–308. (https://doi.org/10.1109/TPC.2014.2374011).

Grasmick, H. G., and Bursik, R. J. 1990. “Conscience, Significant Others, and Rational Choice: Extending the Deterrence Model,” *Law & Society Review* (24:3), pp. 837–861. (https://doi.org/10.2307/3053861).

Guerin, B. 1986. “Mere Presence Effects in Humans: A Review,” *Journal of Experimental Social Psychology* (22:1), pp. 38–77. (https://doi.org/10.1016/0022-1031(86)90040-5).

Hair, J. F., Hult, G. T. M., Ringle, C. M., and Sarstedt, M. 2017. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, (Second edition.), Los Angeles: SAGE Publications.

Herath, T., and Rao, H. R. 2009. “Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness,” *Decision Support Systems* (47:2), pp. 154–165. (https://doi.org/10.1016/j.dss.2009.02.005).

Hoffman, M. L. 1973. *Empathy, Role-Taking, Guilt, and Development of Altruistic Motives*. (https://files.eric.ed.gov/fulltext/ED085109.pdf).

de Hooge, I. E., Zeelenberg, M., and Breugelmans, S. M. 2010. “Restore and Protect Motivations Following Shame,” *Cognition & Emotion* (24:1), pp. 111–127. (https://doi.org/10.1080/02699930802584466).

Hu, Q., Dinev, T., Hart, P., and Cooke, D. 2012. “Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*: Managing Employee Compliance with Information Security Policies,” *Decision Sciences* (43:4), pp. 615–660. (https://doi.org/10.1111/j.1540-5915.2012.00361.x).

Izard, C. E. 1977. *Human Emotions*, New York: Plenum Press.

Izard, C. E. 1991. *The Psychology of Emotions*, Springer Science & Business Media.

Janis, I. L. 1967. “Effects of Fear Arousal on Attitude Change: Recent Developments in Theory and Experimental Research1,” in *Advances in Experimental Social Psychology* (Vol. 3), L. Berkowitz (ed.), Academic Press, pp. 166–224. (https://doi.org/10.1016/S0065-2601(08)60344-5).

Johnston, A. C., and Warkentin, M. 2010a. “Fear Appeals and Information Security Behaviors: An Empirical Study,” *MIS Quarterly* (34:3), pp. 549–566. (https://doi.org/10.2307/25750691).

Johnston, A. C., and Warkentin, M. 2010b. “Fear Appeals and Information Security Behaviors: An Empirical Study,” *MIS Quarterly* (34:3), pp. 549–566. (https://doi.org/10.2307/25750691).

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., and Wei, K.-K. 2003. “An Integrative Study of Information Systems Security Effectiveness,” *International Journal of Information Management* (23:2), pp. 139–154. (https://doi.org/10.1016/S0268-4012(02)00105-6).

Kaufman, B. E. 1999. “Emotional Arousal as a Source of Bounded Rationality,” *Journal of Economic Behavior & Organization* (38:2), pp. 135–144. (https://doi.org/10.1016/S0167-2681(99)00002-5).

Kelman, H. C. 1958. “Compliance, Identification, and Internalization Three Processes of Attitude Change,” *Journal of Conflict Resolution* (2:1), pp. 51–60. (https://doi.org/10.1177/002200275800200106).

Klepper, S., and Nagin, D. 1989. “The Deterrent Effect of Perceived Certainty and Severity of Punishment Revisited,” *Criminology* (27:4), pp. 721–746.

Kligyte, V., Connelly, S., Thiel, C., and Devenport, L. 2013. “The Influence of Anger, Fear, and Emotion Regulation on Ethical Decision Making,” *Human Performance* (26:4), pp. 297–326. (https://doi.org/10.1080/08959285.2013.814655).

Kugler, K., and Jones, W. H. 1992. “On Conceptualizing and Assessing Guilt,” *Journal of Personality and Social Psychology* (62:2), pp. 318–327.

Lazarus, R. S. 1966. *Psychological Stress and the Coping Process*, Psychological Stress and the Coping Process, New York, NY, US: McGraw-Hill.

Lazarus, R. S. 1991. “Progress on a Cognitive-Motivational-Relational Theory of Emotion,” *American Psychologist* (46:8), pp. 819–834.

