Journal of the Association for Information Systems (2019) **20**(12), 1794-1843
**doi:** 10.17705/1jais.00586

RESEARCH PAPER

ISSN 1536-9323

# Integrating Cognition with an Affective Lens to Better Understand Information Security Policy Compliance

**Dustin Ormond[1], Merrill Warkentin[2], Robert E. Crossler[3]**

[1]Creighton University, USA, dustinormond@creighton.edu
[2]Mississippi State University, USA, m.warkentin@msstate.edu
[3]Washington State University, USA, rob.crossler@wsu.edu

## Abstract

Information systems security behavioral research has primarily focused on individual *cognitive processes* and their impact on information security policy noncompliance. However, *affective processes* (operationalized by affective absorption and affective flow) may also significantly contribute to misuse or information security policy noncompliance. Our research study evaluated the impact of affective absorption (i.e., the trait or disposition to allow one's emotions to drive decision-making) and affective flow (i.e., a state of immersion with one's emotions) on cognitive processes in the context of attitude toward and compliance with information security policies. Our conceptual model was evaluated using a laboratory research design. We found that individuals who were frustrated by work-related tasks experienced negative affective flow and violated information security policies. Furthermore, perceptions of organizational injustice increased negative affective flow. Our findings underscore the need for understanding affective processes as well as cognitive processes which may lead to a more holistic understanding regarding information security policy compliance.

**Keywords:** Affect, Affective Absorption, Affective Flow, Attitude, Compliance, Information Security Policy, Negative Affect, Organizational Injustice.

Fred Neiderman was the accepting senior editor. This research article was submitted on February 28, 2018 and underwent three revisions.

## 1 Introduction

Establishing mandatory security requirements through the creation of information security policies is vital to protecting organizational assets. These policies detail the processes and procedures employees should follow to maintain the security objectives of an organization: confidentiality, integrity, and availability of information and assets (Vroom & von Solms, 2004). Various studies have examined the best procedures to create and effectively apply these policies to encourage information security policy compliance behavior (C. Hsu, J.-N. Lee, & Straub, 2012; Puhakainen & Siponen, 2010; Siponen, 2000; Siponen & Iivari, 2006; Warkentin & Johnston, 2006; Warkentin, Johnston, & Shropshire, 2011), but policy violations continue to be a grave concern (Bulgurcu, Cavusoglu, & Benbasat, 2010; Hu, Xu, Dinev, & Ling, 2011). Despite organizational efforts to deter abuse through information security training, insider abuse is still an ongoing problem (Holdgrafer, 2015; Vormetric, 2016) and is the largest cause for data loss resulting in 42% of all confidential data loss (Emm, 2015). Additionally, insider abuse is continually increasing (Skyhigh Networks, 2015); however, 59.1% of organizations still believe that losses are not due to malicious insiders (R. Richardson, 2011).

In attempting to address this concern, researchers have devoted substantial attention to compliance with information security policies by exploring antecedents

of information security policy compliance intention and behavior (Herath & Rao, 2009b; Johnston & Warkentin, 2010; Johnston, Warkentin, & Siponen, 2015; Keith, Shao, & Steinbart, 2007; Siponen & Vance, 2010). The role and impact of *cognitive appraisals* on information security policy compliance behavior have been the primary focus of previous research. Cognitions are thoughts, awareness, perceptions, attitudes, and beliefs (Newell, 1987) and these cognitive appraisals have typically been explained by theories such as the theory of planned behavior (Ajzen, 1991; Fishbein & Ajzen, 1975; Herath & Rao, 2009b), rational choice theory (Li, Zhang, & Sarathy, 2010; Paternoster & Simpson, 1996; Westland, 1997), deterrence theory (D'Arcy & Herath, 2011), and neutralization theory (Barlow, Warkentin, Ormond, & Dennis, 2013; Siponen & Vance, 2010). Even the substantial body of information security research built upon protection motivation theory and fear appeal theory focuses on cognitive threat and coping appraisals termed "cognitive mediating processes" by Floyd, Prentice-Dunn, & Rogers (2000). In fact, Warkentin, Johnston, Walden, & Straub (2016) found no neurophysiological evidence of actual affective fear response to fear appeal messages. Though these theories have proven to be useful in explaining information security intentions and behaviors, they do not include affective processes and thus may not fully capture the relationships that lead to noncompliance behavior because of their sole focus on cognitive influences. We show how affective processes together with cognitive processes can be useful in explaining information security behaviors.

In an organizational setting, environmental factors may impede the work process, which can adversely affect an employee's success and cause repeated frustration. For example, both personal (e.g., marital and other familial issues) and work-related (e.g., obstacles, constraints, new assignments, new challenges, pressures, conflicts, politics) environmental factors can lead to frustration, and this frustration can lead to negative behaviors in the workplace (Spector, 1978). These behaviors often result from blockage of established workflows, which can prevent an employee from completing a task without violating employer policies (Fries, Wiesche, & Krcmar, 2016). Workplace IT constraints and requirements can be a particularly frustrating source of negative affect (Haag & Eckhardt, 2014). Frustrated employees often seek alternate solutions (or "workarounds" (Alter, 2014) for accomplishing a given task, which may include engaging in noncompliant (but nonmalicious) security behaviors, such as time-saving shortcuts (Willison & Warkentin, 2013). This category of security violations is sometimes termed "volitional" (see figure 1 in Willison and Warkentin, 2013); they are voluntary or intentional. These rule-breaking acts may benefit the employee (e.g., saving time by skipping a procedure), yet may pose a security risk or cause damage to the organization (Guo, Yuan, Archer, & Connelly, 2011). Despite the potential harm to the organization, employees may engage in these noncompliant behaviors (e.g., not locking computer, sharing passwords, delaying software patches) to expeditiously complete their work tasks (Burns, Young, Roberts, Courtney, & Ellis, 2015; Holdgrafer, 2015; Koppel, Smith, Blythe, & Kothari, 2015).

Factors beyond those that are cognitive in nature, particularly affective processes, may offer increased insight regarding information security policy violations. In fact, Zhang (2013) calls for more empirical investigations of the causes and consequences of affect in the context of information systems, including the nature of the stimuli that cause the emotions, in order to gain a more holistic understanding. Affective processes are necessary and important components of rational decision-making (Djamasbi, Strong, & Dishaw, 2010) and often influence cognitive processes such as judgments and decisions (Lerner & Keltner, 2000; Loewenstein, 1996; Russell, 2003). Additionally, emotions influence all forms of behavior and their influence is proportionate to their strength level (Loewenstein, 1996), such that strong emotions may lead individuals to behave contrary to self-interests (Willison & Warkentin, 2013) as they become deeply involved with or immersed in their emotions. For example, positive affect influences decision-making and has been shown to improve efficiency (Isen & Means, 1983), whereas perceived acts of injustice typically activate brain activity associated with negative emotion and are predictive of subsequent behavior (Sanfey, Rilling, & Aronson, 2003). Furthermore, individuals who perceive that they have been treated unfairly by their organization are likely to experience strong emotions as fairness perceptions directly or indirectly influence people's emotions (Cohen-Charash & Spector, 2001). This rationale leads to our primary research questions:

**RQ1:** How do both cognition and affect interplay to influence IS security policy compliance or noncompliance?

**RQ2:** What role does frustration play in the presence of both cognitive and affective responses to situational stimuli?

Because measuring actual behavior when exploring information security phenomena provides better theory validation than collecting behavioral intention (Anderson & Agarwal, 2010; Crossler et al., 2013; Mahmood, Siponen, Straub, Rao, & Raghu, 2010; Straub, 2009; Warkentin, Straub, & Malimage, 2012), the dependent variable in our study is *actual information security policy compliance behavior*

captured in a laboratory setting as a proxy for behavior experienced in an organizational environment. We expand our understanding of information security policy compliance behavior by drawing upon various cognitive and affective theories: (1) the theory of planned behavior (Ajzen, 1991; Fishbein & Ajzen, 1975; Herath & Rao, 2009b); (2) prekinetic events—work-related events that occur prior to abuse (Willison & Warkentin, 2013); and (3) affective events theory (Weiss & Cropanzano, 1996).

Our study utilized a workplace-type task in a laboratory setting to underscore the need for understanding affective processes with regard to information security policy compliance behavior. Specifically, we wanted to explore whether frustrated individuals are more likely to violate information security policies in order to complete their work-related tasks, which required that some of the subjects were frustrated. Similar to the organizational setting described above, we created a situation in which experimental subjects needed to perform well on a simulated workplace task to be successful. Though workplace tasks can cause inherent frustration themselves (and though outside personal factors can also contribute toward feelings of frustration during workplace activities), to ensure relatively equal distribution of frustration, the simulated task was designed to induce varying levels of frustration among the subjects. Much like in the work environment (Forman & Watkins, 2009) and despite any well-intentioned reason for committing violations, frustrated subjects are likely to violate existing policies (e.g., password management) due to the frustration they experience from repeatedly completing frustrating tasks.

The remainder of this paper is organized as follows. In Section 2, we review the relevant research and lay the theoretical foundation for our study. In Section 3, we present the research model with its associated hypotheses. In Section 4, we detail the research method. In Section 5, we describe the data analysis and present the results. In Section 6, we discuss implications for research and practice, limitations, and future research. In Section 7, we conclude with a summary of our contributions.

# 2 Literature Review and Theoretical Framework

Cognitive theories such as rational choice theory and deterrence theory have successfully evaluated why individuals engage in deviant cybersecurity behavior and have informed us about how to better motivate positive behavior through the application of sanctions (D'Arcy & Herath, 2011; D'Arcy, Hovav, & Galletta, 2009; Gopal & Sanders, 1997; Herath & Rao, 2009b; Herrnstein, 1990; Onwudiwe, Odo, & Onyeozili, 2005; Peace, Galletta, & Thong, 2003; Simon, 1947, 1952) or through persuasive messaging such as "fear appeals" (Boss, Galletta, Lowry, Moody, & Polak, 2015; Johnston & Warkentin, 2010; Johnston, Warkentin, Dennis, & Siponen, 2019; Johnston et al., 2015). Even if robust, the implications that can be drawn from these theories are limited, in part because human behavior is often characterized by nonrational processes (Dennis; & Minas, 2018). Scholars are currently identifying new theoretical lenses to explain and predict both positive and negative cybersecurity behaviors, and our understanding of these phenomena can be greatly enhanced by extending current theories with new constructs, by testing the boundary conditions of these theories, by contextualizing other theories to these behaviors, and by developing new theories. Willison and Warkentin (2013) identified prekinetic events (i.e., neutralization, disgruntlement, organizational injustice, and expressive motives) that may reduce the effectiveness of these deterrent techniques. Additionally, other studies have explored diverse cognitive influences such as the impact of neutralization (Barlow et al., 2013; Barlow, Warkentin, Ormond, & Dennis, 2018; Siponen & Vance, 2010), unethical use of IT (Chatterjee, Sarker, & Valacich, 2015), accountability (Vance, Lowry, & Eggett, 2013), self-control (Hu, West, & Smarandescu, 2015), and nonmalicious security violations (Guo et al., 2011). Nevertheless, information security behavior research has primarily focused on cognition, whereas affect, which is noncognitive in character (Baskerville, Park, & Kim, 2010) and which influences reflexes, perceptions, cognitions, and behavior (Lerner & Keltner, 2000; Loewenstein, 1996; Russell, 2003), has received little attention. This is alarming, given that affect has been shown to override rational deliberations (Carmichael & Piquero, 2004). Additionally, affect infiltrates nearly every aspect of decision-making (Carmichael & Piquero, 2004). Therefore, understanding its role in information security behavior may lead to a more holistic view of what motivates compliant and noncompliant behaviors. As research in this domain progresses and as these research streams converge, the results will reveal greater insights that will likely illuminate why employees and others continue to engage in deviant behavior despite all the safeguards in place.

## 2.1 Affect and Affective Events Theory

Affect is an umbrella term for a set of more specific concepts that include emotions, moods, and feelings (Bagozzi, Gopinath, & Nyer, 1999; Russell, 2003; Zhang, 2013). An individual's core affect can be broken into two dimensions: trait affect and state affect (Carmichael & Piquero, 2004). Trait affect drives a person's mood, defined as the enduring predominance of certain types of subjective feelings that have no stimulus or quasi-stimulus (Russell, 2003; Scherer,

2005). Trait affect is important to understand as it impacts an individual's reflexes, perception, cognition, and behavior (Russell, 2003). Essentially, trait affect is the relatively stable tendency to experience certain emotions over time which are not subject to stimuli. These tendencies have been shown to moderate existing relationships and influence key constructs such as job satisfaction, performance, and job turnover (Judge, 1993; Weiss & Cropanzano, 1996). On the other hand, state affect is the mental state of readiness that arises from cognitive appraisals of events or thoughts (Bagozzi et al., 1999) and is determined by five different appraisals: situational state, probability, agency, motivational state, and power (Roseman, Spindel, & Jose, 1990). In other words, trait affect is engrained into the person's being, while state affect is triggered by a certain event or thought.

Knowing that affect influences judgment, attitude, and behavior, we examined affective events theory as the foundational theory that guides this study. Affective events theory (1) focuses on the structure, causes, and consequences of affective experiences, (2) directs attention to events as proximal causes of affective reactions, (3) includes time as a critical parameter between affect and satisfaction, and (4) considers the structure of affective reactions as important as the structure of environments (Weiss & Cropanzano, 1996). For instance, an employee may affectively react (e.g., with anger) to a work-related event (e.g., organizational injustice) which may lead to severe consequences for the organization (e.g., system misuse or policy noncompliance). Additionally, Weiss and Cropanzano (1996) state that individuals with greater dispositions toward negative affect are likely to have more intense bouts of emotion and react stronger when negative events occur. By paying attention to affective experiences over time, organizations may be able to "calm the flames" before anything disastrous happens to organizational assets and information. Using affective events theory and prior literature as a foundation, we introduce two new constructs, *affective absorption and affective flow*, which inform our study and enable us to further understand attitudes and behaviors specifically related to information security policies.

## 2.2 Affective Absorption

Absorption is the trait or disposition to devote all attentional resources to an object of attention (Tellegen & Atkinson, 1974). Roche and McConkey (1990, p. 91) summarize absorption as the "readiness for experiences of deep involvement, a heightened sense of the reality of the attentional object, an imperviousness to normally distracting events, and an appraisal of information in unconventional and idiosyncratic ways." In essence, it is an individual's "openness to absorbing and self-altering experiences" (Tellegen & Atkinson, 1974, p. 268). Absorption has been applied to cognitive IT-mediated activities that are cognitively engaging, resulting in an immersive interaction with technology that can result in temporal disassociation and heightened enjoyment (Agarwal & Karahanna, 2000). However, in this study, we apply absorption by specifically looking at the degree to which an *individual's disposition is to devote attentional resources to emotions rather than to an object of attention*.

This disposition is a permanent trait of individuals, and the extent to which they become deeply absorbed in their emotions may differ drastically from one individual to another. Based on this theoretical foundation, we posit that affective absorption is the trait or disposition to allow emotions to drive the decision-making process to the point that it renders individuals unable to register the passage of time, results in total engagement with these emotions to the point that nothing else matters, and leads to a lack of control over one's emotions. In other words, this is basically an inherent trait that causes an individual's emotions to become the predominant motivator for decision-making to the point that cognitive reasoning may be completely set aside in certain situations. Two central aspects of affective absorption include *positive affective absorption*, the disposition to allow positive emotions to drive decision-making, and *negative affective absorption*, the disposition to allow negative emotions to drive decision-making. In essence, a person who is affectively absorbed may have stronger and deeper reactions to emotion-inducing events.

## 2.3 Affective Flow

Flow is defined as "the state in which people are so involved in an activity that nothing else seems to matter…even at great cost" (Csikszentmihaiyi, 1990, p. 4). Essentially, a person in a state of flow feels as if time stands still because he or she becomes one with a task, believing that nothing else matters (Agarwal & Karahanna, 2000; Csikszentmihaiyi, 1990). In this state, an individual's attention will be consumed by the object of attention (Agarwal & Karahanna, 2000). This level of focused attention influences attitudes toward information systems and information systems adoption decisions (Trevino & Webster, 1992; Zhang, Li, & Sun, 2006). For example, individuals who enjoy browsing the web or playing video games will experience strong hedonic emotions which may cause them to neglect other aspects of their life.

Emotion is defined as a mental state of readiness that arises from cognitive appraisals of events or thoughts (Bagozzi et al., 1999). Compared to moods, emotions are typically more intense, shorter in duration, and have specificity with regard to a particular object or behavioral response (Weiss & Cropanzano, 1996). Eventually, these emotions or affective states direct and

motivate behavior (Ilies & Judge, 2002); therefore, they should be properly regulated. Heilman et al. (2010) discuss the impact of emotion regulation (i.e., the effort to control emotion-inducing experiences) on risk-taking decisions and found that cognitive reappraisal of emotion may lead to high risk-taking decisions while expressive suppression (e.g., facial expressions, verbal utterances, gestures) does not decrease risk aversion because it does not regulate the unpleasant feelings. Additionally, Seo and Barrett (2007, p. 923) determined that "individuals who were better able to identify and distinguish among their current feelings achieved higher decision-making performance via their enhanced ability to control the possible biases induced by those feelings." Subsequent studies have also indicated that the regulation of emotions promotes optimal decisions (Heilman et al., 2010; Seo & Barrett, 2007). It also reduces behavioral and psychological loss aversion in financial situations (Sokol-Hessner et al., 2009; Sokol-Hessner, Camerer, & Phelps, 2013) and susceptibility to framing (Miu & Crisan, 2011). Given the impact that states of affect can have on specific behaviors, emotional responses need to be regulated so as not to interfere with rational thought processes (Yang, Tang, Gu, Luo, & Luo, 2014).

In this study, informed by the literature about flow and emotional regulation, we posit that an individual's level of state affect can cause him or her to have difficulty registering the passage of time, feel that nothing else matters, and lack emotional control. An individual's attention can be consumed by emotions rather than by an object of attention itself. In this state, unfettered emotions can spiral out of control and can drastically influence behavior. Conversely, positive emotions may also lead to impulse-driven behaviors, such as discrete acts of organizational citizenship behaviors, whereas negative emotions may trigger negative short-term events (such as policy violations) as well as longer-term outcomes, such as job turnover, patterns of deviance, or other withdrawal behaviors. For example, an employee who feels he or she has been mistreated by his or her organization may experience a state of anger. Users with a negative affective response, "adopt clear coping strategies of self-preservation or disturbance handling" (Stein, Newell, Wagner, & Galliers, 2015, p. 387). Although the event-driven anger may be intense and short-lived, this employee may impulsively react negatively toward the organization.

Based on the prior literature, we derive the construct *affective flow* and define it as the state of immersion with one's emotions that leads to the point that nothing else matters. Essentially, affective flow differs from flow in that an individual focuses on emotions rather than an object of attention itself. As with affective absorption, affective flow also manifests itself in two ways: (1) positive affective flow, the state of immersion with positive emotions, and (2) negative affective flow, the state of being immersed in negative emotions. In the latter case, employees may experience negative affective flow to the extent that nothing else matters other than quenching their emotions through detrimental actions such as insider abuse or noncompliance with information security policies.

In summary, affective absorption is like the size of a container before emotions completely take over, whereas affective flow is like the volume of emotions inside the respective container. As the container fills up, emotions begin to cloud other judgments (e.g., cognitive evaluations). Depending on the size of the container, this may happen quicker for some individuals than for others. Because nonmalicous security events occur in the moment of task completion, our focus is on the negative emotion of frustration that may cause a security policy violation that the individual may not have enacted under normal circumstances. Therefore, the present study will focus only on the negative side of these affective constructs. Positive affect is further discussed in the limitations and future research section.

