2021

An Empirical Examination of the Impact of Organizational Injustice and Negative Affect on Attitude and Non-Compliance with Information Security Policy

Celestine Kemah
Nova Southeastern University, celestokemah@yahoo.com

An Empirical Examination of the Impact of Organizational Injustice and Negative Affect on Attitude and Non-Compliance with Information Security Policy

by

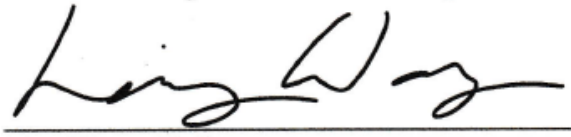
Celestine Kemah

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

Nova Southeastern University
College of Computing and Engineering

2021

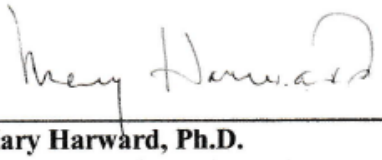
We hereby certify that this dissertation, submitted by Celestine Kemah conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.



4/28/21

Ling Wang, Ph.D
Chairperson of Dissertation Committee

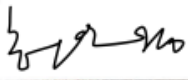
Date



4.28.21

Mary Harward, Ph.D.
Dissertation Committee Member

Date

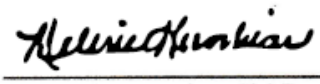


4/28/2021

Inkyoung Hur, Ph.D.
Dissertation Committee Member

Date

Approved:



4/28/2021

Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

Date

College of Computing and Engineering
Nova Southeastern University

2021

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

An Empirical Examination of the Impact of Organizational Injustice and Negative Affect on Attitude and Non-Compliance with Information Security Policy

by
Celestine Kemah
April 2021

Employees' non-compliance with Information Security (IS) policies is an important socio-organizational issue that represents a serious threat to the effective management of information security programs in organizations. Prior studies have demonstrated that information security policy (ISP) violation in the workplace is a common significant problem in organizations. Some of these studies have earmarked the importance of this problem by drawing upon cognitive processes to explain compliance with information security policies, while others have focused solely on factors related to non-compliance behavior, one of which is affect. Despite the findings from these studies, there is a dearth of extant literature that integrates both affective and cognitive theories that shed light on a more holistic understanding of information security non-compliance behaviors. This research developed a theoretical model of the relationship between negative affect and cognitive processes and their influence on employees' ISP non-compliance at the workplace. Cognitive processes provide a significant foundation in understanding why employees show non-compliance behavior with ISPs and rules at the workplace. However, they do not completely explain the motivations behind the deviant employee's non-compliance behavior. This research examined how the relationships between organizational injustice frameworks and negative affect influence attitude, which, in turn, influences behaviors that can be used to understand ISP non-compliance. Extant literature has explored theories like neutralization, deterrence, theory of planned behavior, rational choice theory, affective events theory, and work-related events as an outcome of neutralization, and organizational injustice, to explain cognitive reactions.

The research model was empirically tested using the data collected from 115 participants who participated in a scenario-based survey. The results showed that negative affect has a significantly positive impact on employees' attitude and ISP non-compliance behavior. Distributive, informational and interpersonal injustices were also found to influence ISP non-compliance in a significant but negative direction. The study contributes to both theory for IS research and practice for organizational management of security policies.

Acknowledgments

"It is not the answer that enlightens, but the question"
Eugene Ionesco

Thanks and Glory unto God for endearing in me the strength and resources to undertake this great and successful journey. This work would not have been completed without His grace and blessings.

Immense thanks and gratitude to my committee chair, Dr. Ling Wang. I cannot express how grateful I am for her endless support and direction. Her commitment, patience and dedication in the face of obstacles were very invaluable to me completing this important milestone. She is an embodiment of what every doctoral student wishes to have as mentor. I would also like to thank Dr. Mary Harward and Dr. Inkyoung Hur for their valuable feedback and suggestions. Your detailed critique helped shape this dissertation report. A special thanks to you all.

Thank you, Mercy Kemah, for your love, endless sacrifices and support even in difficult times throughout the years. Your continued belief has been a source of encouragement and drive to me throughout this journey. I appreciate you putting the kids to bed without me. To my $2A^2$: Aiden, Avery, Arielle-Estelle, and Adrian, thank you for cheering me up and believing that those missed play dates were not in vain. And to mom and dad, thank you for giving me a foundation for a better future.