Leary, M. R. 1990. “Responses to Social Exclusion: Social Anxiety, Jealousy, Loneliness, Depression, and Low Self-Esteem,” *Journal of Social and Clinical Psychology* (9:2), pp. 221–229. (https://doi.org/10.1521/jscp.1990.9.2.221).

Leary, M. R. 2005. “Sociometer Theory and the Pursuit of Relational Value: Getting to the Root of Self-Esteem,” *European Review of Social Psychology* (16:1), pp. 75–111. (https://doi.org/10.1080/10463280540000007).

Leary, M. R. 2012. “Sociometer Theory,” in *Handbook of Theories of Social Psychology*, Los Angeles: SAGE, pp. 141–159.

Leary, M. R., and Baumeister, R. F. 2000. “The Nature and Function of Self-Esteem: Sociometer Theory,” in *Advances in Experimental Social Psychology* (Vol. 32), Academic Press, pp. 1–62. (https://doi.org/10.1016/S0065-2601(00)80003-9).

Leary, M. R., Terdal, S. K., Tambor, E. S., and Downs, D. L. 1995. “Self-Esteem as an Interpersonal Monitor: The Sociometer Hypothesis,” *Journal of Personality and Social Psychology* (68:3), pp. 518–530.

Lerner, J. S., Gonzalez, R. M., Small, D. A., and Fischhoff, B. 2003. “Effects of Fear and Anger on Perceived Risks of Terrorism: A National Field Experiment,” *Psychological Science* (14:2), pp. 144–150.

Lerner, J. S., and Keltner, D. 2000. “Beyond Valence: Toward a Model of Emotion-Specific Influences on Judgement and Choice,” *Cognition & Emotion* (14:4), pp. 473–493. (https://doi.org/10.1080/026999300402763).

Lerner, J. S., and Keltner, D. 2001. “Fear, Anger, and Risk,” *Journal of Personality and Social Psychology* (81:1), p. 146.

Lewis, M. 1995. *Shame: The Exposed Self*, Simon and Schuster.

Lickel, B., Kushlev, K., Savalei, V., Matta, S., and Schmader, T. 2014. “Shame and the Motivation to Change the Self.,” *Emotion* (14:6), pp. 1049–1061. (https://doi.org/10.1037/a0038235).

Lindell, M. K., and Whitney, D. J. 2001. “Accounting for Common Method Variance in Cross-Sectional Research Designs.,” *Journal of Applied Psychology* (86:1), pp. 114–121. (https://doi.org/10.1037//0021-9010.86.1.114).

Lowry, P. B., and Gaskin, J. 2014. “Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It,” *IEEE Transactions on Professional Communication* (57:2), pp. 123–146. (https://doi.org/10.1109/TPC.2014.2312452).

Lowry, P. B., and Moody, G. D. 2015. “Proposing the Control-Reactance Compliance Model (CRCM) to Explain Opposing Motivations to Comply with Organisational Information Security Policies: Proposing the Control-Reactance Compliance Model (CRCM),” *Information Systems Journal* (25:5), pp. 433–463. (https://doi.org/10.1111/isj.12043).

Mackenzie, S. B. 2001. “Opportunities for Improving Consumer Research through Latent Variable Structural Equation Modeling,” *Journal of Consumer Research* (28:1), pp. 159–166. (https://doi.org/10.1086/321954).

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. “Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model,” *Information Systems Research* (15:4), pp. 336–355. (https://doi.org/10.1287/isre.1040.0032).

Marschall, D., Sanftner, J., and Tangney, J. P. 1994. *The State Shame and Guilt Scale*, Fairfax, VA: George Mason University. (https://gospel-app.com/wp-content/uploads/2018/10/SSGS.pdf).

Mosher, D. L., and White, B. B. 1981. “On Differentiating Shame and Shyness,” *Motivation and Emotion* (5:1), pp. 61–74. (https://doi.org/10.1007/BF00993662).

Murphy, S. A., and Kiffin-Petersen, S. 2017. “The Exposed Self: A Multilevel Model of Shame and Ethical Behavior,” *Journal of Business Ethics* (141:4), pp. 657–675. (https://doi.org/10.1007/s10551-016-3185-8).

Nagin, D. S., and Paternoster, R. 1993. “Enduring Individual Differences and Rational Choice Theories of Crime,” *Law & Society Review* (27:3), pp. 467–496. (https://doi.org/10.2307/3054102).