# 3 Research Model and Hypotheses

Based on this theoretical foundation, we propose the research model illustrated in Figure 1, which we use to explain information security policy compliance and violation behavior. Consistent with affective events theory (Weiss & Cropanzano, 1996), the model incorporates a sample of cognitive (i.e., organizational injustice), affective (affective absorption and affective flow), and attitudinal states. In this model, fairness (i.e., organizational injustice) is expected to have a negative relationship with negative affective flow. Negative affective flow and attitude toward information security policy are expected to influence information security policy compliance behavior. See Table 1 for the definition and source of each construct in the conceptual model.

## 3.1 Attitude Toward Information Security Policy

According to Hogg and Vaughan (2005, p. 150), an attitude is "a relatively enduring organization of beliefs, feelings, and behavioral tendencies toward socially significant objects, groups, events, or symbols." Therefore, three components of attitude include: (1) a cognitive component that relates to thoughts and beliefs about a subject; (2) an affective component that relates to how the object, person, issue, or event makes one feel; and (3) a behavioral component that relates to how an attitude influences one's behavior.

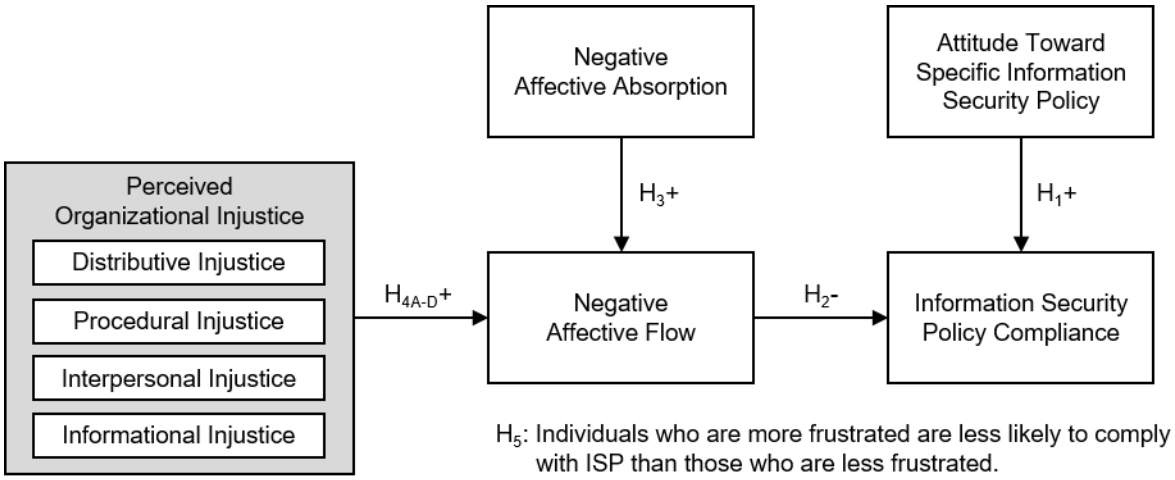


**Figure 1. Conceptual Model with Hypotheses**

**Table 1. Definition and Source of Constructs**

| Variable | Definition | Type | Definition Source |
|---|---|---|---|
| Distributive injustice | The ratio of work outputs (rewards) and input (contributions) to the ratio of a comparative other are perceived to be unfair. | State or event driven | Adams, 1965; Willison & Warkentin, 2013 |
| Procedural injustice | The perceived unfairness of the process by which the outcomes were achieved. | State or event driven | Cohen-Charash & Spector, 2001 |
| Interpersonal injustice | The degree to which people are not treated with politeness, dignity, and respect by decision makers. | State or event driven | Turel, Yuan, & Connelly, 2008 |
| Informational injustice | The perception that managerial explanations do not sufficiently convey the reasoning behind processes and outcomes. | State or event driven | Turel et al., 2008 |
| Negative affective absorption | The trait or predisposition to become deeply involved with one's negative emotions. | Trait | Developed for this study. |
| Negative affective flow | The state of immersion with one's emotions to the point that nothing else matters. | State or event driven | Developed for this study. |
| Attitude toward specific information security policy | Relatively enduring beliefs and predispositions (favorable or unfavorable) toward a specific information security policy. | Trait | Ajzen, 1991; Herath & Rao, 2009b; Scherer, 2005 |
| Information security policy compliance | An employee's actual behavior to protect the information and technology resources of an organization from potential security breaches. | State or event driven | Bulgurcu et al., 2010 Adapted to actual compliance |

Previous literature across multiple disciplines has repeatedly shown that attitudes influence intention and intention influences behavior. In the context of information security, attitudes have been shown to impact behavioral information security intention and behavior (Bulgurcu et al., 2010; Herath & Rao, 2009b; Johnston & Warkentin, 2010; Pahnila, Siponen, & Mahmood, 2007; Warkentin et al., 2011). Attitude toward information security policy is defined as the relatively enduring beliefs and predispositions (favorable or unfavorable) concerning information security policies (Ajzen, 1991; Herath & Rao, 2009b; Scherer, 2005).

Prior behavioral theories such as the theory of reasoned action and the theory of planned behavior (Ajzen, 1991; Fishbein & Ajzen, 1975) have shown that behavioral intention is influenced by attitude, normative beliefs, and perceived behavioral control. Existing literature in information systems has demonstrated the impact these variables have on behavioral information security intention variables such as information security policy compliance

intention (Bulgurcu et al., 2010; Herath & Rao, 2009b; Siponen, Pahnila, & Mahmood, 2007; Warkentin et al., 2011). However, in the context of information security, it is important to focus on people's actual behaviors, as the actual performance of the behavior determines whether or not an organization's resources are protected from the vulnerability of interest (Crossler et al., 2013). Further, when exploring phenomena related to information security, measuring actual behavior as the dependent variable provides better theoretical validation than collecting behavioral security intentions (Anderson & Agarwal, 2010; Crossler et al., 2013; Mahmood et al., 2010; Straub, 2009; Warkentin et al., 2012). Hence, in this study we examine information security policy compliance behavior in a simulated environment within a laboratory experiment:

**H1:** Attitude toward a specific information security policy is positively associated with information security policy compliance.

## 3.2 Negative Affective Flow

State affect is described as a person's current emotions that arise from cognitive appraisals of events or thoughts (Bagozzi et al., 1999). Personal and work-related experiences can both cause high-intensity emotions (Kim, Park, & Baskerville, 2012; Willison & Backhouse, 2006), which may lead to decisions that are contrary to self-interest (Willison & Warkentin, 2013) such as workplace deviance (Judge, Scott, & Ilies, 2006; K. Lee & Allen, 2002). In addition, these emotions form affective processes—necessary and important components of rational decision-making (Djamasbi et al., 2010)—and influence cognitive processes and behavior (Lerner & Keltner, 2000; Loewenstein, 1996). As the intensity of affect increases, so does its direct influence on behavior (Carmichael & Piquero, 2004; Ilies & Judge, 2002; Loewenstein, 1996). The concept of negative affective flow is derived from an integration of these theories in that the state of immersion (flow) with one's emotions (affect) leads to the point that nothing else matters. Essentially, an individual's state is consumed by emotions rather than by an object of attention. Determined by the level of emotions experienced, this affective state may result in employees leaving work (job turnover), organizational or interpersonal deviance, or other withdrawal behaviors (Ilies & Judge, 2002). Based on the above rationale and that which was described in the theoretical framework section, we postulate that:

**H2:** Negative affective flow is negatively related to information security policy compliance.

## 3.3 Negative Affective Absorption

Absorption describes an individual's readiness to experience deep involvement with an object of attention (Roche & McConkey, 1990) to the point that nothing else matters. It is a trait or disposition of one's persona. A trait is a relatively stable characteristic regardless of situational stimuli (Webster & Martocchio, 1992). In addition to absorption, trait affect impacts an individual's reflexes, perception, cognition, and behavior (Russell, 2003). Individuals with a trait or disposition toward negative affect are likely to have more intense bouts of emotion and react stronger when negative events occur (Weiss & Cropanzano, 1996). Both absorption and trait affect are shown to influence their state-like counterparts (Agarwal & Karahanna, 2000; Judge et al., 2006). Negative affective absorption integrates these two theories and is defined as the disposition to experience deep involvement (absorption) with negative emotions (trait affect). Intense levels of affect coupled with repeat occurrences of injustice may result in people becoming deeply involved in their emotions, thereby impacting attitudes, judgments, and behavior (Ilies & Judge, 2002). For example, in the onset of negative events, a person whose trait-like capacity to contain his or her emotions will largely determine his or her readiness to become deeply immersed in his or her state-like emotions. In other words, people who are known to have a "short-fuse," or a lower capacity to handle negative emotions, may experience stronger and deeper reactions to emotion-inducing events leaving them more prone to enter a state of negative affect flow than their counterparts. Therefore, just as absorption has been shown to be an antecedent to flow (Agarwal & Karahanna, 2000) and trait affect an antecedent of state affect, we posit that negative affective absorption is an antecedent to negative affective flow:

**H3:** Negative affective absorption is positively related to negative affective flow.

## 3.4 Perceived Organizational Injustice

Information systems security research related to organizational injustice is largely underexplored (Willison & Warkentin, 2013) despite its serious organizational consequences. For this reason, perceptions of organizational injustice are a primary focus in this research. Organizational injustice refers to the phenomena that influence employees' perceptions of fairness/unfairness (Willison & Warkentin, 2013). Three initial justice dimensions or constructs emerged from studies of organizational justice: distributive justice, procedural justice, and interactional justice. Further research has broken interactional justice into subsets of interpersonal justice and informational justice (Greenberg, 1993; Shapiro, Buttner, & Barry, 1994). Essentially, fairness perceptions originate from

an individual's personal perception of how outcomes are distributed (i.e., distributive injustice) (Cohen-Charash & Spector, 2001; Colquitt, Conlon, Wesson, Porter, & Ng, 2001; Lim, 2002), how procedures are executed (i.e., procedural injustice) (Cohen-Charash & Spector, 2001; Colquitt et al., 2001; Leventhal, 1980; Lim, 2002), the way people are treated by authorities or other third parties (i.e., interpersonal injustice) (Bies & Moag, 1986; Colquitt et al., 2001; Tyler & Bies, 1990), and the adequacy of information provided relating to outcomes and procedures (i.e., informational injustice) (Bies & Moag, 1986; Colquitt et al., 2001; Lim, 2002; Shapiro et al., 1994; Tyler & Bies, 1990). Because unfairness directly or indirectly affects people's emotions, cognitions, and behavior (Cohen-Charash & Spector, 2001), employees who perceive that they are being treated unfairly may (1) experience negative emotions such as disgruntlement (Willison, Warkentin, & Johnston, 2018) and anger (Dupré, Barling, Turner, & Stride, 2010), (2) ponder ways to retaliate against the organization (Bennett & Robinson, 2000), and (3) rationalize deviant behavior such as noncompliance or cybercrime (Li et al., 2010; Lim, 2002). Therefore, otherwise normally ethical employees may engage in deviant behaviors (Aquino, Lewis, & Bradfield, 1999). Depending on the level of injustice experienced or perceived, an individual may experience high-intensity emotions that influence cognitive processes and behavior (Judge et al., 2006; Kim et al., 2012; K. Lee & Allen, 2002; Lerner & Keltner, 2000; Loewenstein, 1996; Willison & Backhouse, 2006). Repeat instances of organizational injustice resulting in intense levels of negative affect may cause people to become deeply involved with their negative emotions (i.e., negative affective flow) to the point that nothing else matters other than quenching these emotions through actions which may result in harmful outcomes.

### 3.4.1 Perceived Distributive Injustice

Distributive injustice is defined as the unfairness of outcome distributions or allocations (Cohen-Charash & Spector, 2001; Colquitt et al., 2001; Lim, 2002). When inputs and outcomes are perceived to be out of balance, individuals will develop perceptions of distributive injustice (Adams, 1965). These perceptions affect attitude, satisfaction, commitment, and job turnover (Ambrose & Cropanzano, 2003; Sager, 1991). Additionally, Aquino et al. (1999, p. 1075) suggest that these injustice perceptions "evoke feelings of dissatisfaction and resentment that motivate aggrieved parties to react, either by modifying their behavior to restore equity or by seeking to change the system." Consistent perceptions of distributive injustice may cause individuals to have their negative emotions drive decision-making.

**H4A:** Perceived distributive injustice is positively related to negative affective flow.

### 3.4.2 Perceived Procedural Injustice

In addition to an individual's perception of outcome fairness, individuals will also form judgments regarding the decision process for how outcome allocation is determined and executed, known as procedural injustice. Procedural injustice is defined as the unfairness of procedures used to determine outcome distributions or allocations (Cohen-Charash & Spector, 2001; Colquitt et al., 2001; Leventhal, 1980; Lim, 2002). Because procedures are a representation of how an organization allocates resources, procedural injustice is expected to be related to cognitive, affective, and behavioral reactions toward the organization (Cohen-Charash & Spector, 2001). Reoccurring unfair processes experienced by an individual will result in one's negative emotions driving decision-making, which may lead to actions that put the organization at risk.

**H4B:** Perceived procedural injustice is positively related to negative affective flow.

### 3.4.3 Perceived Interactional (Interpersonal and Informational) Injustice

Interactional injustice is the quality of treatment and explanation one receives from organizational authorities when procedures are implemented (Bies & Moag, 1986; Tyler & Bies, 1990). Interactional injustice has two dimensions: (1) interpersonal injustice defined as the unfairness of treatment (e.g., politeness, dignity, and respect) one receives from authorities involved in executing procedures and determining outcomes (Colquitt et al., 2001) and (2) informational injustice defined as the inadequacy of explanations (e.g., unreasonable, untimely, and general) that convey information regarding why given procedures were used and how outcomes were distributed (Colquitt et al., 2001; Shapiro et al., 1994). When an individual perceives a situation as unfair, both interpersonal injustice and informational injustice become important determinants of cognitive, affective, and behavioral reactions to the source of injustice (Cohen-Charash & Spector, 2001; Greenberg, 1990). Individuals who continually feel that they have not been treated politely or with dignity or respect or who feel that they have been given incomplete or inaccurate information may become deeply entrenched in their negative emotions. Based on this rationale, we hypothesize the following:

**H4C:** Perceived interpersonal injustice is positively related to negative affective flow.

**H4D:** Perceived informational injustice is positively related to negative affective flow.

### 3.5 Frustration

Affective events theory informs us that frustrating tasks may cause negative affective reactions (Weiss & Cropanzano, 1996). Also, individuals who experience negative emotions are more likely to act out negatively in their work and interpersonal settings, resulting in a decrease in their job performance. This process can then continue in a cyclical manner such that the decrease in job performance leads to further negative emotions that likewise continue to decrease job performance. Further research demonstrates that these emotions direct and motivate behavior, especially at the time that the emotion is being experienced (Ilies & Judge, 2002). These emotions may result directly from work-related tasks or interactions with co-workers and could lead to negative consequences for both the individual and the organization. For example, the findings of negative emotions influencing job behavior are consistent with Agnew (1992) who found that negative emotions could lead to deviant behaviors, such as not complying with policies or misusing organizational systems. Aquino et al. (1999) also found that negative emotions would increase the likelihood that an individual would perform both interpersonal deviant behavior (e.g., refuse to talk to a co-worker) and organizational deviant behavior (e.g., purposefully ignored a supervisor's instruction).

One type of negative emotion that is experienced in the moment of trying to complete a task is frustration. Gaming research has shown that frustration "arises when the progress a user is making toward achieving a given goal is impeded" (Gilleade & Dix, 2004, p. 229). Factors such as workplace constraints and barriers can lead to frustration, and this frustration can lead to negative behaviors in the workplace (Spector, 1978), including policy violation (Fries et al., 2016; Haag & Eckhardt, 2014; Willison et al., 2018). If emotions are unmitigated, completing the task at hand will continue to be dissatisfying, thereby breeding further frustration (Judge et al., 2006). When trying to complete a work-related task, research suggests that experiencing a negative emotion, such as frustration, will lead to a negative influence on job behavior decisions (Ilies, De Pater, & Judge, 2007). When experiencing frustration, it is more likely that someone would act in violation of a company's information security policy. Therefore, we hypothesize that:

**H5:** Individuals who are more frustrated are less likely to comply with an ISP than those who are less frustrated.

## 4 Research Method

We tested our model by conducting a laboratory experiment with various simulated workplace-type tasks designed to cause some degree of frustration. Workplace tasks can produce frustration in and of themselves, but we also sought to enhance the levels of frustration in some cases. Tasks were designed to generate varying levels of frustration among subjects to better tease out the impact of frustration on compliance. Ultimately, we were able to rigorously measure the levels of frustration to test the impact of this affect in the context of our focal phenomenon. Instruments for this study were refined through expert panel reviews and exploratory data analysis from a pretest and two pilot tests as described below. After finalizing the instruments and the experimental design, the final study was then conducted.

### 4.1 Item Development

All scales were developed following the recommended guidelines of Churchill (1979) and Mackenzie et al. (2011) to ensure scale validity and reliability. The constructs evaluated in this study included organizational injustice, negative affective absorption, negative affective flow, and attitude toward specific information security policy. Information security policy compliance was a direct measure of behavior captured through an experiment and is measured with a binary measurement of compliance (1) or noncompliance (0). All other measurements were multi-item scales adapted from previous research or developed for this study. Attitudinal items were adapted from Herath and Rao's (2009b) security policy attitude scale and Bulgurcu et al.'s (2010) attitude scale. Organizational injustice items were adapted from Lim's (2002) distributive justice scale and Turel et al.'s (2008) procedural justice, informational justice, and interpersonal justice scales. Additionally, scales for negative affective absorption and negative affective flow were developed for this study and are reflective constructs. All constructs were composed of multi-item scales and were measured using fully anchored 5-point Likert agreement scales. The items with their associated item ID, original item, and source are listed in Appendix A.

### 4.2 Instrument Pretesting and Refinement

Before full data collection, a preliminary investigative procedure was conducted to improve instrument validity and reliability (Campbell & Fiske, 1959; Gefen, Straub, & Boudreau, 2000; Gefen & Straub, 2005; Mackenzie et al., 2011; Nunnally & Bernstein, 1994; Peter, 1981; Straub et al., 2004). Consistent with the steps of determining content and construct validity (Churchill, 1979; MacKenzie et al., 2011), the preliminary investigative procedure was used to refine scales through (1) feedback from expert panel reviews, (2) suggestions from pretests, (3) and initial data analysis conducted from a pilot study. During the expert panel reviews, seven information security faculty and doctoral students who publish and are

trained in information security research evaluated the experiment and instrument items for clarity and realism. Feedback from expert panel reviews was implemented prior to data collection. For example, experimental procedures were reworded for clarity and revised to collect actual compliance behavior rather than compliance intention.

To further refine the instrument, a sample of 21 faculty, staff, and students participated in a pretest of the study. The purpose of the pretest was to identify any necessary revisions to the instrument or instructions. Subjects evaluated the full experiment, ensured procedures and technologies were properly established, and identified any flaws or inconsistencies. For example, issues related to a video presentation used at the beginning of the study were corrected and items in the instrument were reworded for better clarification.

After remedying problems discovered in the pretest, the final experiment was readied for a pilot test. Two pilot tests were conducted to assess reliability and validity of the constructs used to measure the phenomena. A sample of 111 students completed the initial pilot test. Validity issues were found with the organizational injustice constructs; therefore, procedural injustice and informational injustice scales were reevaluated and reworded to partial out the differences between the two scales. A second pilot study with a sample of 24 more students was conducted and indicated reliability for the modified constructs.

## 4.3 Instrument Design and Procedure

Because emotional response is an integral part of this study, adequately collecting these responses is essential to explaining the research phenomenon. Bradley and Lang (1994) indicate three primary means of measuring emotional response: (1) through the observation of behavior, (2) through self-report, or (3) via physiological response. We incorporated two of these means in our research design; our subjects reported their levels of frustration using a validated multi-item scale and we also observed actual behavior in our laboratory experiment which served as a proxy for capturing *actual real-world behavior* related to individual emotional response in an organizational environment. To test the conceptual model and hypotheses of this study, we first received approval for our experiment from the institutional research ethics board. Next, we conducted our laboratory experiment in which subjects experienced simulated tasks with varying levels of fair conditions designed to increase frustration levels in some of the subjects, thereby enhancing the inherent frustration felt by many individuals when completing workplace tasks. We expected subjects who perceived the task to be unfair would experience relatively higher levels of frustration, whereas those who perceived the conditions to be fair would be less frustrated, *ceteris paribus*. Research has shown that people who are unable to complete a specific task may have cause to become frustrated because of the apparent lack of fairness (Gilleade & Dix, 2004). Such frustration may lead individuals to violate organizational rules to "cheat the system," though they may simply be viewing such violations as workplace workarounds (Alter, 2014). For example, research has indicated that cheating is not caused by the difficulty of the task—rather it is caused by perceptions of a lack of caring or of fairness (Stephens, 2005). People in these situations feel that they can justify cheating (Barlow et al., 2013; Siponen & Vance, 2010). Subjects in our study were randomly assigned to the simulated tasks to induce varying levels of frustration and perceptions of injustice. Randomization reduces the impact of any internal validity issues because any confounding variables are distributed across the tasks (Campbell & Stanley, 1963). Additionally, all instrument items were randomized to reduce order effects (Podsakoff, MacKenzie, J.-Y. Lee, & Podsakoff, 2003).

Subjects were students who were informed of the laboratory experiment through in-class invitations to earn extra credit for their participation. This population was an appropriate sampling frame because just as employees, undergraduate students must comply with university security policies, including those that address password protection, and also experience a range of affects.

Subjects were initially invited to visit an online survey that first presented an electronic informed consent form. Those who consented and elected to participate in the experiment then provided their name and ID, then selected the most convenient time to participate in the experiment. Additionally, we collected some of the individual-level data from each subject—the initial survey contained a preliminary assessment of each subject's self-reported perceptions of the latent variable negative affective absorption—to avoid having this item bias other items in the later survey in the laboratory. Finally, this survey was used to collect demographic information. See Figure B1 (in Appendix B) for a graphical depiction of the experimental procedures.

After the recruitment survey, subjects returned during their selected lab time slot. Upon entering the lab, similar to the study by Wright and Marett (2010), they were given a username and password and were told never to share their password no matter the circumstance using the following dialogue, "*In order to protect company information, organizations establish information security policies and procedures to inform employees of organizational expectations and consequences. Password guidelines are included as part of these policies which state that users should never share passwords with others. Similarly, you are*

*expected to keep your password secret.*" Then they viewed a video presentation detailing the laboratory exercise in which they were told they would make 20 decisions pertaining to a supply-and-demand scenario. After each decision, subjects received a reward based on their decision; they understood that they would receive greater rewards if they made better decisions about the allocations. Further, the subjects were told that their total reward points would determine how much extra credit they would receive for their participation in this study. However, depending on which simulated task they completed, the probability that some of the subjects would make an accurate decision was decreased. These conditions resulted in lower rewards, which contributed to the higher levels of frustration among many subjects, which led to perceptions of unfairness.

Although subjects were expecting 20 decision rounds, the task presented a situation after just 10 decisions in which the subjects were informed that they could share their password with a co-worker (violating information security policy) to potentially improve their score. *Actual compliance with information security policy* in the experiment, a proxy for actual compliance in an organizational setting, was then captured based on whether the subjects shared their password. The subjects were then directed to a survey in which we captured responses related to perceived organizational injustice, negative affective absorption, negative affective flow, and attitude toward specific information security policy. Next, subjects indicated the estimated time it took to complete the experiment and the level of frustration experienced. Finally, subjects viewed a debrief statement informing them that they would not complete the remaining 10 decisions and they would fairly receive full extra credit despite their performance, consistent with our experimental protocol's full consent provision, as approved by the appropriate research ethics board.

During the experiment and depending on the task, subjects were rewarded points based on the decisions they made. Their perceptions of unfairness regarding the tasks and point allocation contributed to their feelings of frustration. The responses from all respondents were split using a median split based on the frustration level experienced similar to the method used by Tsai and Bagozzi (2014), Bhattacherjee (2001), and Harrington (1996). Rucker et al. (2015) recommend three approaches for representing the median split: (1) scatterplot with regression lines, (2) a median split plot, (3) a simple slopes plot, and (4) a dot-plot. In this research, we examined the median split using the median split plot. Other median split plots are more informative, but this method allows the reader to quickly assess how the Y varies depending on the X (see Figure 2). In other words, the figure allows us to quickly see the level of frustration experienced by our subjects. The median split was used to determine the impact of frustration level on information security policy compliance. Differences were then compared using structural equation modeling in AMOS 22.

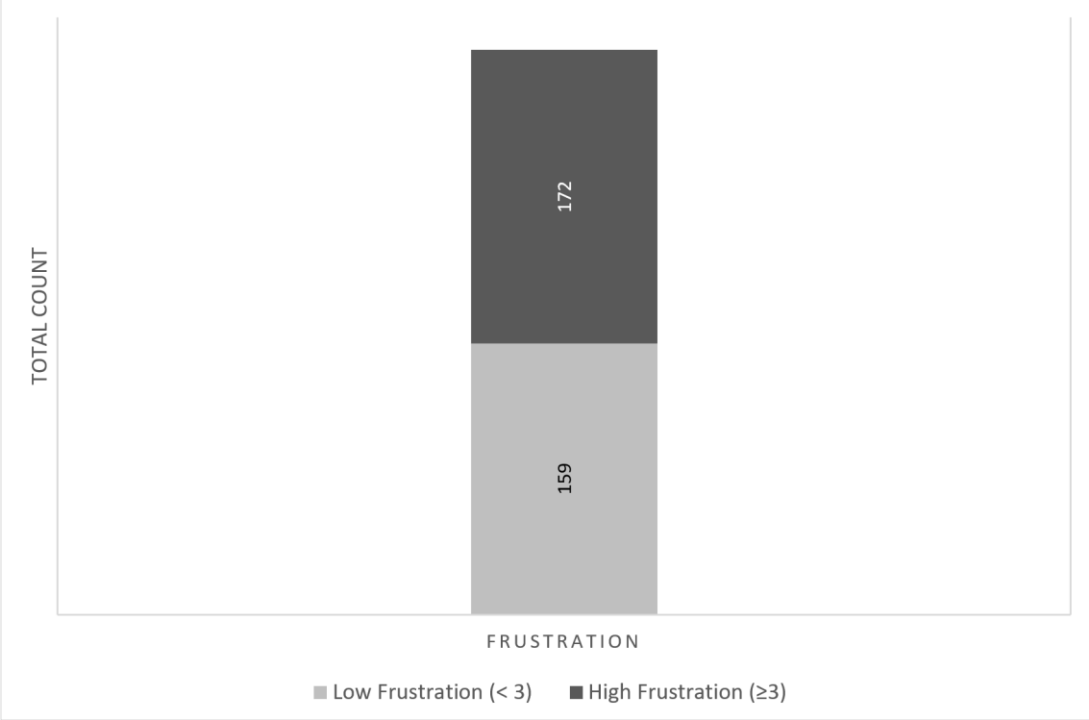


**Figure 2. Frustration Experienced by Subjects Engaged in Simulated Tasks**

Our laboratory setting was comparable to an organizational setting in that employees are often provided with passwords to access and interact with information on a company's network such as a corporate database. These employees are told to never reveal these passwords. However, they often do not consider the problems that might arise from breaking this rule (Zorz, 2013). In fact, research has shown that only 22% of employees indicated that they had never shared their password (Aytes & Connolly, 2004). As for the other 78%, the reasons for sharing passwords are varied and may include situations where employees perceive injustice. In so doing, they may decide to share their password to receive help from the co-worker and counter the perceived injustice.

# 5 Data Analyses and Results

In order to test the relationships among constructs, we conducted data analysis using structural equation modeling in AMOS 22 using the two-step approach identified by Anderson and Gerbing (1988): (1) exploratory factor analysis and (2) confirmatory factor analysis. Using this statistical package, we assessed the measurement model to examine reliability and convergent and discriminant validity. In addition, we determined predictive validity through the assessment of the structural model. A total of 398 students participated in the experiment, but 67 responses were dropped due to incompleteness or *response set*—the tendency of subjects to respond automatically and independent of item content (Andrich, 1978; Kerlinger, 1973; Rennie, 1982). This left a final usable sample size of 331. See Appendix C for sample characteristics. We conducted independent-sample *t*-tests and determined there was no difference in information security policy compliance or frustration experienced between early subjects versus late subjects.

## 5.1 Instrument Validity

Exploratory factor analysis indicated several issues with both convergent validity and discriminant validity. Given the reflective nature of the constructs in this study, measures can be removed to improve construct validity without affecting content validity (Petter, Straub, & Rai, 2007). Therefore, the following items were removed to establish construct validity: two items from the negative affective absorption scale, one item from the negative affective flow scale, and one item from the informational injustice scale. Additionally, we removed procedural injustice from the model due to significant cross-loadings with interpersonal and informational injustice and then reassessed reliability and convergent and discriminant validity (see Appendix D).

Confirmatory factor analysis was used to assess both the measurement model to determine reliability and convergent and discriminant validity and the structural model to determine predictive validity. The data of the measurement model indicated that the model has good fit (see Appendix E), that configural and metric invariance are established (see Appendix F), and that common method variance is not a problem (see Appendix G). Additionally, initial reliability scores were obtained through a reliability analysis by computing composite reliability (see Table H-1 in Appendix H). All constructs had an acceptable level of reliability (≥ 0.70) (MacKenzie et al., 2011; Peter, 1979). The results indicate convergent validity because all items loaded significantly on their higher order construct with loadings greater than 0.70 (Straub et al., 2004) (see Table H1) and had an average variance extracted greater than 0.50 (Gefen & Straub, 2005) (see Table H2). The results also indicate discriminant validity because the square root of average variance extracted was greater than interconstruct correlations (Gefen et al., 2000) (see Table H2).

An assessment of the structural model was used to evaluate model fit and establish predictive validity by determining the magnitude and direction of the relationships. The data of the structural model indicated that the model exhibited good fit (see Appendix E). We used a multistage approach to analyze our research model similar to that used by Siponen and Vance (2010) and Johnston, Warkentin, and Siponen (2015). We conducted analyses on three different path models, starting with a simple model that tests the relationship between attitude and information security compliance behavior. Subsequent models then included negative affective absorption and flow, followed by the inclusion of organizational injustice. This approach was taken in order to establish the foundational relationships derived from prior research and then demonstrate the increase in explained variance ($R^2$) as additional constructs were added to the model as part of this research. The first path model evaluates attitude and its impact on compliance, indicating that attitude explains 25.6% of the variance of information security policy compliance for individuals who experienced more frustration, but only 6.8% for individuals who experienced less frustration. Consistent with prior literature, the standardized path estimates (see Figure 3) were found to be statistically significant, indicating that attitude had an impact on information security policy compliance for both groups.

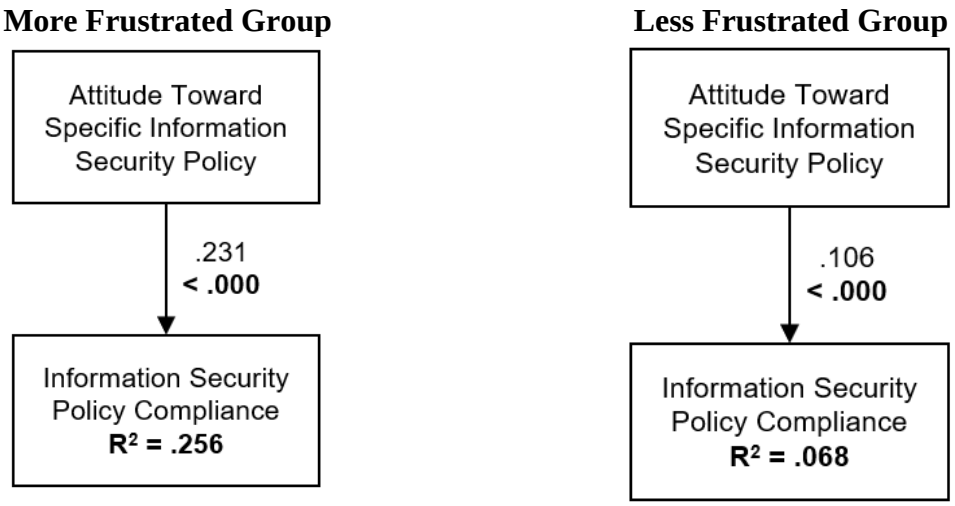


**Figure 3. Attitudinal Model with Significant Path Coefficients**

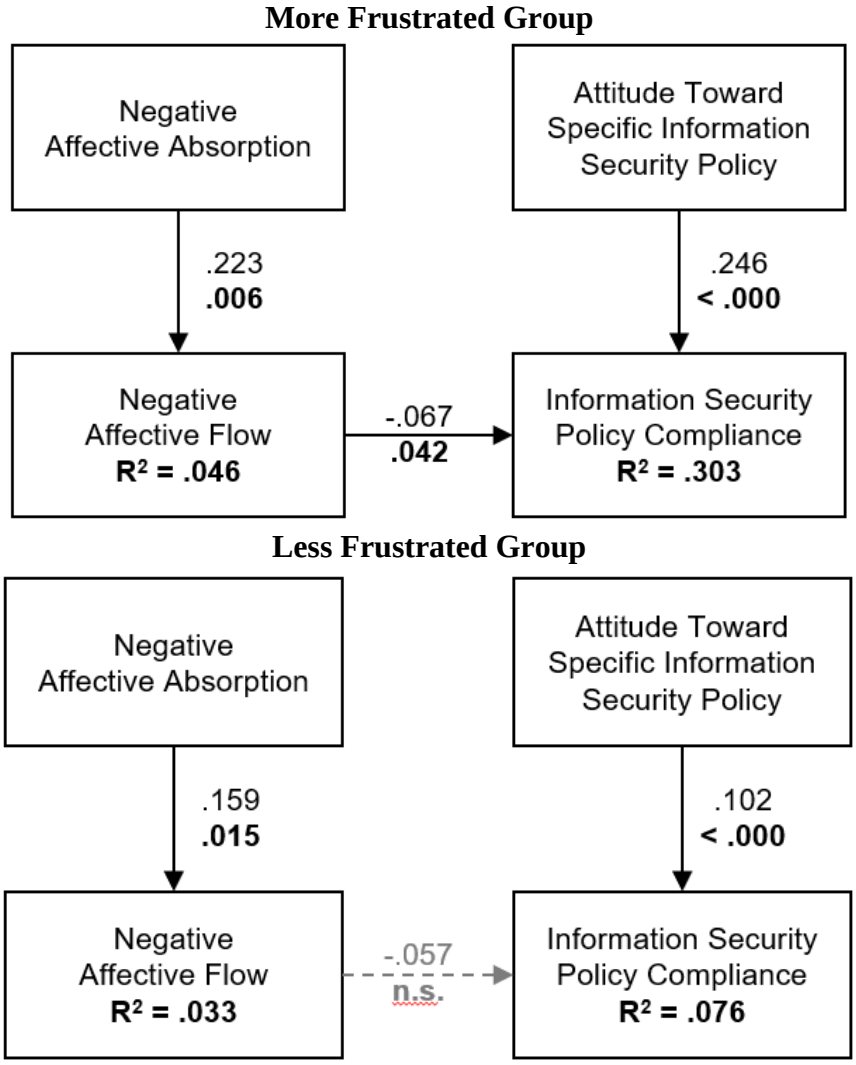


**Figure 4. Affective Model with Significant Path Coefficients**

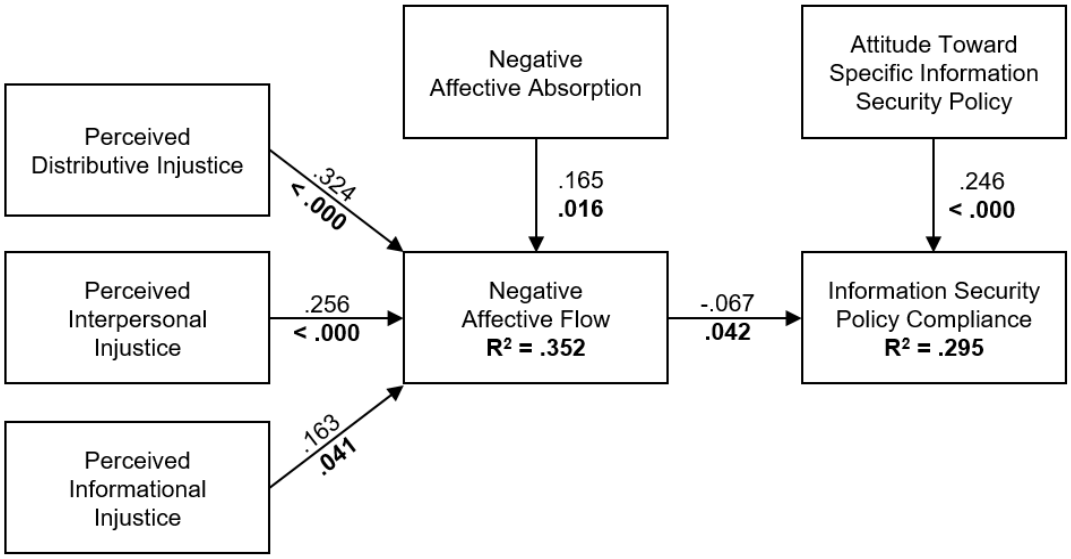


**Figure 5. Model with Significant Path Coefficients (More Frustrated Group)**

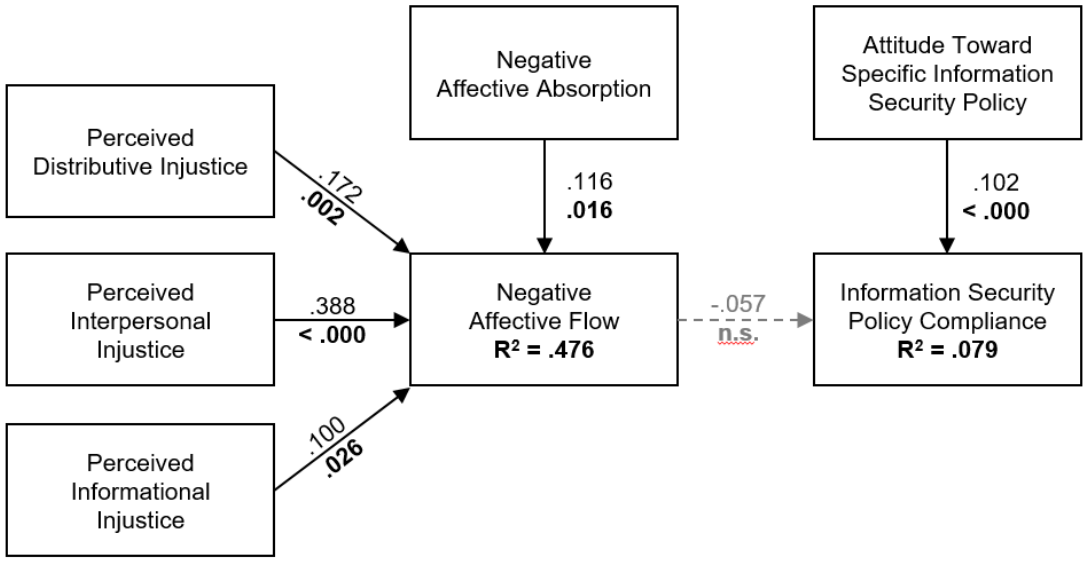


**Figure 6. Model with Significant Path Coefficients (Less Frustrated Group)**

The second path model, the main contribution of this study, evaluates attitude together with the affective constructs prescribed earlier and their combined impact on information security policy compliance. All standardized path estimates were statistically significant (see Figure 4) for the more frustrated individuals, indicating that individuals entered into a state of negative affective flow as they experienced repeated frustration, which impacted their compliance with information security policy. The inclusion of negative affective flow and negative affective absorption in the variance model increased the explained variance from 25.6% to 30.3% for individuals who experienced more frustration; whereas, for individuals who experienced less frustration, the affect constructs had no influence on information security policy compliance. Additionally, individuals with the dispositional tendency to become immersed in their negative emotions (i.e., negative affective absorption) experienced higher levels of negative affective flow.