Nicolini, D., Hartley, J., Stansfield, A., and Hurcombe, J. 2011. “Through the Eyes of Others: Using Developmental Peer Reviews to Promote Reflection and Change in Organizations,” *Journal of Organizational Change Management* (24:2), (O. Eikeland, ed.), pp. 211–228. (https://doi.org/10.1108/09534811111119771).

Paternoster, R., and Simpson, S. 1993. “A Rational Choice Theory of Corporate Crime,” in *Routine Activity and Rational Choice* (Vol. 5), Transaction Publishers, pp. 37–58.

Paternoster, R., and Simpson, S. 1996. “Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime,” *Law & Society Review* (30:3), p. 549. (https://doi.org/10.2307/3054128).

Pavlou, Liang, and Xue. 2007. “Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective,” *MIS Quarterly* (31:1), p. 105. (https://doi.org/10.2307/25148783).

Pirola-Merlo, A., Härtel, C., Mann, L., and Hirst, G. 2002. “How Leaders Influence the Impact of Affective Events on Team Climate and Performance in R&D Teams,” *The Leadership Quarterly* (13:5), pp. 561–581. (https://doi.org/10.1016/S1048-9843(02)00144-3).

Plutchik, R. 1994. *The Psychology and Biology of Emotion*, The Psychology and Biology of Emotion, New York, NY, US: HarperCollins College Publishers.

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.,” *Journal of Applied Psychology* (88:5), pp. 879–903. (https://doi.org/10.1037/0021-9010.88.5.879).

Pogarsky, G. 2004. “Projected Offending and Contemporaneous Rule-Violation: Implications for Hetrotypic Continuity,” *Criminology* (42:1), pp. 111–136. (https://doi.org/10.1111/j.1745-9125.2004.tb00515.x).

Ponemon Institute. 2018. “2018 Cost of a Data Breach Study: Global Overview,” Ponemon Institute, July. (https://www.ibm.com/downloads/cas/861MNWN2).

PwC. 2017. “The Global State of Information Security® Survey 2018,” , October 18. (https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html, accessed January 22, 2019).

Ringle, C. M., Sarstedt, M., and Straub, D. W. 2012. “Editor’s Comments: A Critical Look at the Use of PLS-SEM in ‘MIS Quarterly,’” *MIS Quarterly* (36:1), iii–xiv. (https://doi.org/10.2307/41410402).

Sabini, J., Garvey, B., and Hall, A. L. 2001. “Shame and Embarrassment Revisited,” *Personality and Social Psychology Bulletin* (27:1), pp. 104–117. (https://doi.org/10.1177/0146167201271009).

Scheff, T. J. 1984. “The Taboo on Coarse Emotions,” *Review of Personality & Social Psychology* (5), pp. 146–169.

Scherer, K. R. 2004. “Feelings Integrate the Central Representation of Appraisal-Driven Response Organziation in Emotion,” in *Feelings and Emotions: The Amsterdam Symposium*, Cambridge University Press, pp. 136–157.

Scherer, K. R. 2005. “What Are Emotions? And How Can They Be Measured?,” *Social Science Information* (44:4), pp. 695–729.

Sergeeva, A., Huysman, M., Soekijad, M., and van den Hooff, B. 2017. “Through the Eyes of Others: How Onlookers Shape the Use of Technology at Work,” *MIS Quarterly* (41:4).

Simpson, S. 2000. *Of Crime and Criminality: The Use of Theory in Everyday Life*, SAGE Publications.

Siponen, M., and Vance, A. 2010. “Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations,” *MIS Quarterly* (34:3), pp. 487–502. (https://doi.org/10.2307/25750688).

Siponen, M., Vance, A., and Willison, R. 2012. “New Insights into the Problem of Software Piracy: The Effects of Neutralization, Shame, and Moral Beliefs,” *Information & Management* (49:7–8), pp. 334–341. (https://doi.org/10.1016/j.im.2012.06.004).

Smith, C. A., and Ellsworth, P. C. 1985. “Patterns of Cognitive Appraisal in Emotion.,” *Journal of Personality and Social Psychology* (48:4), pp. 813–838. (https://doi.org/10.1037/0022-3514.48.4.813).