Using the third and full path model, we obtained the standardized path estimates for all constructs (see Table 2). For individuals who experienced more frustration, six out of six paths were statistically significant (see Figure 5). For individuals who experienced less frustration, five out of six paths in model were found to be statistically significant (see Figure 6). See squared multiple correlations in Table 2 for the variance explained. Figures 5 and 6 display the conceptual model with the parameter estimates, *p*-values, and variance explained for both frustration levels.

**Table 2. Path Estimates, t-values, and Squared Multiple Correlations***

| | More Frustrated Group | | | Less Frustrated Group | | |
|---|---|---|---|---|---|---|
| **Hypothesized Relationship** | **Std. Estimate** | **T-Value** | ***p*-value** | **Std. Estimate** | **T-Value** | ***p*-value** |
| H1: ↑SATT → ↑COMP | .246 | 7.869 | *** | .102 | 3.445 | *** |
| H2: ↑NAF → ↓COMP | -.067 | -2.029 | .042 | -.057 | -1.474 | n.s. |
| H3: ↑NAA → ↑NAF | .165 | 2.418 | .016 | .116 | 2.411 | .016 |
| H4A: ↑DINJ → ↑NAF | .324 | 3.625 | *** | .172 | 3.070 | .002 |
| H4B: ↑IINJ → ↑NAF | .256 | 3.348 | *** | .388 | 6.579 | *** |
| H4C: ↑FINJ → ↑NAF | .163 | 2.046 | .041 | .100 | 2.230 | .026 |
| **Squared Multiple Correlations** | | | | | | |
| NAF | 0.352 | | | 0.476 | | |
| COMP | 0.295 | | | 0.079 | | |

**Note:** *** $p < 0.001$; DINJ = perceived distributive injustice; IINJ = perceived interpersonal injustice; FINJ = perceived informational injustice; NAA = negative affective absorption; NAF = negative affective flow; SATT = attitude toward specific information security policy; COMP = information security policy compliance

*Due to the dependent variable of information security policy compliance (COMP) being binary, we tested the robustness of our findings by running a binary logistic regression with negative affective flow (NAF) and attitude toward specific information security policy (SATT) as independent variables. This analysis was run twice, depending on whether individuals were frustrated. The results confirm the findings from AMOS. For the more frustrated group H1 supported: SATT→COMP (*p*-value < 0.000; *B*= 1.314) & H2 supported NAF→COMP (*p*-value = 0.034; *B*= -0.423). For the less frustrated group, H1 supported SATT→ COMP (*p*-value = 0.001; *B*= 0.702) & H2 not supported NAF→COMP (p-value = 0.103; *B* = -0.503).

## 5.2 Mean Comparison

To test our fifth hypothesis and provide compelling evidence that the subjects' emotions were manipulated during the experiment, we conducted two mean comparison tests. The data for both tests were divided using a median split that resulted in a total sample size of 155 for the more frustrated group and 176 for the less frustrated group. Although there was an inherent underlying perceived frustration from task completion, software interface, time pressures, and other factors, the analysis indicates that we achieved the desired results of having a sample that included both highly frustrated and relatively low frustrated subjects. Additionally, a *t*-test was then conducted to determine whether there was a statistical difference in negative affective flow and compliance based on frustration experienced.

The first *t*-test determined the impact of a subjects' frustration on negative affective flow. Given that negative affective flow is a multi-item scale, an average score for the scale was used in the mean comparison test. Table 3 shows the descriptive statistics, indicating a mean of 3.22 out of 5.00 for subjects who experienced higher levels of frustration and 1.81 out of 5.00 for subjects who experienced lower levels of frustration. Table 3 also shows that the differences in frustration experienced is statistically significant indicating that individuals who perceived tasks to be frustrating experienced higher levels of negative affective flow.

The second *t*-test determined the impact of a subject's frustration on compliance. Table 4 shows the descriptive statistics, indicating that 68% of all subjects who experienced higher levels of frustration complied with information security policy; whereas, 85% of all subjects who experienced lower levels of frustration complied with information security policy. Table 4 also shows that the differences in frustration experienced is statistically significant, indicating that individuals who perceived tasks to be frustrating were less likely to comply with information security policy. This supports the fifth hypothesis that individuals who are more frustrated are less likely to comply with information security policies than those who are less frustrated. This is also supported in that the relationships in the model are strengthened and the variance in information security policy compliance is increased as seen in Figures 4, 5, and 6.

## 5.3 Analyses Summary

After accounting for control variables (see Appendix I), the results indicated support for all six hypotheses in the more frustrated group and four hypotheses in the less frustrated group (see Table 5). Additionally, the results indicated support for H5 which posited that more frustrated individuals are less likely to comply with information security policy than less frustrated individuals (see Table 5). It is worth noting that, among those who were less frustrated, though attitude

contributed to security policy compliance, negative affective flow had no significant impact on compliance.

**Table 3. Descriptive Statistics and Independent Samples Test for Negative Affective Flow Based on Frustration**

| Group | *N* | Mean | Std. Deviation | Std. Error Mean | |
|---|---|---|---|---|---|
| More Frustrated (≥ 3) | 155 | 3.22 | 0.975 | .078 | |
| Less Frustrated (< 3) | 176 | 1.81 | 0.683 | .052 | |
| | | | | | |
| **Equal variances assumed** | ***F*** | **Sig.** | ***t*** | ***df*** | **Sig.** |
| Yes | 21.532 | 0.000 | 15.416 | 329 | 0.000 |
| No | | | 15.084 | 271.27 | 0.000 |

**Table 4. Descriptive Statistics and Independent Samples Test for Compliance Based on Frustration***

| Group | *N* | Mean | Std. Deviation | Std. Error Mean | |
|---|---|---|---|---|---|
| More Frustrated (≥ 3) | 155 | 0.68 | 0.466 | .037 | |
| Less Frustrated (< 3) | 176 | 0.85 | 0.361 | .027 | |
| | | | | | |
| **Equal variances assumed** | ***F*** | **Sig.** | ***t*** | ***df*** | **Sig.** |
| Yes | 52.085 | 0.000 | -3.569 | 329 | 0.000 |
| No | | | -3.513 | 288.83 | 0.001 |

*A binary logistic regression was run to obtain a Wald test as a robustness check of the independent sample *t*-test results. The Wald test was significant at 0.000 when utilizing the median split of more frustrated (≥ 3) and less frustrated (< 3). The Wald test was significant at 0.001 when utilizing the raw frustration scores for individuals. These results confirm H5 that individuals who are more frustrated are less likely to comply with information security policies than those who are less frustrated.

**Table 5. Hypotheses and Support**

| HO | Structural Relationship | Supported |
|---|---|---|
| **The More Frustrated Group** | | |
| H1 | Attitude toward specific ISP is positively related to ISP compliance. | Yes |
| H2 | Negative affective flow is negatively related to compliance with ISP. | Yes |
| H3 | Negative affective absorption is positively related to negative affective flow. | Yes |
| H4A | Perceived distributive injustice is positively related to negative affective flow. | Yes |
| H4B | Perceived interpersonal injustice is positively related to negative affective flow. | Yes |
| H4C | Perceived informational injustice is positively related to negative affective flow. | Yes |
| **The Less Frustrated Group** | | |
| H1 | Attitude toward specific ISP is positively related to ISP compliance. | Yes |
| H2 | Negative affective flow is negatively related to compliance with ISP. | No |
| H3 | Negative affective absorption is positively related to negative affective flow. | Yes |
| H4A | Perceived distributive injustice is positively related to negative affective flow. | Yes |
| H4B | Perceived interpersonal injustice is positively related to negative affective flow. | No |
| H4C | Perceived informational injustice is positively related to negative affective flow. | Yes |
| **Frustration** | | |
| H5 | Individuals who are more frustrated are less likely to comply with ISP than those who are less frustrated. | Yes |
| *Note:* ISP = information security policy | | |

### 5.4 Mediation Effect

Mediation occurs when an independent variable is able to influence the dependent variable of interest through a third variable (Baron & Kenny, 1986). Using the bootstrapping method in AMOS, our model indicates indirect mediation effects from negative affective absorption and interpersonal injustice to information security policy compliance via negative affective flow for those who experienced more frustration. However, no indirect mediation effects were specified for individuals who experienced less frustration (see Table 6).

**Table 6. Descriptive Statistics and Independent Samples Test for Compliance Based on Frustration***

| Group | DINJ | IINJ | FINJ | NAA |
|---|---|---|---|---|
| More Frustrated | 0.051 | 0.031 | 0.054 | 0.044 |
| Less Frustrated | 0.080 | 0.111 | 0.087 | 0.080 |

*Notes:* DINJ = perceived distributive injustice; IINJ = perceived interpersonal injustice; FINJ = perceived informational injustice; NAA = negative affective absorption

*A binary logistic regression was run to obtain a Wald test as a robustness check of the independent sample *t*-test results. The Wald test was significant at 0.000 when utilizing the median split of more frustrated (≥ 3) and less frustrated (< 3). The Wald test was significant at 0.001 when utilizing the raw frustration scores for individuals. These results confirm H5 that individuals who are more frustrated are less likely to comply with information security policies than those who are less frustrated.

## 6 Discussions, Implications, and Future Research

By evaluating a sample of affective processes and cognitive processes in information security decision-making, we increase our understanding pertaining to compliance with organizational security policies. Our results contribute to theory by expanding the understanding of affective events theory and the influence that both cognitive and affective states have on security policy compliance. In doing so, we introduced two new constructs, affective absorption (i.e., the trait or disposition to allow one's emotions to drive decision-making) and affective flow (i.e., a state of immersion with one's emotions), which can be leveraged to explore other behaviors and their influence on other cognitive processes.

Our research also contributes to practice by revealing how unfair treatment of employees, experienced as a result of engaging in frustrating tasks, can influence affective reactions. By proactively treating employees fairly and rewarding them emotionally, organizations may be able to prevent noncompliant behaviors. In addition, when employees experience negative affect due to perceptions of organizational injustice or in response to other work-related events, we identify how organizations might address sensitive issues prior to the development of a state of negative affective flow.

### 6.1 Theoretical Contributions

Our study provides a more nuanced understanding of the phenomenon of information security policy violation by clarifying the perceptions and behavior of individual users in the domain of security decisions that are subject to the impact of affect. Salovaara and Merikivi (2015) urge scholars to extend the findings of previous research to increase knowledge associated with existing theories, thereby strengthening and improving theoretical knowledge (Whetten, Felin, & King, 2009). In this study, we incorporated and analyzed affect (i.e., negative affective flow) to expand on the knowledge surrounding deviant behavior in the context of information security policy violations. We further heeded the call of Straub (2009), Warkentin et al. (2012), and Crossler et al. (2013) by collecting actual violation behavior, rather than simply intention, thereby grounding our contributions in a richer, more meaningful empirical base.

Building upon affective events theory, we introduce two new constructs to the study of security policy compliance behavior—affective absorption and affective flow—and analyze their impact on compliance behavior. Negative affective absorption is the disposition to allow negative emotions to drive decision-making. Weiss and Cropanzano (1996) showed that individuals with dispositions toward negative affect are likely to have more intense bouts of emotion and to react more strongly when negative events occur. The results of our study extend this idea and indicate that negative affective absorption leads to negative affective flow. Our study demonstrates the need to distinguish between trait- and state-like emotions when evaluating information systems and information security research.

Another contribution of our study is that individuals who perceive that they have experienced organizational injustice through, for example, being repeatedly asked to perform frustrating tasks, are more

likely to experience negative affective flow. Additionally, the results provide evidence that the state of negative affective flow negatively influences information security policy compliance behavior for those who experienced more frustration. However, though people who have lower levels of frustration do enter into a state of negative affective flow, our findings do not reveal any impact on compliance. Future research should investigate underlying reasons for this phenomenon. Our study sheds further light on what influences information security policy compliance behavior by showing the effect affective emotions have on security compliance behavior. This provides a greater understanding regarding the depth of these emotions and their influence on information security policy compliance behavior. Therefore, organizations should focus on minimizing frustration as a result of work-related tasks. Previous research has indicated that even something as small as interface design for entering passwords has influenced people's security compliance behavior (Steinbart, Keith, & Babb, 2016). Seemingly insignificant tasks may increase employee frustration, potentially resulting in retaliation against an organization (Bennett & Robinson, 2000) or rationalization of deviant behavior (Li et al., 2010; Lim, 2002).

The results of our study indicate that regardless of individuals' frustration level their attitude toward information security policy compliance positively influences their compliance behavior. This reinforces the importance of managerial efforts to influence attitude including SETA programs (D'Arcy et al., 2009) and communications such as nudges and reminders (Barlow et al., 2018).

Our study captured both a sample of cognitive and affective processes in a unified model to better explain information security policy compliance behavior. Although the results indicate that the cognitive aspects of the model have a greater influence on information security compliance behaviors than affect, affect still significantly impacted these behaviors. Given the impact of negative affective flow, understanding the role of affect and its influence of deterrence is critical (Willison & Warkentin, 2013). Therefore, we have integrated both cognitive (i.e., organizational injustice) and affective (i.e., negative affective absorption and negative affective flow) aspects into one framework in the attempt to achieve a more holistic understanding of compliance behavior that future research can advance.

Another interesting finding pertains to control variables, specifically gender and estimated student grade. Gender only impacted the results in the less frustrated group. This seems to indicate that when people are frustrated, regardless of gender, they are likely to experience higher levels of negative affective flow which, in turn, impacts their information security policy compliance. Additionally, a student's estimated grade significantly influenced information security policy compliance in the less frustrated group. The fact that students' beliefs about their estimated grades were much lower than their actual grade highlights how important perceptions relate to actual behavior. In our study, many subjects chose to violate information security policy in order to earn extra course credit. Equally important, perceptions of poor performance may lead individuals to act contrary to work policies. Further investigation into the role of gender and performance could offer a greater understanding of information security behaviors when examining cognition and affect together.

Furthermore, we contribute to information systems research by capturing actual compliance with information security policy. Given measurement issues associated with collecting only behavioral intention in the context of information security (Crossler et al., 2013), our study achieves richer and more meaningful findings regarding information security behaviors by collecting and analyzing actual compliance behavior. As such, this study demonstrates one method to capture actual compliance as a dependent variable.

## 6.2 Practical Implications

Security education, training, and awareness (SETA) programs have proven effective in motivating individuals to comply with information security policies (Crossler & Bélanger, 2009; D'Arcy et al., 2009; Puhakainen, 2006; Siponen, 2000, 2005; Siponen et al., 2007; Thomson & von Solms, 1998); however, violations are still a grave concern for information security management (Bulgurcu et al., 2010; Hu et al., 2011). Most of these training programs focus on cognitive responses (reasoned actions) to situations (e.g., neutralization, Barlow et al., 2013), which may not be the most effective approach. Our research identifies the need to include training regarding affective responses in addition to cognitive responses. Training that emphasizes issues relating to both cognitive and affective processes may provide individuals with a more in-depth understanding of company expectations. During these training sessions, managers could explain that employees may experience negative emotions due to their interaction with fellow employees, managers, or existing or new policies and procedures. Further, managers could explain that it is not necessary or acceptable to bottle up negative emotions; rather, they could describe appropriate outlets to address such emotions. Outlets may include sessions focused on emotional support, discussions with managers, or anonymous suggestion boxes. Such outlets would facilitate idea generation regarding how to effectively reduce further frustration and grant employees the ability to proactively do something to counter the negative emotions they experience. Additionally, training of management

should focus on work-related factors that might frustrate employees and describe how to address issues with disgruntled employees before they engage in noncompliant behaviors.

More importantly, employers could focus on training oriented toward helping employees develop positive coping responses to feelings of frustration. Similar to the coping response to "security-related stress" discussed in D'Arcy, et al. (2014), responses to workplace stress and frustration could potentially be fostered, developed, and maintained through a targeted campaign of behavioral training programs that could provide affective relief to employers facing such situations. An even better strategy would be to identify, then mitigate or remediate the actual situational factors that instigate the frustration themselves.

Information technology governance and monitoring play critical roles in influencing compliance behaviors (D'Arcy et al., 2009; Herath & Rao, 2009a; Hovav & D'Arcy, 2012; Stanton, Stam, Mastrangelo, & Jolton, 2005; Warkentin & Johnston, 2006, 2008). Our findings highlight the importance of controlling and/or monitoring employee levels of affect, which is a critical element of the protection of organizational information and assets. In fact, if frustration is monitored, it can be used to indicate when a user is in need of assistance (Gilleade & Dix, 2004) before the frustration escalates into a larger problem. Periodically, organizations (or third-party consultants) could distribute anonymous surveys to employees to determine their propensity to experience negative affective flow. Individual employees could be evaluated for negative affect using various direct and indirect measures. For example, the PANAS survey could be used directly to measure affect (Watson, Clark, & Tellegen, 1988), other surveys that have been shown to correlate with the frustration affect could also be used (Inventado, Legaspi, Suarez, & Numao, 2011), and technology that visually identifies emotions based on facial cues may also be helpful in this regard (Cowie et al., 2001). Organizations could then use the resulting survey data to identify and address any issues prior to the appearance of deviant workplace behavior.

Ethical organizational managers would never intentionally frustrate employees. However, as the experiment in this study indicates, employees may experience frustration resulting from workplace processes, including workplace technology use, rather than from the direct actions of the organization or its managers. Given the range of workplace technologies, employees' inability to effectively understand or use the systems they must interact with each day may lead to frustration. Therefore, to better mitigate employee frustration, organizations must carefully use proper care when selecting which systems and applications to use or when designing in-house systems and applications.

Finally, our research highlights the need to quickly respond to any noticeable issues related to perceptions of unfairness. By addressing these issues quickly, negative affect can be controlled before negative affective flow is experienced. In order to assess such issues, organizations should focus on training managers to address sensitive issues with individual employees in a respectful and courteous manner so that employees understand the repercussions of uncontrolled emotions in the workplace. By controlling negative affective flow, organizations can facilitate a healthier and more secure workplace.

## 6.3 Limitations and Future Research

This study underscores the need for understanding affective processes with regard to information systems compliance behavior. In order to maintain model parsimony, we limited the number of factors we explored in order to better understand compliance with information security policy. Achieving a balance between completeness and parsimony introduces theoretical limitations that future research could address. For example, examining other constructs such as affective quality, emotion regulation, neutralization, risk tolerance, and time orientation together with affective absorption and affective flow may provide a deeper understanding regarding individual behaviors.

Affective quality, the ability to change core affect (Russell, 2003), may diminish an individual's negative affective absorption which would lead to reduced negative affective flow. Like affective quality, research on emotion regulation, specifically concerning the cognitive reappraisal side, would offer more understanding. Cognitive reappraisal "is an antecedent-focused emotion regulation strategy that alters the trajectory of emotional responses by reformulating the meaning of the situation" (Heilman et al., 2010, p. 258). Neutralization theory examines behavioral rationalizations through various justification techniques to reduce an individual's view of the consequences (Sykes & Matza, 1957). Examining neutralization together with the affective constructs of this study could provide a deeper understanding regarding the impact of cognition versus affect on information security policy compliance behavior. Risk tolerance refers to the maximum amount of uncertainty that one is willing to accept (Liang & Xue, 2009) and by assessing risk tolerance together with affective flow, researchers may achieve a greater understanding regarding information security policy compliance behavior. Time orientation looks at the manner in which individuals and cultures partition human experiences into temporal categories of past, present, and future, which fluctuate based on learned

preferences (Zimbardo, Keough, & Boyd, 1997). Evaluating time orientation differences among individuals may offer greater insights with respect to affective flow. For example, future time-oriented individuals may be less likely to become immersed in present negative emotions.

Another limitation of this study is that only the negative aspect of affective absorption and affective flow was investigated. Positive affective absorption and positive affective flow could also be examined in this and other research contexts. For example, Gottman (1994) found successful marriages maintain a 5:1 ratio of positive-to-negative interactions; whereas, marriages that end in divorce have closer to a 1:1 ratio of positive-to-negative interactions. Additionally, bad events have a stronger impact than good events and take longer to wear off (Baumeister, Bratslavsky, Finkenauer, & Vohs, 2001). These statistics might potentially be adapted to a business context; accordingly, increasing the number of positive experiences or replacing negative experiences with positive experiences could result in a successful relationship between organizations and their employees. This focus might result in a net positive experience; in other words, positive interactions would offset any negative interactions that individuals experience in the organization or with a specific technology (Etherington, 2013). Future research is needed to explore the impact of these experiences on both positive and negative affective flow, which may provide increased understanding regarding attitude toward information security policy and information security policy compliance behavior.

Additionally, researchers might apply affective absorption and affective flow to additional phenomena such as information systems use to determine their impact in other contexts. Although affective absorption was applied in a security context, future research could be applied throughout many aspects of information systems research. For example, affective absorption and affective flow might be included in the taxonomy of affective concepts as identified by Zhang (2013). Affective absorption may be indicative of other constructs such as satisfaction, usefulness, and ease of use in addition to beliefs, attitudes, and behaviors. Through future studies on affective absorption and affective flow, we may gain greater insight regarding additional factors that lead individuals to become completely immersed in their emotions which ultimately affects information security policy compliance behavior.

According to affective events theory, time and satisfaction are critical parameters when evaluating affective reactions (Weiss & Cropanzano, 1996). This research study attempted to evaluate affect using a series of simulations over a short period of time; however, a longitudinal study may grant additional understanding of the factors that increase/decrease negative affective flow and its impact on organizations. With respect to satisfaction, we excluded it from the model to ensure a parsimonious model. Additionally, capturing information security policy compliance rather than satisfaction as the ultimate dependent variable was more applicable due to the nature of this study.

Another area in need of future research is the tendency of certain individuals to respond to frustrating challenges like those our manipulation posed by "digging in" even further to solve the problem. This may be a learned response for some individuals and may be a disposition for others. Additional measures are probably necessary to identify this individual difference, or perhaps a pretest could be used to identify a new sample comprised entirely of such individuals, and this small, but important subpopulation (and others) could be further analyzed to determine the impacts of organizational injustice and frustration on employees who may be statistical outliers in their responses to the factors we have explored.

The relationship between affect and cognition should also be explored by behavioral psychologists, as well as security researchers advancing this area of knowledge. Is all attention devoted to affect and cognition such that it is a zero-sum game or do individuals have a separate independent capacity for each at a given time?

This research utilized an experimental design that incentivized individuals to complete a task in order to receive extra course credit. Therefore, the laboratory experiment may have motivated individuals to react to a given task so they could excel regardless of any existing information security policy. However, the fact that frustration led to increased password sharing (H5) suggests that this was not a limitation of our research design. However, it should be noted that our experimental manipulations were likely limited in their ability to generate frustration when compared to the higher levels of frustration that would occur in a real-world workplace setting. It would be reasonable to expect a greater effect when employees perceive frustration and injustice, such that the negative affective flow would be more extreme and more persistent and would lead to more consequences. As researchers continue to investigate and further the field's understanding of determinants underlying security behaviors, future studies could then design specific interventions and test them in laboratory and field settings.

Although past research has disputed the use of the unmeasured latent method construct (ULMC) based on its viability to adequately address common method variance (Chin, Thatcher, & Wright, 2012), it has not

provided a strong argument for alternative forms of assessing common method variance. Therefore, we employed the ULMC method along with the recommended a priori procedures to ameliorate potential common method variance as discussed in Appendix G.

Future research might also explore the roles of both positive affect (in general) and positive affective flow (specifically) in the context of information security behaviors, such as extra-role behaviors (J.S.-C. Hsu, Shih, Hung, & Lowry, 2015; Warkentin, Shropshire, & Straub, 2018) that go beyond simple policy compliance. Self-reported attitudes, perceptions, and beliefs are subject to bias; therefore, additional research could explore alternative methods to capture actual levels of affect, such as neurophysiological measurements (Crossler et al., 2013; Dimoka et al., 2012). Future studies could use galvanic skin response to measure skin conductance caused by sweat, electroencephalography (EEG) devices to record brain activity such as the Warkentin et al. (2016) fMRI study, or thermal cameras to determine blood rush.

# 7 Conclusion

Information security policy violations are a grave concern for information security management (Bulgurcu et al., 2010; Hu et al., 2011). Research has focused on identifying why individuals do not comply with information security policy; however, the majority of this research falls short in two ways: (1) the main focus of these studies is on information security policy compliance intention instead of actual information security policy compliance, and (2) prior literature has predominantly examined the impact of cognitive processes, rather than affective processes, on information security policy compliance behavior. Through understanding both affective processes and cognitive processes in decision-making, we better understand why individuals engage in deviant behavior.

Derived from information security and social psychology, our study examined the impact of unfairness (i.e., organizational injustice) and immersion with one's emotions (i.e., affective flow) on attitudes toward and compliance with information security policies. The results indicate that individual perceptions of unfairness can lead people to become completely involved with their negative emotions. Further, people who are immersed in their negative emotions are less likely to comply with information security policy.

These findings contribute to information systems security literature by introducing two new constructs, affective absorption and affective flow, which inform our understanding regarding information security policy compliance. In addition, our study demonstrates the need to capture actual behavior rather than only attitude and intentions. The findings convey the importance of discussing emotions in security, education, training, and awareness programs. Additionally, organizations should focus on eliminating frustrating tasks or reducing frustration caused by these tasks. Finally, organizations should strive to induce positive affect by evaluating employee affect levels, identifying areas that need correction, and quickly responding to issues prior to deviance or noncompliance.

## References


Adams, J. S. (1965). Inequity in social exchange. In L. Berkowitz (Ed.), *Advances in Experimental Social Psychology* (pp. 267-299). New York: Academic Press.

Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS Quarterly*, *24*(4), 665-694.

Aguirre-Urreta, M. I., & Marakas, G. M. (2012). Revisiting bias due to construct misspecification: Different results from considering coefficients in standardized form. *MIS Quarterly*, *36*(1), 123-138.

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology*, *30*(1), 47-87.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*, 179-211.

Alter, S. (2014). Theory of workarounds. *Communications of the Association for Information Systems*, *34*(55), 1041-1066.

Ambrose, M. L., & Cropanzano, R. (2003). A longitudinal analysis of organizational fairness: An examination of reactions to tenure and promotion decisions. *Journal of Applied Psychology*, *88*(2), 266-275.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613-643.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, *103*(3), 411-423.

Andrich, D. (1978). A rating formulation for ordered response categories. *Psychometrika*, *43*(4), 561-573.

Aquino, K., Lewis, M. U., & Bradfield, M. (1999). Justice constructs, negative affectivity, and employee deviance: A proposed model and empirical test. *Journal of Organizational Behavior*, *20*, 1073-1092.

Aytes, K., & Connolly, T. (2004). Computer security and risky computing practices. *Journal of Organizational and End User Computing*, *16*(3), 22-40.

Bagozzi, R. P., Gopinath, M., & Nyer, P. U. (1999). The role of emotions in marketing. *Journal of the Academy of Marketing Science*, *27*(2), 184-206.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*, *39*(Part B), 145-159.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don't even think about it! The effects of anti-neutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems*, *19*(8), 689-715.

Baron, R. M., & Kenny, D. A. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, *51*(6), 1173-1182.

Baron, S. W. (2007). Street youth, gender, financial strain, and crime: Exploring Broidy and Agnew's extension to general strain theory. *Deviant Behavior, 28*(3), 273-302.

Baskerville, R., Park, E. H., & Kim, J. W. (2010). An emote opportunity model of computer abuse. In *Proceedings of the 2010 Dewald Roode Information Security Workshop IFIP WG 8.11/11.13* (pp. 14-42).

Baumeister, R. F., Bratslavsky, E., Finkenauer, C., & Vohs, K. D. (2001). Bad is stronger than good. *Review of General Psychology*, *5*(4), 323-370.

Bennett, R. J., & Robinson, S. L. (2000). Development of a measure of workplace deviance. *Journal of Applied Psychology*, *85*(3), 349-360.

Bhattacherjee, A. (2001). Understanding information systems continuance: An expectation-confirmation model. *MIS Quarterly*, *25*(3), 351-370.

Bentler, P. M. (1992). On the fit of models to covariances and methodology to the Bulletin. *Psychological Bulletin, 112*(3), 400-404.

Bentler, P. M., & Bonett, D. G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological Bulletin, 88*(3), 588-606.

Bies, R. J., & Moag, J. F. (1986). Interactional justice: Common criteria of fairness. In R. Lewicki, B. Sheppard, & M. Bazerman (Eds.), *Research on Negotiations in Organizations* (1st ed., pp. 43-53). Greenwich, CT: JAI Press.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837-864.

Bradley, M. M., & Lang, P. J. (1994). Measuring

emotion: The self-assessment manikin and the semantic differential. *Journal of Behavioral Therapy and Experimental Psychiatry*, *25*(1), 49-59.

Browne, M. W., & Cudeck, R. (1992). Alternative Ways of Assessing Model Fit. *Sociological Methods Research, 21*(2), 230-258.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548.

Burns, A. J., Young, J., Roberts, T. L., Courtney, J. F., & Ellis, T. S. (2015). Exploring the role of contextual integrity in electronic medical record (EMR) system workaround decisions: an information security and privacy perspective. *AIS Transactions on Human-Computer Interaction*, *7*(3), 142-165.

Burton-Jones, A. (2009). Minimizing method bias through programmatic research. *MIS Quarterly*, *33*(3), 445-471.

Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin*, *56*(2), 81-105.

Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin*, *56*(2), 81-105.

Campbell, D. T., & Stanley, J. C. (1963). Experimental and quasi-experimental designs for research. In *Experimental and quasi-experimental designs for research*. Boston, MA: Houghton Mifflin.

Carmichael, S., & Piquero, A. R. (2004). Sanctions, perceived anger, and criminal offending. *Journal of Quantitative Criminology*, *20*(4), 371-393.

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems*, *31*(4), 49-87.

Chin, W. W., Thatcher, J. B., & Wright, R. T. (2012). Assessing common method bias: Problems with the ULMC Technique. *MIS Quarterly*, *36*(3), 1-11.

Chin, W. W., & Todd, P. A. (1995). On the use, usefulness, and ease of use of structural equation modeling in MIS research: A note of caution. *MIS Quarterly, 19*(2), 237-246.

Churchill, G. A. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research*, *16*, 64-73.

Cohen-Charash, Y., & Spector, P. E. (2001). The role of justice in organizations: A meta-analysis. *Organizational Behavior and Human Decision Processes*, *86*(2), 278-321.

Colquitt, J. A., Conlon, D. E., Wesson, M. J., Porter, C. O. L. H., & Ng, K. Y. (2001). Justice at the millenium: A meta-analytic review of 25 years of organizational justice research. *Journal of Applied Psychology*, *86*(3), 425-445.

Cowie, R., Douglas-Cowie, E., Tsapatsoulis, N., Votsis, G., Kollias, S., Fellenz, W., & Taylor, J. G. (2001). Ieee signal processing magazine. *IEEE Signal Processing Magazine*, *18*(1), 32-80.

Crossler, R. E., & Bélanger, F. (2009). The effects of security education training and awareness programs and individual characteristics on end user security tool usage. *Journal of Information System Security*, *5*(3), 3-22.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*(1), 90-101.

Csikszentmihaiyi, M. (1990). *Flow: The psychology of optimal experience*. New York, NY: Harper & Row.

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643-658.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, *31*(2), 285-318.

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

Dennis, A. R., & Minas, R. K. (2018). Security on autopilot: Why current security theories hijack our thinking and lead us astray. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *49*(SI), 15-38.

Dimoka, A., Banker, R. D., Benbasat, I., Davis, F. D., Dennis, A. R., Gefen, D., … Weber, B. (2012). On the use of neurophysiological tools in IS research: Developing a research agenda for NeuroIS. *MIS Quarterly*, *36*(3), 679-702.

Djamasbi, S., Strong, D. M., & Dishaw, M. (2010). Affect and acceptance: Examining the effects of positive mood on the technology acceptance

model. *Decision Support Systems*, *48*(2), 383-394.

Dupré, K. E., Barling, J., Turner, N., & Stride, C. B. (2010). Comparing perceived injustices from supervisors and romantic partners as predictors of aggression. *Journal of Occupational Health Psychology*, *15*(4), 359-370.

Ellis, M. E., Aguirre-Urreta, M. I., Sun, W. N., & Marakas, G. M. (2008). Establishing the need for measurement invariance in information systems research: A step-by-step example using technology acceptance research. *Proceedings of the Decision Science Institute* (pp. 4461-4466).

Emm, D. (2015). Navigating the threat landscape: A practical guide. *Kaspersky Lab Global IT Risks Security Survey 2015*, 1-20. Retrieved from https://media.kaspersky.com/pdf/kaspersky-threat-navigation-10-tips.pdf

Etherington, D. (2013). Android's design principles and the calculus of the human pleasure response. *TechCrunch*. Retrieved from http://techcrunch.com/2013/05/19/androids-design-principles-and-the-calculus-of-the-human-pleasure-response.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior*. Reading, MA: Addison-Wesley.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407-429.

Forman, A. S., & Watkins, E. E. (2009). Employee Sabotage. *Human Resource Executive Online*. Retrieved from http://www.hreonline.com/HRE/view/story.jhtml?id=225549614.

Fries, V., Wiesche, M., & Krcmar, H. (2016). The dualism of workarounds: Effects of technology and mental workload on improvement and noncompliant behavior within organizations. *Proceedings of the Thirty-Seventh International Conference on Information Systems*.

Gefen, D., & Straub, D. W. (2005). A practical guide to factorial validity using PLS-graph: Tutorial and annotated example. *Communications of the Association for Information Systems*, *16*(5), 91-109.

Gefen, D., Straub, D. W., & Boudreau, M.-C. (2000). Structural equation modeling techniques and regression: Guidelines for research practice. *Communications of the Association for Information Systems*, *4*(7), 1-77.

Gilleade, K. M., & Dix, A. (2004). Using frustration in the design of adaptive videogames. In *Proceedings of the 2004 ACM SIGCHI International Conference on Advances in computer entertainment technology* (pp. 228-232).

Gopal, R. D., & Sanders, G. L. (1997). Preventive and deterrent controls for software piracy. *Journal of Management Information Systems*, *13*(4), 29-47.

Gottman, J. (1994). *Why marriages succeed or fail*. New York, NY: Simon & Schuster.

Greenberg, J. (1990). Employee theft as a reaction to underpayment inequity: The hidden cost of pay cuts. *Journal of Applied Psychology*, *75*(6), 561-568.

Greenberg, J. (1993). Stealing in the name of justice: lnformational and interpersonal moderators of theft reactions to underpayment inequity. *Organizational Behavior and Human Decision Processes*, *54*(1), 81-103.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*(2), 203-236.

Haag, S., & Eckhardt, A. (2014). Normalizing the shadows: The role of symbolic models for individuals' shadow IT usage. *Proceedings of the International Conference on Information Systems* (pp. 1-13).

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis: A global perspective* (7th ed.). Upper Saddle River, NJ: Pearson Education.

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly*, *20*(3), 257-278.

Heilman, R. M., Cris, L. G., Houser, D., Miclea, M., & Miu, A. C. (2010). Emotion regulation and decision making under risk and uncertainty. *Emotion*, *10*(2), 257-265.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.

Herrnstein, R. J. (1990). Rational choice theory: Necessary but not sufficient. *American Psychologist*, *45*(3), 356-367.

Hogg, M. A., & Vaughan, G. M. (2005). *Social*

*Psychology* (4th ed.). London: Prentice-Hall.

Holdgrafer, R. (2015). Humans: Still the weakest link in the enterprise information security posture. Retrieved from https://www.linkedin.com/pulse/humans-still-weakest-link-enterprise-information-rachel-holdgrafer/?articleId=9140213823717830248.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management*, *49*(2), 99-110.

Hsu, C., Lee, J.-N., & Straub, D. W. (2012). Institutional influences on information systems security innovations. *Information Systems Research*, *23*(3-Part-2), 918-939.

Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., & Lowry, P. B. (2015). Effectiveness, the role of extra-role behaviors and social controls in information security policy. *Information Systems Research*, *26*(2), 282-300.

Hu, Q., West, R., & Smarandescu, L. (2015). The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems*, *31*(4), 6-48.

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

Ilies, R., De Pater, I. E., & Judge, T. A. (2007). Differential affective reactions to negative and positive feedback, and the role of self-esteem. *Journal of Managerial Psychology*, *22*(6), 590-609.

Ilies, R., & Judge, T. A. (2002). Understanding the dynamic relationships among personality, mood, and job satisfaction: A field experience sampling study. *Organizational Behavior and Human Decision Processes*, *89*(2), 1119-1139.

Inventado, P. S., Legaspi, R., Suarez, M., & Numao, M. (2011). Predicting student emotions resulting from appraisal of its feedback. *Research and Practice in Technology Enhanced Learning*, *6*(2), 107-133.

Isen, A. M., & Means, B. (1983). The influence of positive affect on decision-making strategy. *Social Cognition*, *2*(1), 18-31.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549-566.

Johnston, A. C., Warkentin, M., Dennis, A. R., & Siponen, M. (2019). Speak their language: Designing effective messages to improve employees' information security decision making. *Decision Sciences*, *50*(2), 245-284.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, *39*(1), 113-134.

Judge, T. A. (1993). Does affective disposition moderate the relationship between job satisfaction and voluntary turnover? *Journal of Applied Psychology*, *78*(3), 395-401.

Judge, T. A., Scott, B. A., & Ilies, R. (2006). Hostility, job attitudes, and workplace deviance: Test of a multilevel model. *The Journal of Applied Psychology*, *91*(1), 126-138.

Keith, M., Shao, B., & Steinbart, P. J. (2007). The usability of passphrases for authentication: An empirical field study. *International Journal of Human-Computer Studies*, *65*(1), 17-28.

Kerlinger, F. N. (1973). *Foundations of behavioral research* (2nd ed.). London, UK: Holt Reinhart & Winston.

Kim, J. J., Park, E. H., & Baskerville, R. (2012). Vengeance is mine: A model of emotional appraisal and computer abuse. *Proceedings of the 2012 Dewald Roode Information Security Workshop IFIP WG 8.11/11.13* (pp. 1-26).

Kline, R. B. (1998). *Principles and practice of structural equation modeling.* New York, NY: Guilford.