Stam, K. R., and Stanton, J. M. 2010. “Events, Emotions, and Technology: Examining Acceptance of Workplace Technology Changes,” *Information Technology & People* (23:1), pp. 23–53. (https://doi.org/10.1108/09593841011022537).

Tangney, J. P., and Dearing, R. L. 2003. *Shame and Guilt*, Guilford Press.

Tangney, J. P., Miller, R. S., Flicker, L., and Barlow, D. H. 1996. “Are Shame, Guilt, and Embarrassment Distinct Emotions?,” *Journal of Personality and Social Psychology* (70:6), pp. 1256–1269.

Tangney, J. P., Stuewig, J., and Mashek, D. J. 2007. “Moral Emotions and Moral Behavior,” *Annual Review of Psychology* (58), pp. 345–372. (https://doi.org/10.1146/annurev.psych.56.091103.070145).

Tangney, J. P., and Tracy, J. L. 2012. “Self-Conscious Emotions,” in *Handbook of Self and Identity, 2nd Ed*, New York, NY, US: The Guilford Press, pp. 446–478.

Taylor, S. E. 1991. “Asymmetrical Effects of Positive and Negative Events: The Mobilization-Minimization Hypothesis,” *Psychological Bulletin* (110:1), p. 19.

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

Tracy, J. L., and Robins, R. W. 2004. “Putting the Self into Self-Conscious Emotions: A Theoretical Model,” *Psychological Inquiry* (15:2), pp. 103–125.

Tracy, J. L., Robins, R. W., and Tangney, J. P. (eds.). 2007. *The Self-Conscious Emotions: Theory and Research*, New York: Guilford Press.

Trevino, L. K. 1992. "Experimental Approaches to Studying Ethical-Unethical Behavior in Organizations," *Business Ethics Quarterly* (2:2), pp. 121–136. (https://doi.org/10.2307/3857567).

Tyler, J. M. 2008. "In the Eyes of Others: Monitoring for Relational Value Cues," *Human Communication Research* (34:4), pp. 521–549. (https://doi.org/10.1111/j.1468-2958.2008.00331.x).

Vance, A., Lowry, P. B., and Eggett, D. 2013. "Using Accountability to Reduce Access Policy Violations in Information Systems," *Journal of Management Information Systems* (29:4), pp. 263–290.

Vieira da Cunha, J. 2013. "A Dramaturgical Model of the Production of Performance Data," *MIS Quarterly* (37:3), pp. 723–748. (https://doi.org/10.25300/MISQ/2013/37.3.03).

Vroom, C., and Von Solms, R. 2004. "Towards Information Security Behavioural Compliance," *Computers & Security* (23:3), pp. 191–198. (https://doi.org/10.1016/j.cose.2004.01.012).

Wang, Y., Meister, D. B., and Gray, P. H. 2013. "Social Influence and Knowledge Management Systems Use: Evidence from Panel Data," *MIS Quarterly* (37:1), pp. 299–313. (https://doi.org/10.25300/MISQ/2013/37.1.13).

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18:2), pp. 101–105. (https://doi.org/10.1057/ejis.2009.12).

Weber, J. 1992. "Scenarios in Business Ethics Research: Review, Critical Assessment, and Recommendations," *Business Ethics Quarterly* (2:2), pp. 137–160. (https://doi.org/10.2307/3857568).

Weiner, B. 1985. "An Attributional Theory of Achievement Motivation and Emotion.," *Psychological Review* (92:4), pp. 548–573. (https://doi.org/10.1037/0033-295X.92.4.548).

Weiss, H. M., and Cropanzano, R. 1996. "Affective Events Theory: A Theoretical Discussion of The Structure, Cause and Consequences of Affective Experiences at Work," *Research in Organziational Behavior* (18), pp. 1–74.

Whitman, M. E. 2004. "In Defense of the Realm: Understanding the Threats to Information Security," *International Journal of Information Management* (24:1), pp. 43–57. (https://doi.org/10.1016/j.ijinfomgt.2003.12.003).

Wicker, F. W., Payne, G. C., and Morgan, R. D. 1983. “Participant Descriptions of Guilt and Shame,” *Motivation and Emotion* (7:1), pp. 25–39. (https://doi.org/10.1007/BF00992963).

Zhang, P. 2013. “The Affective Response Model: A Theoretical Framework of Affective Concepts and Their Relationships in the ICT Context,” *MIS Quarterly* (37:1), pp. 247–274.