Koppel, R., Smith, S., Blythe, J., & Kothari, V. (2015). Workarounds to computer access in healthcare organizations: You want my password or a dead patient? In *Driving Quality in Informatics: Fulfilling the Promise* (Vol. 208, pp. 215-220). Amsterdam: IOS Press.

Lee, K., & Allen, N. J. (2002). Organizational citizenship behavior and workplace deviance: The role of affect and cognitions. *Journal of Applied Psychology*, *87*(1), 131-142.

Lerner, J. S., & Keltner, D. (2000). Beyond valence: Toward a model of emotion-specific influences on judgement and choice. *Cognition and Emotion*, *14*(4), 473-494.

Leventhal, G. S. (1980). What should be done with equity theory? New approaches to the study of fairness in social relationships. In K. J. Gergen, M. S. Greenberg, & R. H. Willis (Eds.), *Social exchange: Advances in theory and research* (pp. 27-55). New York, NY: Plenum.

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the

perspective of rational choice theory. *Decision Support Systems, 48*(4), 635-645.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, *33*(1), 71-90.

Lim, V. K. G. (2002). The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice. *Journal of Organizational Behavior*, *23*(5), 675-694.

Loewenstein, G. (1996). Out of control: Visceral influences on behavior. *Organizational Behavior and Human Decision Processes*, *65*(3), 272-292.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, *35*(2), 293-334.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., & Raghu, T. S. (2010). Moving toward black hat research in information systems security: An editorial introduction to the special issue. *MIS Quarterly*, *34*(3), 431-433.

Marakas, G. M., Yi, M. Y., & Johnson, R. D. (1998). The multilevel and multifaceted character of computer self-efficacy: Toward clarification of the construct and an integrative framework for research. *Information Systems Research, 9*(2), 126-163.

Marsh, H. W., Hau, K., & Wen, Z. (2004). In search of golden rules: Comment on hypothesis-testing approaches to setting cutoff values for fit indexes and dangers in overgeneralizing Hu and Bentler's (1999) findings. *Structural Equation Modeling, 11*(3), 320-341.

Miu, A. C., & Crisan, L. G. (2011). Cognitive reappraisal reduces the susceptibility to the framing effect in economic decision making. *Personality and Individual Differences*, *51*, 478-482.

Nakhaie, M. R., Silverman, R. A., & LaGrange, T. C. (2000). Self-control and social control: An examination of gender, ethnicity, class and delinquency. *Canadian Journal of Sociology, 25*(1), 35-59.

Newell, A. (1987). *Unified Theories of Cognition*. Harvard University Press.

Nunnally, J., & Bernstein, I. (1994). *Psychometric Theory* (3rd ed.). New York: McGraw-Hill.

Onwudiwe, I. D., Odo, J., & Onyeozili, E. C. (2005). Deterrence theory. In M. Bosworth (Ed.), *Encyclopedia of Prisons & Correctional Facilities* (Vol. 1, pp. 233-237). Thousand Oaks, CA: SAGE.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Which factors explain employees' adherence to information security policies? An empirical study. In *PACIS 2007 Proceedings* (pp. 438-439). Auckland, New Zealand.

Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law & Society Review*, *30*(3), 549-583.

Peace, A. G., Galletta, D. F., & Thong, J. Y. L. (2003). Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems*, *20*(1), 153-177.

Peter, J. P. (1979). Reliability: A review of psychometric basics and recent marketing practices. *Journal of Marketing Research*, *16*(1), 6-17.

Peter, J. P. (1981). Construct validity: A review of basic issues and marketing practices. *Journal of Marketing Research*, *18*(2), 133-145.

Peter, T., LaGrange, T. C., & Silverman, R. A. (2003). Investigating the interdependence of strain and self-control. *Canadian Journal of Criminology & Criminal Justice*, *45*(4), 431-464.

Petter, S., Straub, D. W., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly*, *31*(4), 623-656.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & 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), 879-903.

Puhakainen, P. (2006). *A design theory for information security awareness* (PhD Diss., University of Oulu, Oulu, Finland).

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 757-778.

Rennie, L. J. (1982). Detecting a response set to Likert-style attitude items with the rating model. *Education Research and Perspectives*, *9*(1), 114-118.

Richardson, H. A., Simmering, M. J., & Sturman, M. C. (2009). A tale of three perspectives: Examining post hoc statistical techniques for detection and correction of common method variance. *Organizational Research Methods*, *12*(4), 762-800.

Richardson, R. (2011). *2010/2011 CSI computer crime and security survey*. Retrieved from https://cours.etsmtl.ca/gti619/documents/divers/

CSIsurvey2010.pdf

Roche, S. M., & McConkey, K. M. (1990). Absorption: Nature, assessment, and correlates. *Journal of Personality and Social Psychology*, *59*(1), 91-101.

Roseman, I. J., Spindel, M. S., & Jose, P. E. (1990). Appraisals of emotion-eliciting events: Testing a theory of discrete emotions. *Journal of Personality and Social Psychology*, *59*(5), 899-915.

Rucker, D. D., McShane, B. B., & Preacher, K. J. (2015). A researcher's guide to regression, discretization, and median splits of continuous variables. *Journal of Consumer Psychology*, *25*(4), 666-678.

Russell, J. A. (2003). Core affect and the psychological construction of emotion. *Psychological Review*, *110*(1), 145-172.

Sager, J. K. (1991). A longitudinal assessment of change in sales force turnover. *Journal of the Academy of Marketing Science*, *19*(1), 25-36.

Salovaara, A., & Merikivi, J. (2015). IS research progress would benefit from increased falsification of existing theories. *Proceedings of the European Conference on Information Systems*.

Sanfey, A. C., Rilling, J. K., & Aronson, J. A. (2003). The neural basis of economic decision-making in the ultimatum game. *Science*, *300*(5626), 1755-1759.

Scherer, K. R. (2005). What are emotions? And how can they be measured? *Social Science Information*, *44*(4), 695-729.

Schumacker, R. E., & Lomax, R. G. (2004). *A beginner's guide to structural equation modeling* (2nd ed.). Mahwah, NJ: Lawrence Erlbaum.

Seo, M., & Barrett, L. F. (2007). Being emotional during decision making—good or bad? An empirical investigation. *The Academy of Management Journal*, *50*(4), 923-940.

Shapiro, D. L., Buttner, E. H., & Barry, B. (1994). Explanations: What factors enhance their perceived adequacy? *Organizational Behavior and Human Decision Processes*, *58*(3), 346-368.

Simon, H. A. (1947). Rationality in administrative behavior. In *Administrative Behavior* (4th ed., Vol. 2, pp. 72-86). New York, NY: The Free Press.

Simon, H. A. (1952). A behavioral model of rational choice. *Quarterly Journal of Economics*, 99-118.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31-41.

Siponen, M. (2005). An analysis of the traditional IS security approaches: Implications for research and practice. *European Journal of Information Systems*, *14*(3), 303-315.

Siponen, M., & Iivari, J. (2006). Six design theories for IS security policies and guidelines. *Journal of the Association for Information Systems*, *7*(7), 445-472.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: An empirical study. *Proceedings of the IFIP SEC 2007 Conference*.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487-502.

Skyhigh Networks. (2015). Skyhigh report: Average enterprise experiences more than 16 insider threats, exploited account credentials and data exfiltration incidents each month. Retrieved from https://www.skyhighnetworks.com/press/skyhigh-report-average-enterprise-experiences-more-than-16-insider-threats-exploited-account-credentials-and-data-exfiltration-incidents-each-month/.

Sokol-Hessner, P., Camerer, C. F., & Phelps, E. A. (2013). Emotion regulation reduces loss aversion and decreases amygdala responses to losses. *SCAN*, *8*, 341-350.

Sokol-Hessner, P., Hsu, M., Curley, N. G., Delgado, M. R., Camerer, C. F., Phelps, E. A., & Smith, E. E. (2009). Thinking like a trader selectively reduces individuals' loss aversion. *Proceedings of the National Academy of Sciences of the United States of America* (Vol. 106, pp. 5035-5040).

Spector, P. E. (1978). Organizational frustration: A model and review of the literature. *Personnel Psychology*, *31*(4), 815-829.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124-133.

Steenkamp, J.-B. E. M., & Baumgartner, H. (1998). Assessing measurement invariance in cross-national consumer research. *Journal of Consumer Research*, *25*(1), 78-107.

Stein, M.-K., Newell, S., Wagner, E. L., & Galliers, R. D. (2015). Coping with information technology:

Mixed emotions, vacillation, and nonconforming use patterns. *MIS Quarterly*, *39*(2), 367-392.

Steinbart, P. J., Keith, M. J., & Babb, J. (2016). Examining the continuance of secure behavior: A longitudinal field study of mobile device authentication. *Information Systems Research*, *27*(2), 219-239.

Stephens, J. M. (2005). Justice of just us? What to do about cheating. In A. Lathrop & K. Foss (Eds.), *Guiding students from cheating and plagiarism to honesty and integrity: Strategies for change* (pp. 32-34). Westport, CT: Libraries Unlimited

Straub, D. W. (2009). *Black hat, white hat studies in information security*. Keynote address presented at IFIP WG 8.11/11.13 Workshop on Information Security Research. Cape Town, South Africa.

Straub, D. W., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, *13*(1), 381-427.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, *22*(6), 664-670.

Tellegen, A., & Atkinson, G. (1974). Openness to absorbing and self-altering experiences ("absorption"), a trait related to hypnotic susceptibility. *Journal of Abnormal Psychology*, *83*(3), 268-277.

Thomson, M. E., & von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management & Computer Security*, *6*(4), 167-173.

Trevino, L. K., & Webster, J. (1992). Flow in computer-mediated communication: Electronic mail and voice mail evaluation and impacts. *Communication Research*, *19*(5), 539-573.

Tsai, H., & Bagozzi, R. P. (2014). Contribution behavior in virtual communities: Cognitive, emotional, and social influences. *MIS Quarterly*, *38*(1), 143-163.

Turel, O., Yuan, Y., & Connelly, C. E. (2008). In justice we trust: Predicting user acceptance of e-customer services. *Journal of Management Information Systems*, *24*(4), 123-151.

Tyler, T. R., & Bies, R. J. (1990). Beyond formal procedures: The interpersonal context of procedural justice. In J. S. Carroll (Ed.), *Applied Social Psychology in Business Settings* (pp. 77-98). Hillsdale, NJ: Erlbaum.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, *29*(4), 263-290.

Vormetric. (2016). *Data Threat Report*. Retrieved from http://enterprise-encryption.vormetric.com/rs/480-LWA-970/images/Vormetric_2016_Data_Threat_Report_Global_WEB.pdf.

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*(3), 191-198.

Warkentin, M., & Johnston, A. C. (2006). IT security governance and centralized security controls. In M. Warkentin & R. B. Vaughn (Eds.), *Enterprise Information Systems Assurance and System Security: Managerial and Technical Issues* (1st ed., pp. 16-24). Hershey, PA: Idea Group.

Warkentin, M., & Johnston, A. C. (2008). IT governance and organizational design for security management. In D. Straub, S. Goodman, & R. L. Baskerville (Eds.), *Information Security Policies and Practices* (pp. 46-68). Armonk, NY: Sharpe.

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, *20*(3), 267-284.

Warkentin, M., Johnston, A., Walden, E., & Straub, D. (2016). Neural correlates of protection motivation for secure IT behaviors: An fMRI examination. *Journal of the Association for Information Systems*, *17*(3), 194-215.

Warkentin, M., Shropshire, J. D., & Straub, D. W. (2018). *Protect their information: Fostering employee compliance with information security protocols*.

Warkentin, M., Straub, D., & Malimage, K. (2012). Measuring secure behavior: A research commentary. *Proceedings of the Annual Symposium on Information Assurance*.

Watson, D., Clark, L. A., & Tellegen, A. (1988). Development and validation of brief measures of positive and negative affect: The PANAS scales. *Journal of Personality and Social Psychology*, *54*(6), 1063-1070.

Webster, J., & Martocchio, J. J. (1992). Microcomputer playfulness: Development of a measure with workplace implications. *MIS Quarterly*, *16*(2), 201-226.

Weiss, H. M., & Cropanzano, R. (1996). Affective events theory: A theoretical discussion of the structure, causes and consequences of affective experiences at work. In B. M. Staw & L. L. Cummings (Eds.), *Research in Organizational*

*Behavior: An Annual Series of Analytical Essays and Critical Reviews* (pp. 1-74). Greenwich, CT: JAI Press.

Westland, C. (1997). A rational choice model of computer and network crime. *International Journal of Electronic Commerce*, *1*(2), 109-126.

Whetten, D. A., Felin, T., & King, B. G. (2009). The practice of theory borrowing in organizational studies: Current issues and future directions. *Journal of Management*, *35*(3), 537-563.

Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: Considering systems risk from a criminological perspective. *European Journal of Information Systems*, *15*(4), 403-414.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, *37*(1), 1-20.

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence, and neutralization perspectives. *Information Systems Journal*, *28*(2), 266-293.

Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, *27*(1), 273-303.

Yang, Q., Tang, P., Gu, R., Luo, W., & Luo, Y. (2014). Implicit emotion regulation affects outcome evaluation. *Social Cognitive and Affective Neuroscience*, *10*(6), 1-8.

Zhang, P. (2013). The affective response model: A theoretical framework of affective concepts and their relationships in the ICT context. *MIS Quarterly*, *37*(1), 247-274.

Zhang, P., Li, N., & Sun, H. (2006). Affective quality and cognitive absorption: Extending technology acceptance research. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*.

Zimbardo, P. G., Keough, K. A., & Boyd, J. N. (1997). Present time perspective as a predictor of risky driving. *Personality and Individual Differences*, *23*(6), 1007-1023.

Zorz, Z. (2013). Snowden social-engineered co-workers to share their passwords. Retrieved from https://www.helpnetsecurity.com/2013/11/11/snowden-social-engineered-co-workers-to-share-their-passwords/.

# Appendix A: Items, Original Items, and Source

**Table A1. Construct Items and Source**

| Item ID | Item | Original item | Source |
|---|---|---|---|
| **Negative affective absorption** | | | |
| NAA1 | In general, I lose track of time when I experience negative emotions. | | Developed for this study |
| NAA2 | In general, negative emotions occupy my attention. | | |
| NAA3 | In general, it is hard for me to focus on something other than my negative emotions. | | |
| NAA4 | In general, I become deeply involved with my negative emotions. | | |
| NAA5 | In general, I have no control over my negative emotions. | | |
| **Distributive injustice** | | | |
| DINJ1 | Based on the effort I put into this exercise, the extra credit I received was unfair. | How fairly has the organization been rewarding you for the amount of effort you have put in? | Lim (2002) |
| DINJ2 | Based on the instructions I was assigned during this exercise, the extra credit I received was unfair. | How fairly has the organization been rewarding you for the responsibilities you have? | |
| DINJ3 | Based on the decisions I completed during this exercise, the extra credit I received was. | How fairly has the organization been rewarding you for the work that you have done well? | |
| DINJ4 | Based on the stress I experienced during this exercise, the extra credit I received was unfair. | How fairly has the organization been rewarding you for the stresses and strains of your job? | |
| DINJ5 | Based on the training provided during the exercise, the extra credit I received was unfair. | How fairly has the organization been rewarding you for the amount of education and training you received? | |
| **Procedural injustice** | | | |
| PINJ1 | The decision process of this exercise was unreasonable. | Have you had influence over the outcome arrived at by those procedures? | Turel, Yuan, & Connelly (2008) |
| PINJ2 | The decision process of this exercise was inconsistent. | Have those procedures been applied consistently? | |
| PINJ3 | The decision process of this exercise was unfair. | Have those procedures been free of bias? | |
| PINJ4 | The decision process of this exercise was flawed. | Have those procedures been based on accurate information? | |
| PINJ5 | The decision process of this exercise was rigged. | Created for this study. | |
| **Interpersonal injustice** | | | |
| IINJ1 | During the exercise, I was treated in a polite manner. | The service representative treated you in a polite manner? | Turel, Yuan, & Connelly (2008) |
| IINJ2 | During the exercise, I was treated with dignity. | The service representative treated you with dignity? | |
| IINJ3 | During the exercise, I was treated with respect. | The service representative treated you with respect? | |

**Table A1. Construct Items and Source**

| | | | |
|---|---|---|---|
| **Informational injustice** | | | |
| FINJ1 | The video presentation did not explain this exercise thoroughly. | Has the service representative explained the procedure thoroughly? | Turel, Yuan, & Connelly (2008) |
| FINJ2 | The video presentation explanations regarding this exercise were unreasonable. | Were the service representative explanations regarding the procedure reasonable? | |
| FINJ3 | The experimental instructions were conveyed using a method I do not prefer. | Has the service representative seemed to tailor communications to individuals' specific needs? | |
| FINJ4 | The video presentation did not sufficiently provide detailed instructions about the exercise. | Has the service representative been candid in communications with you? | |
| **Attitude toward specific information security policy** | | | |
| SATT1 | In this exercise, it was important that I not share my password. | Adopting security technologies and practices is important. | Herath & Rao (2009b); Bulgurcu et al. (2010) |
| SATT2 | In this exercise, it was critical that I not share my password. | Adopting security technologies and practices is beneficial. | |
| SATT3 | In this exercise, it was essential that I not share my password. | Adopting security technologies and practices is helpful. | |
| SATT4 | In this exercise, it was necessary that I not share my password. | To me, complying with the requirements of the ISP is unnecessary/necessary. | |
| **Negative affective flow** | | | |
| NAF1 | During this exercise, I lost track of time due to my negative emotions. | | Developed for this study. |
| NAF2 | During this exercise, negative emotions occupied my attention. | | |
| NAF3 | During this exercise, it was hard to focus on something other than the negative emotions I experienced. | | |
| NAF4 | During this exercise, I became deeply involved with negative emotions. | | |
| NAF5 | During this exercise, I had no control over my negative emotions. | | |

# Appendix B: Survey Instrument

## B.1 Consent

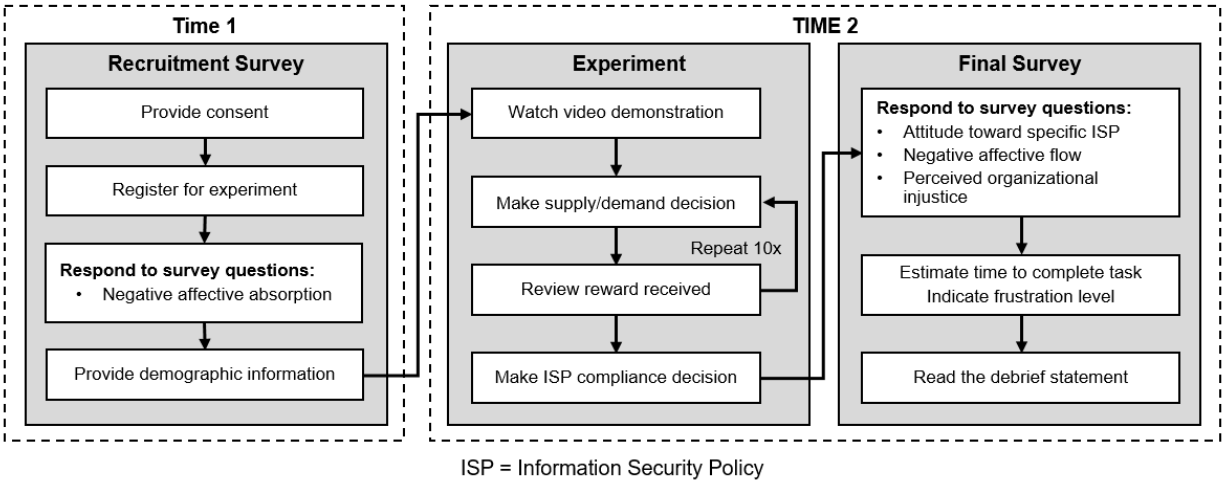


**Figure B1. Laboratory Experiment Flow**

Organizations are increasingly concerned about protecting company information. Therefore, they have established necessary safeguards (such as information security policies and procedures) to inform employees of organizational expectations and consequences. Policy compliance is vital to protecting organizational information.

In order for us to better understand ISP compliance, we ask that you participate in this study. If you participate in this study, you will be asked to complete a laboratory experiment that will take about 20-30 minutes to complete. The laboratory experiment involves a series of supply and demand tasks.

Please understand that your **participation is voluntary**. Your **refusal to participate will involve no penalty or loss of benefits** to which you are otherwise entitled. You **may discontinue your participation** at any time without penalty or loss of benefits. Through the duration of the study, your name and netID will be collected in order to register you for a lab time and award you extra credit upon the completion of the laboratory experiment.

Participating in this research may lead to heightened understanding about the importance of information security policies. In order to be rewarded extra credit you must complete the laboratory experiment.

## B.1 Recruitment Survey

Please provide the following information to register for the laboratory experiment.

**Table B1. Registration**

| Categories | Measure |
|---|---|
| First Name: | |
| Last Name: | |
| Net ID (e.g., abc123): | |
| Time slot: | [drop down including available time slots] |

Please indicate the degree to which you **agree** with each statement (1 = *strongly disagree*, 2 = *disagree*, 3 = *neutral*, 4 = *agree*, and 5 = *strongly agree*). Please note that while some of these questions are similar to each other, each question has a specific purpose. Thus, please pay careful attention to each question.

**Table B2. Negative Affective Absorption**

| Item | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| In general, I lose track of time when I experience negative emotions (NAA1). | | | | | |
| In general, negative emotions occupy my attention (NAA2). | | | | | |
| In general, it is hard for me to focus on something other than my negative emotions (NAA3). | | | | | |
| In general, I become deeply involved with my negative emotions (NAA4). | | | | | |
| In general, I have no control over my negative emotions (NAA5). | | | | | |

Please answer the following demographic information. This demographic information will not be used to identify respondents.

**Table B3. Demographics**

| | |
|---|---|
| Grade: To the best of your knowledge, what is your current grade in the class? | A |
| | B |
| | C |
| | D |
| | F |
| Expected Grade: What grade do you expect to earn in class? | A |
| | B |
| | C |
| | D |
| | F |
| Extra credit: How important is earning extra credit to you? | Not important |
| | Somewhat important |
| | Moderately important |
| | Important |
| | Very important |
| Gender: What is your gender? | Male |
| | Female |
| Age: Please select your age. | 18-100 |
| Education: What is the highest level of education you have completed? | High school |
| | Associate's degree |
| | Bachelor's degree |
| | Master's degree |
| | Doctorate/professional degree |
| | Other |
| Ethnicity: What is your ethnicity? | American Indian or Alaska Native |
| | Asian |
| | Black or African American |
| | Native Hawaiian or other Pacific Islander |
| | White |

## B.2 File Download Instructions

Please visit the following URL: [insert download location]. An Excel document will be downloaded to your computer. Save the file to your desktop or some other location and then open it.

When you open the document, your document may open in protected view. If it opens in protected view, please click "Enable Editing." Similarly, you may see a security warning that macros have been disabled. Please "Enable Content" in order to begin the simulation.

If you run into errors, please close and reopen the document. When everyone is ready, I will begin a video presentation that describes the laboratory experiment.

## B.3 Video Presentation and Laboratory Experiment

The purpose of this video presentation is to describe the task you are about to complete. After opening the Excel document, a pop-up message appears asking you to enter your user ID. Please enter the three-digit number you were provided when you entered the lab.

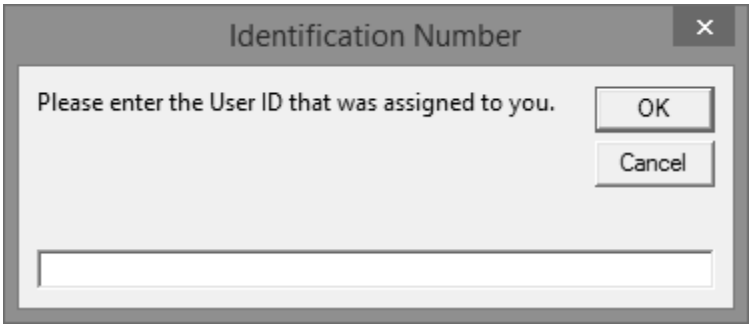


**Figure B2. User ID Popup Message**

After entering your user ID, you will see a production simulation. In this simulation, you play the role of a production manager for a new company product. In order to protect company information, organizations establish information security policies and procedures to inform employees of organizational expectations and consequences. Password guidelines are included as part of these policies which state that users should never share passwords with others. Therefore, you are expected to keep your password secret.

As a production manager, you are required to determine how many units to produce each month in order to meet demand. In addition to meeting the expected demand, your company wants you to maintain an additional 325 units in inventory. You will complete 20 decisions in this simulation.

This table (Figure B3) shows your production information. Your decision # shows you the decision you are currently on. Your current inventory displays how much you have in storage; this number begins at 0, but ideally you want to keep it at 325. The following three rows show you the expected demand for the current month, the next month, and in two months. Use this information to help you make a decision; enter your decision in the yellow box here and then click "Submit." Repeat this process for 20 decisions.

Since you will need to make 20 decisions, I will demonstrate one decision. First, we look at the expected demand for the current month and add enough production units to maintain 325 units of current inventory. Next, enter a value based on the summation of these two values. For example, let's try 2850 units and click "Submit."

After each decision, you will receive immediate feedback (see Figure B3). You will see your decision and how it compares to the actual required production needed. A percent error is calculated based on the difference and a reward is given. Ten reward points are given if your percent error is in the green range (less than 10% error), five reward points if it is in the yellow range (greater than or equal to 10% error but less than 25% error), and zero reward points if it is in the red range (greater than or equal to 25% error).

| Production Information | | | Decision History | | | | |
|---|---|---|---|---|---|---|---|
| User ID: | 025 | Total | Decision # | Your Decision | Required Production | Percent Error | Reward |
| Decision #: | | 9 | 6 | 2500 | 2540 | 1.57% | 10 |
| Current inventory (Try to keep 325 units): | | 312 | 7 | 2500 | 2359 | 5.98% | 10 |
| Expected demand for current month: | | 2593 | 8 | 2200 | 2309 | 4.72% | 10 |
| Expected demand for next month: | | 2623 | 9 | 2500 | 2212 | 13.02% | 5 |
| Expected demand in two months: | | 2279 | 10 | 3000 | 2302 | 30.32% | 0 |
| Enter decision #9: | | | Average Percent Error | | | 7.37% | Good |
| | | Submit | Total Reward | | | 80 | |

**Figure B3. Production Information, Decision History, and Feedback**

Note that the reward points earned in this simulation determine how much extra credit you will receive at the end (i.e., percentage of total extra credit is determined as a percentage of total possible points earned in the experiment). Use this information to help you make better decisions.

If you forget anything that was described in the demo, these two cells (see Figure B.4) serve as a summary on how to make a decision and what the decision history means. Now, go ahead and make your decisions. Good luck!

| | |
|---|---|
| **Do the following for each decision:**<br>1) Determine how many units to produce to meet expected demand<br>2) Maintain an additional 325 units in inventory<br>3) Enter your decision and then click submit | The "Decision History" section shows your decision as it compares to the actual required production. A percent error is calculated and color-coded:<br>• Good performance < 10% error<br>• Okay performance ≥ 10% error and < 25% error<br>• Poor performance ≥ 25% error |

**Figure B4. Summary Guide to Decision-Making and Decision History**

## B.4 Information Security Policy Compliance

A co-worker has offered to help you select the appropriate supply to meet expected demand. However, in order to receive help from your co-worker, you will need to share your password.

If you want to receive help from your co-worker, please enter your password and click the “OK” button. Otherwise, please click the “Cancel” button.

## B.5 Final Survey (All Items Were Randomized)

Please indicate the degree to which you **agree** with each statement (1 = *strongly disagree*, 2 = *disagree*, 3 = *neutral*, 4 = *agree*, and 5 = *strongly agree*). Please note that while some of these questions are similar to each other, each question has a specific purpose. Thus, please pay careful attention to each question.

**Table B4. Negative Affective Absorption**

| Item | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| In this exercise, it was important that I not share my password (SATT1). | | | | | |
| In this exercise, it was critical that I not share my password (SATT2). | | | | | |
| In this exercise, it was essential that I not share my password (SATT3). | | | | | |
| In this exercise, it was necessary that I not share my password (SATT4). | | | | | |
| During this exercise, I lost track of time due to my negative emotions (NAF1). | | | | | |
| During this exercise, negative emotions occupied my attention (NAF2). | | | | | |
| During this exercise, it was hard to focus on something other than the negative emotions I experienced (NAF3). | | | | | |
| During this exercise, I became deeply involved with negative emotions (NAF4). | | | | | |
| During this exercise, I had no control over my negative emotions (NAF5). | | | | | |
| Based on the effort I put into this exercise, the amount of extra credit I received was unfair (DINJ1). | | | | | |
| Based on the instructions I was given during this exercise, the amount of extra credit I received was unfair (DINJ2). | | | | | |
| Based on the decisions I completed during this exercise, the amount of extra credit I received was unfair (DINJ3). | | | | | |
| Based on the stress I experienced during this exercise, the amount of extra credit I received was unfair (DINJ4). | | | | | |
| Based on the training provided during the exercise, the amount of extra credit I received was unfair (DINJ5). | | | | | |
| The decision process of this exercise was unreasonable (PINJ1). | | | | | |
| The decision process of this exercise was inconsistent (PINJ2). | | | | | |
| The decision process of this exercise was unfair (PINJ3). | | | | | |
| The decision process of this exercise was flawed (PINJ4). | | | | | |
| The decision process of this exercise was rigged (PINJ5). | | | | | |
| The video presentation did not explain this exercise thoroughly (FINJ1). | | | | | |
| The video presentation explanations regarding this exercise were unreasonable (FINJ2). | | | | | |
| The experimental instructions were conveyed using a method I do not prefer (FINJ3). | | | | | |
| The video presentation did not sufficiently provide detailed instructions about the exercise (FINJ4). | | | | | |
| During the exercise, I was not treated in a polite manner (IINJ1). | | | | | |
| During the exercise, I was not treated with dignity (IINJ2). | | | | | |
| During the exercise, I was not treated with respect (IINJ3). | | | | | |

**Table B5. Additional Items**

| | |
|---|---|
| Without looking at the clock, please indicate how much time you think it took to complete all ten decisions. | Minutes |
| Please indicate how irritated this exercise made you. | Not irritated at all |
| | Somewhat irritated |
| | Moderately irritated |
| | Very irritated |
| | Extremely irritated |
| Previously, you indicated that you were [frustration level] during this exercise. Please describe why this exercise you were [frustration level]? | |

## B.6 Debrief

Thank you for your participation in the experiment. You will not be required to complete the remaining 10 decisions. Also, despite that the experiment indicated previously that the total extra credit you earned was determined on your success, you will be rewarded **full extra credit** for your participation.

Please check the following box indicating that you promise not to disclose this experiment to others.

# Appendix C: Sample Characteristics

**Table C1. Demographic Frequency and Percentages (n = 331)**

| Item | Measure | Frequency | Percentage |
|---|---|---|---|
| **Grade:** To the best of your knowledge, what is your current grade in the class | A | 7 | 2.4% |
| | B | 26 | 8.2% |
| | C | 76 | 24.2% |
| | D | 127 | 40.8% |
| | F | 80 | 24.5% |
| **Expected Grade:** What grade do you expect to earn in class? | A | 238 | 74.0% |
| | B | 74 | 24.8% |
| | C | 4 | 1.2% |
| | D | 0 | 0% |
| | F | 0 | 0% |
| **Extra credit:** How important is earning extra credit to you | Not important | 1 | 0.3% |
| | Somewhat important | 3 | 0.9% |
| | Moderately important | 14 | 4.2% |
| | Important | 66 | 20.2% |
| | Very important | 232 | 74.3% |
| **Gender:** What is your gender? | Male | 176 | 53.8% |
| | Female | 140 | 46.2% |
| **Education:** What is the highest level of education you have completed? | High school | 249 | 79.5% |
| | Associate's degree | 58 | 17.8% |
| | Bachelor's degree | 6 | 1.8% |
| | Master's degree | 0 | 0% |
| | Doctorate/professional degree | 0 | 0% |
| | Other | 3 | 0.9% |
| **Ethnicity:** What is your ethnicity? | American Indian or Alaska Native | 3 | 0.9% |
| | Asian | 14 | 4.2% |
| | Black or African American | 58 | 18.1% |
| | Native Hawaiian or Other Pacific Islander | 0 | 0% |
| | White | 241 | 76.7% |
| **Age:** Please select your age. | 18-100 | Average: 21.38 | |

# Appendix D: Exploratory Factor Analysis

Reliability scores were reassessed by computing Cronbach's Alpha with all constructs for both groups exhibiting an acceptable level of reliability (Nunnally & Bernstein, 1994, see Table D1; $\alpha \geq .70$). Additionally, convergent and discriminant validity were assessed using principal components analysis and varimax rotation in SPSS 21 (Hair, Black, Babin, & Anderson, 2010). Both groups indicated that each construct had convergent and discriminant validity in the more frustrated group and all but informational injustice had convergent and discriminant validity in the less frustrated group (Campbell & Fiske, 1959; Hair et al., 2010; J. P. Peter, 1981; Straub, Boudreau, & Gefen, 2004, see Table D2 and Table D3). No adjustments were made to the informational injustice items because confirmatory factor analysis did not indicate any convergent or discriminant validity issues (see Tables H-1 and H-2).

**Table D1. Cronbach's Alpha**

| | More frustrated group (*n* = 155) | | Less frustrated group (*n* = 176) | |
|---|---|---|---|---|
| **Item** | **Cronbach's alpha** | **Cronbach's alpha if Item deleted** | **Cronbach's alpha** | **Cronbach's alpha if Item deleted** |
| NAA2 | 0.819 | 0.774 | 0.783 | 0.679 |
| NAA3 | | 0.726 | | 0.737 |
| NAA4 | | 0.753 | | 0.701 |
| DINJ1 | 0.926 | 0.910 | 0.937 | 0.925 |
| DINJ2 | | 0.914 | | 0.915 |
| DINJ3 | | 0.905 | | 0.914 |
| DINJ4 | | 0.914 | | 0.932 |
| DINJ5 | | 0.904 | | 0.924 |
| IINJ1 | 0.884 | 0.807 | 0.855 | 0.808 |
| IINJ2 | | 0.853 | | 0.808 |
| IINJ3 | | 0.844 | | 0.778 |
| FINJ1 | 0.886 | 0.805 | 0.891 | 0.796 |
| FINJ2 | | 0.876 | | 0.894 |
| FINJ4 | | 0.833 | | 0.833 |
| NAF2 | 0.884 | 0.843 | 0.873 | 0.863 |
| NAF3 | | 0.841 | | 0.805 |
| NAF4 | | 0.832 | | 0.836 |
| NAF5 | | 0.884 | | 0.843 |
| SATT1 | 0.922 | 0.911 | 0.901 | 0.871 |
| SATT2 | | 0.875 | | 0.847 |
| SATT3 | | 0.901 | | 0.854 |
| SATT4 | | 0.908 | | 0.917 |

*Notes:* DINJ = perceived distributive injustice; IINJ = perceived interpersonal injustice; FINJ = perceived informational injustice; NAA = negative affective absorption; NAF = negative affective flow; SATT = attitude toward specific information security policy

**Table D2. Construct Validity for the More Frustrated Group**

| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| **NAA2** | 0.825 | | | | | |
| **NAA3** | 0.860 | | | | | |
| **NAA4** | 0.847 | | | | | |
| **DINJ1** | | 0.863 | | | | |
| **DINJ2** | | 0.801 | | | | |
| **DINJ3** | | 0.833 | | | | |
| **DINJ4** | | 0.802 | | | | |
| **DINJ5** | | 0.832 | | | | |
| **IINJ1** | | | 0.898 | | | |
| **IINJ2** | | | 0.816 | | | |
| **IINJ3** | | | 0.863 | | | |
| **FINJ1** | | | | 0.844 | | |
| **FINJ2** | | | | 0.780 | | |
| **FINJ4** | | | | 0.835 | | |
| **NAF2** | | | | | 0.790 | |
| **NAF3** | | | | | 0.805 | |
| **NAF4** | | | | | 0.846 | |
| **NAF5** | | | | | 0.698 | |
| **SATT1** | | | | | | 0.877 |
| **SATT2** | | | | | | 0.906 |
| **SATT3** | | | | | | 0.861 |
| **SATT4** | | | | | | 0.854 |

*Notes:* correlations below 0.40 were suppressed (Hair et al., 2010)

DINJ = perceived distributive injustice; IINJ = perceived interpersonal injustice; FINJ = perceived informational injustice; NAA = negative affective absorption; NAF = negative affective flow; SATT = attitude toward specific information security policy

**Table D3. Construct Validity for the Less Frustrated Group**

| | 1 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| **NAA2** | 0.840 | | | | | |
| **NAA3** | 0.804 | | | | | |
| **NAA4** | 0.821 | | | | | |
| **DINJ1** | | 0.857 | | | | |
| **DINJ2** | | 0.852 | | | | |
| **DINJ3** | | 0.877 | | | | |
| **DINJ4** | | 0.794 | | | | |
| **DINJ5** | | 0.811 | | | | |
| **IINJ1** | | | 0.802 | | | |
| **IINJ2** | | | 0.764 | | | |
| **IINJ3** | | | 0.870 | | | |
| **FINJ1** | | 0.413 | | 0.811 | | |
| **FINJ2** | | 0.516 | | 0.588 | | |
| **FINJ4** | | | | 0.825 | | |
| **NAF2** | | | | | 0.703 | |
| **NAF3** | | | | | 0.818 | |
| **NAF4** | | | | | 0.684 | |
| **NAF5** | | | | | 0.822 | |
| **SATT1** | | | | | | 0.844 |
| **SATT2** | | | | | | 0.900 |
| **SATT3** | | | | | | 0.900 |
| **SATT4** | | | | | | 0.798 |

*Notes:* correlations below 0.40 were suppressed (Hair et al., 2010)

DINJ = perceived distributive injustice; IINJ = perceived interpersonal injustice; FINJ = perceived informational injustice; NAA = negative affective absorption; NAF = negative affective flow; SATT = attitude toward specific information security policy

# Appendix E: Model Fit

The $\chi^2$ index ($\chi^2/df$), considered one of the better goodness of fit statistics (Marsh, Hau, & Wen, 2004), should be below 5 for ok fit (Schumacker & Lomax, 2004) or below 3 for acceptable fit (Kline, 1998). Additionally, the Incremental Fit Index, Tucker-Lewis Index, and Comparative Fit Index statistics should be greater than or equal to 0.90 (Bentler, 1992; Bentler & Bonett, 1980; Chin & Todd, 1995). The root mean square error of approximation should be less than 0.08 (Browne & Cudeck, 1992). A measurement model and structural model could not be obtained for the attitudinal model (See Figure 2) because the only other construct other than attitude was information security policy compliance which is a binary variable. In both the affective model and complete model, all fit indices suggest that both the measurement model and the structural model were a good fit to the data (see Table E1, Table E2, Table E3, and Table E4).

**Table E1. Model Fit Statistics for the Affective Measurement Model (See Figure 4)**

| Goodness of fit statistic | Recommended value | Calculated value |
|---|---|---|
| $\chi^2$ | -- | 115.411 |
| Degrees of freedom (*df*) | -- | 82 |
| $\chi^2$ statistical significance (p-value) | -- | 0.009 |
| $\chi^2$ Index ($\chi^2/df$) | $\leq 3$ | 1.407 |
| Incremental Fit Index (IFI) | $\geq .90$ | 0.984 |
| Tucker-Lewis Index (TLI) | $\geq .90$ | 0.978 |
| Comparative Fit Index (CFI) | $\geq .90$ | 0.984 |
| Root mean square error of approximation (RMSEA) | $\leq .80$ | 0.035 |

**Table E2. Model Fit Statistics for the Affective Structural Model (See Figure 4)**

| Goodness of fit statistic | Recommended value | Calculated value |
|---|---|---|
| $\chi^2$ | -- | 203.802 |
| Degrees of freedom (*df*) | -- | 108 |
| $\chi^2$ statistical significance (*p*-value) | -- | 0.000 |
| $\chi^2$ Index ($\chi^2/df$) | $\leq 3$; $\leq 5$ | 1.887 |
| Incremental Fit Index (IFI) | $\geq .90$ | 0.954 |
| Tucker-Lewis Index (TLI) | $\geq .90$ | 0.944 |
| Comparative Fit Index (CFI) | $\geq .90$ | 0.954 |
| Root mean square error of approximation (RMSEA) | $\leq .60$; $\leq .80$ | 0.052 |

**Table E3. Model Fit Statistics for the Full Measurement Model (See Figure 5 and Figure 6)**

| Goodness of fit statistic | Recommended value | Calculated value |
|---|---|---|
| $\chi^2$ | -- | 537.01 |
| Degrees of freedom (*df*) | -- | 388 |
| $\chi^2$ statistical significance (p-value) | -- | 0.000 |
| $\chi^2$ Index ($\chi^2/df$) | ≤ 3 | 1.384 |
| Incremental Fit Index (IFI) | ≥ .90 | 0.970 |
| Tucker-Lewis Index (TLI) | ≥ .90 | 0.964 |
| Comparative Fit Index (CFI) | ≥ .90 | 0.970 |
| Root mean square error of approximation (RMSEA) | ≤ .80 | 0.034 |

**Table E4. Model Fit Statistics for the Full Structural Model (See Figure 5 and Figure 6)**

| Goodness of fit statistic | Recommended value | Calculated value |
|---|---|---|
| $\chi^2$ | -- | 554.07 |
| Degrees of freedom (*df*) | -- | 392 |
| $\chi^2$ statistical significance (*p*-value) | -- | 0.000 |
| $\chi^2$ Index ($\chi^2/df$) | ≤ 3; ≤ 5 | 1.413 |
| Incremental Fit Index (IFI) | ≥ .90 | 0.967 |
| Tucker-Lewis Index (TLI) | ≥ .90 | 0.961 |
| Comparative Fit Index (CFI) | ≥ .90 | 0.967 |
| Root mean square error of approximation (RMSEA) | ≤ .60; ≤ .80 | 0.035 |

# Appendix F: Invariance

Because this study evaluated results from two separate sampling frames, responses need to be invariant between the two groups to draw conclusions regarding latent mean differences (Steenkamp & Baumgartner, 1998). Measurement invariance refers to the consistency of measurement across some specified group demarcation (Ellis, Aguirre-Urreta, Sun, & Marakas, 2008). Current information systems literature indicates the need to conduct comprehensive research that includes measurement invariance (Aguirre-Urreta & Marakas, 2012; Ellis et al., 2008). In this study, we established configural invariance and metric invariance. Configural invariance is established when the unconstrained model has good fit (Ellis et al., 2008). Therefore, configural invariance is established because the unconstrained model has good fit as indicated previously. Additionally, metric invariance is established when the measurement weights $\chi 2$ statistic is not significant (Steenkamp & Baumgartner, 1998). The results from a chi-square difference test indicate metric invariance between the groups ($df = 21$; $\chi^2 = 20.08$; $p$-value = 0.516).

# Appendix G: Common Method Variance

We checked for the systematic bias known as common method variance. Common method variance can be addressed both procedurally and statistically (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003); however, procedural (proactive) remedies are more important (Burton-Jones, 2009; H. A. Richardson, Simmering, & Sturman, 2009). Scenarios and scales developed for this study underwent extensive expert panel reviews as suggested in previous research (Petter, Straub, & Rai, 2007; Straub et al., 2004) to address these sources of common method effects and ensure realism, content validity, and face validity. After the expert panel reviews and before full data collection, a preliminary investigative procedure was conducted to reduce common method bias (Burton-Jones, 2009; Petter, Straub, & Rai, 2007; Podsakoff, MacKenzie, Lee, & Podsakoff, 2003; Straub, Boudreau, & Gefen, 2004) and further improve instrument validity and reliability. We further leveraged one of the a priori techniques recommended by Podsakoff et al. (2003) to temporally distance responses to an initial survey from those in a postsurvey. Additionally, we ensured confidentiality and anonymity of responses so the respondents could respond in true fashion and randomized the items so respondents to answer the questions in a systematic fashion (Podsakoff et al., 2003). To statistically address common method variance, we included a single unmeasured latent method factor in the analysis (Podsakoff et al., 2003). A confirmatory factor analysis was performed with and without a common method factor to determine the presence of common method variance. The results of the analysis showed no significant difference because the chi-square difference was less than 3.84 (see Table G1), providing evidence that common method variance was not a substantial concern.

**Table G1. Common Method Variance**

| | **Without method variable** | | **With method variable** | |
|---|---|---|---|---|
| **Model** | $\chi^2$ | ***df*** | $\chi^2$ | ***df*** |
| Unconstrained | 537.01 | 388 | 533.77 | 387 |
| Saturated model | .000 | 0 | .000 | 0 |
| Independence model | 5363.77 | 462 | 5363.77 | 462 |

# Appendix H: Confirmatory Factor Analysis

**Table H1. Factor Loadings and Composite Reliability**

| | Standardized factor loadings (*t*-values) | |
|---|---|---|
| | **More Frustrated** | **Less Frustrated** |
| **Negative affective absorption** | **$\rho$ = .820** | **$\rho$ = .785** |
| In general, negative emotions occupy my attention. | .74 (**) | .77 (**) |
| In general, it is hard for me to focus on something other than my negative emotions. | .82 (8.49) | .69 (7.66) |
| In general, I become deeply involved with my negative emotions. | .77 (8.36) | .75 (7.83) |
| **Distributive injustice** | **$\rho$ = .927** | **$\rho$ = .938** |
| Based on the effort I put into this exercise, the extra credit I received was unfair. | .83 (**) | .84 (**) |
| Based on the task I was assigned during this exercise, the extra credit I received was unfair. | .83 (12.44) | .91 (16.05) |
| Based on the decisions I completed during this exercise, the extra credit I received was unfair. | .87 (13.45) | .91 (15.98) |
| Based on the stress I experienced during this exercise, the extra credit I received was unfair. | .83 (12.38) | .80 (13.00) |
| Based on the training provided during the exercise, the extra credit I received was unfair. | .88 (13.59) | .87 (14.97) |
| **Interpersonal injustice** | **$\rho$ = .885** | **$\rho$ = .857** |
| During the exercise, I was not treated in a polite manner. | .88 (**) | .81 (**) |
| During the exercise, I was not treated with dignity. | .83 (12.29) | .82 (11.31) |
| During the exercise, I was not treated with respect. | .83 (12.24) | .82 (11.23) |
| **Informational injustice** | **$\rho$ = .889** | **$\rho$ = .897** |
| The video presentation did not explain this exercise thoroughly. | .90 (**) | .91 (**) |
| The video presentation explanations regarding this exercise were unreasonable. | .80 (12.22) | .83 (14.18) |
| The video presentation did not sufficiently provide detailed instructions about the exercise. | .86 (13.57) | .86 (15.41) |
| **Negative affective flow** | **$\rho$ = .886** | **$\rho$ = .879** |
| During this exercise, negative emotions occupied my attention. | .84 (**) | .74 (**) |
| During this exercise, it was hard to focus on something other than the negative emotions I experienced. | .85 (12.40) | .88 (11.35) |
| During this exercise, I became deeply involved with negative emotions. | .85 (12.57) | .81 (10.61) |
| During this exercise, I had no control over my negative emotions. | .71 (9.77) | .78 (10.17) |
| **Attitude toward specific information security policy** | **$\rho$ = .923** | **$\rho$ = .907** |
| In this exercise, it was important that I not share my password. | .80 (**) | .86 (**) |
| In this exercise, it was critical that I not share my password. | .96 (14.33) | .93 (16.53) |
| In this exercise, it was essential that I not share my password. | .88 (12.75) | .88 (15.25) |
| In this exercise, it was necessary that I not share my password. | .83 (11.83) | .69 (10.36) |
| *Notes:* ** denotes a constrained relationship to 1.00 in order for identification; $\rho$ = composite reliability | | |

**Table H2. Intercorrelation of Constructs**

| **More frustrated group** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | **Mean** | ***SD*** | **AVE** | **NAA** | **DINJ** | **IINJ** | **FINJ** | **NAF** | **SATT** |
| **NAA** | 2.61 | 0.94 | 0.604 | **(.777)** | | | | | |
| **DINJ** | 3.80 | 0.91 | 0.717 | .054 | **(.847)** | | | | |
| **IINJ** | 2.42 | 0.90 | 0.719 | .101 | .414 | **(.848)** | | | |
| **FINJ** | 3.90 | 0.98 | 0.728 | .108 | .637 | .288 | **(.853)** | | |
| **NAF** | 3.22 | 0.98 | 0.662 | .240 | .544 | .451 | .464 | **(.813)** | |
| **SATT** | 4.03 | 1.02 | 0.752 | -.149 | .178 | .002 | .112 | .255 | **(.867)** |
| **Less frustrated group** | | | | | | | | | |
| | **Mean** | ***SD*** | **AVE** | **NAA** | **DINJ** | **IINJ** | **FINJ** | **NAF** | **SATT** |
| **NAA** | 2.26 | 0.78 | 0.549 | **(.741)** | | | | | |
| **DINJ** | 2.48 | 0.96 | 0.751 | .058 | **(.866)** | | | | |
| **IINJ** | 1.70 | 0.71 | 0.666 | .069 | .501 | **(.816)** | | | |
| **FINJ** | 2.73 | 1.15 | 0.745 | .060 | .736 | .406 | **(.863)** | | |
| **NAF** | 1.81 | 0.68 | 0.647 | .231 | .578 | .660 | .536 | **(.804)** | |
| **SATT** | 4.23 | 0.89 | 0.711 | -.200 | -.094 | -.023 | -.136 | -.125 | **(.843)** |

*Notes: SD* = standard deviation; AVE = average variance extracted; values on the diagonal are the square root of AVE; password sharing was the security policy evaluated in this study

DINJ = perceived distributive injustice; PINJ = perceived procedural injustice; IINJ = perceived interpersonal injustice; FINJ = perceived informational injustice; NAA = negative affective absorption; NAF = negative affective flow; SATT = attitude toward specific information security policy; COMP = information security policy compliance

# Appendix I: Control Variables

Accounting for control variables leads to unbiased estimates by removing any confounding variables. Therefore, information was collected and controlled for the following variables: gender, age, education, ethnicity, current and expected grade, the importance of extra credit, and estimated and actual time to complete the experiment. The purpose of collecting data for these variables is to isolate the constructs of interest (Marakas, Yi, & Johnson, 1998). Current and expected grade perceptions and the importance of extra credit were collected to ensure that the results of our data were not influenced solely by the student's desire to earn a high grade. Estimated and actual time to complete the experiment were collected to determine whether emotions were impacted throughout the duration of the experiment and whether or not an individual complied.

Structural equation modeling using AMOS 22 was conducted to determine whether each of the control variables had an impact on the dependent variables in the model. In the more frustrated group, none of the control variables had an impact on the dependent variables. In the less frustrated group, however, the data indicate that gender, expected grade, the estimated time to complete the experiment, and actual time to complete the experiment influenced the dependent variables (see Table I1). Figure I-1 displays the conceptual model with the parameter estimates, p-values, and variance explained for the less frustrated group together with the control variables that had a significant impact on the model.

**Table I1. Control Variable Path Estimates**

| | | | More frustrated group | | | Less frustrated group | | |
|---|---|---|---|---|---|---|---|---|
| **Control Variable** | → | **Relationship** | **Std. Estimate** | ***t*-value** | ***p*-value** | **Std. Estimate** | ***t*-value** | ***p*-value** |
| GENDER | → | NAF | .231 | 1.706 | n.s. | .189 | 2.537 | .011 |
| GENDER | → | COMP | -.075 | -1.104 | n.s. | -.153 | -3.127 | .002 |
| AGE | → | NAF | -.005 | -0.437 | n.s. | -.006 | 0.437 | n.s. |
| AGE | → | COMP | .006 | 1.013 | n.s. | .009 | 0.833 | n.s. |
| EDU | → | NAF | -.027 | -0.217 | n.s. | .057 | 0.958 | n.s. |
| EDU | → | COMP | -.054 | -0.874 | n.s. | .016 | 0.416 | n.s. |
| GRADE | → | NAF | -.037 | -0.490 | n.s. | -.041 | -0.958 | n.s. |
| GRADE | → | COMP | .008 | 0.222 | n.s. | .015 | 0.507 | n.s. |
| EGRADE | → | NAF | -.077 | -0.493 | n.s. | .058 | 0.705 | n.s. |
| EGRADE | → | COMP | .022 | 0.279 | n.s. | -.191 | -3.711 | *** |
| EC | → | NAF | -.092 | -0.643 | n.s. | .061 | 1.193 | n.s. |
| EC | → | COMP | .059 | 0.839 | n.s. | -.001 | -0.029 | n.s. |
| ESTTIME | → | NAF | -.005 | -0.535 | n.s. | .021 | 3.369 | *** |

*Notes:* *** $p < 0.001$; EDU = education completed; GRADE = current grade; EGRADE = expected grade; EC = importance of extra credit; ESTTIME = estimated time to complete experiment; ACTTIME = actual time to complete experiment; NAF = negative affective flow; COMP = information security policy compliance

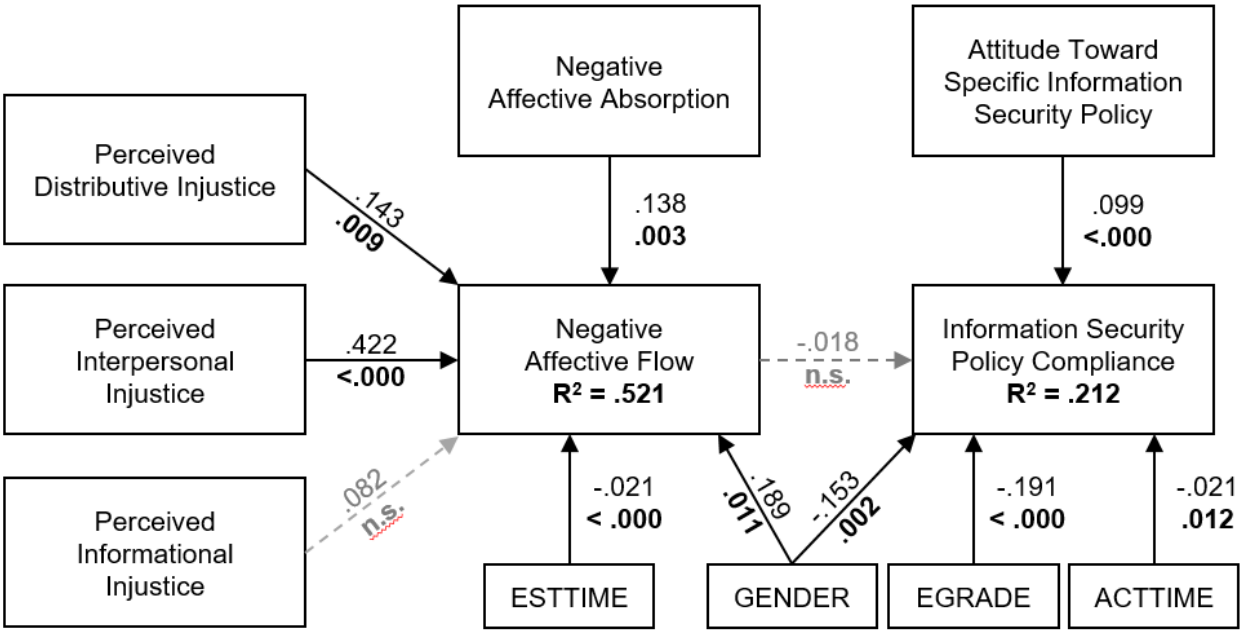


**Figure I1. Less Frustrated Model with Control Variables and Significant Path Coefficients**

Consistent with criminal injustice literature (Baron, 2007; Nakhaie, Silverman, & LaGrange, 2000; T. Peter, LaGrange, & Silverman, 2003) and when applied in the context of information security, males were more likely to experience negative affect (e.g., negative affective flow) and less likely to comply with information security policy than females. Also, individuals who expected to earn a lower grade in the class were less likely to comply with information security policy. In addition, the results demonstrate that the belief about the length for task completion was positively associated with increased negative affective flow. Finally, the actual length for task completion was negatively associated with compliance with information security policy.

Control variables achieving significance only in the less frustrated group may be due to the frustration-inducing simulated tasks leveling these differences. For example, males are more likely to experience negative emotions (see standard estimates) for negative affective flow in both groups; however, the frustrated-inducing simulated tasks were designed to induce a deep level of negative emotion. Because both males and females experience high levels of deep frustration, the difference between genders is diminished.

## About the Authors

**Dustin Ormond** is an assistant professor of business intelligence and analytics at Creighton University. His research, which primarily focuses on behavioral information security, affective computing, and deception, has appeared in *Journal of the Association for Information Systems*, *Computers & Security*, *Journal of Information Privacy and Security*, *Journal of Computer Information Systems*, among other outlets.

**Merrill Warkentin** is a William L. Giles Distinguished Professor and the James J. Rouse Endowed Professor of Information Systems at Mississippi State University. His research, primarily on the impacts of organizational, contextual, and dispositional influences on individual user security and privacy behaviors and social media behaviors, has appeared in *MIS Quarterly*, *Journal of MIS*, *Journal of the Association for Information Systems*, *European Journal of Information Systems*, *Information Systems Journal*, *Information & Management*, and *Decision Sciences*, among other outlets. He has published seven books and over 300 manuscripts, including over 90 peer-reviewed scientific journal articles. He was named a 2018 ACM Distinguished Scientist. He has served in editorial roles for *MIS Quarterly*, *Information Systems Research*, *European Journal of Information Systems*, *Decision Sciences*, and other journals. He is the EIC of the *Journal of Intellectual Capital* and is currently on the editorial boards of *Journal of the Association for Information Systems* and *Information & Management*. His work has been funded by NATO, NSF, NSA, DoD, Homeland Security, IBM, and others. He was the 2016 AMCIS Program co-chair.

**Robert E. Crossler** is an associate professor of information systems in the Carson College of Business at Washington State University. His research focuses on the factors that affect the security and privacy decisions individuals make. He has published in leading MIS journals, including *MIS Quarterly*, *Information Systems Research*, *Journal of Management Information Systems*, *Journal of the Association for Information Systems*, *European Journal of Information Systems*, *Information Systems Journal*, and *Journal of Strategic Information Systems*. He was named an AIS Distinguished Member–Cum Laude in 2019. He is the president of the AIS Special Interest Group on Information Security and Privacy (SIGSEC). He received the 2013 INFORMS Information Systems Society Design Science Award for his information privacy work, his paper in *The DATA BASE for Advances in Information Systems* was recognized as the journal's best paper in 2014, and he received the *Journal of Information Systems* inaugural Best Paper Award in 2017.