Finally, to my friends, colleagues and everyone who cheered and encouraged me throughout this journey, may God bless you all!

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

Insider threat to an organizations' information security is still a growing concern despite extensive and frequent security education, training, and awareness (SETA) programs put in place by these organizations. Results from the "State of cybersecurity implications for 2016" survey conducted by the Information Systems Audit and Control Association (ISACA) showed that 64% of malicious activity emanated from insider damage (ISACA, 2019). In a similar line of study, the "2018 IBM X-Force Threat Intelligence Index" reported that non-malicious insiders who represent one of the most common forms of threat actors that frequently violate enterprise security systems cause 60% of unethical cyber violation (Henry, 2018). Findings from numerous information systems security studies show that information security violations caused by the unethical actions of disgruntled employees and other insiders with legitimate access rights to information systems pose an even greater financial burden and the costliest risks to an organization (Cole, 2015; PwC, 2019). Given that employees with legitimate access privileges have a good knowledge of organizational processes (Willison & Warkentin, 2013), the question becomes therefore how to mitigate insider threats posed by these employees.

Information security policies represent a set of formalized guidelines and procedures, including technical controls, established by organizations to help ensure information security while using information systems to perform their jobs (Bulgurcu et al., 2010). These policies define the security requirements employees need to follow in order to maintain the security objectives (i.e. integrity, accountability, availability, and confidentiality) of an organization (Vroom & von Solms, 2004). They also specify the proper uses and standards of an organization's information technology resources and assign responsibilities for a proper management and response during security crisis (Cram et al., 2017; D'Arcy & Lowry, 2019; Lowry & Moody, 2015).

Information systems and security studies postulate that employees deliberately and routinely undermine and circumvent an organization's information security policies even after undergoing extensive SETA, and some underestimate the security risks associated with the unethical violation of these policies (Dell, 2015; Li et al., 2019; Ng & Xu, 2007). Meanwhile, some studies focus primarily on the role of employees' cognitive processes in information security policy compliance, drawing from rationality-based theories like rational choice theory (Bulgurcu et al., 2010; D'Arcy & Lowry, 2019), protection motivation theory and theory of planned behavior (Lebek et al, 2014; Sommestad et al., 2014). These theories emphasize on cognitive processes and their influence on compliance with ISPs. Even though these studies have made great strides in contributing to the IS literature, they have most often ignored the significant role of affect which is an important element in the rational decision-making process. Eagleman (2011) noted, "most of what we do and think and feel is not under our conscious control…our brains run mostly on autopilot...almost the entirety of what happens in [our] mental life is

not under [our] conscious control" (pp. 4-7). Because cognition cannot be controlled completely, affect can provide very significant insight into understanding ISP non-compliance behavior because affective processes have been influential to cognitive processes (Russell, 2003).

Problem Statement

Employees' compliance with information systems security policy is an important socio-organizational topic (Boss & Kirsch, 2007). It represents a key information security problem for organizations and poses major concerns for information security management (Bulgurcu et al., 2010). Previous research has demonstrated that information security policy violation in the workplace is a commonly significant problem in organizations (Chen et al., 2013; Hu et al., 2011). These studies have primarily drawn upon cognition and its role in compliance with information security policies (Lerner & Keltner, 2000), while others have focused on other factors related to noncompliance behavior, one of which is affect (Samnani et al., 2014; Zhang, 2013).

Cognitive processes are very significant in providing an understanding as to why employees do not comply with policies and procedures. However, they do not completely explain the abusive insider's motivations. Affect is a necessary and important regimen of rational decision-making (Djamasbi et al., 2010) and often influences some cognitive processes such as judgments and decisions (Lerner & Keltner, 2000).

Numerous information security studies have earmarked the importance of cognitive processes to IS security compliance behavior (Herath & Rao, 2009; Johnson & Warkentin, 2010; Siponen & Vance, 2010). Others have examined the decision to disclose information online as a result of affective and cognitive reasoning of online users

using the privacy calculus framework (Kehr et al., 2015; Li et al., 2011; Wagner et al., 2018). These authors concluded that situational factors like emotions and fairness (affect) influence individuals' privacy beliefs and decisions. Notwithstanding, there is a dearth of extant literature that integrates both affective and cognitive theories that could help shed more light on a more holistic understanding of information security compliance behaviors. These studies provide great insight into understanding why employees violate IS security policies and procedures, but they do not provide any rationale of the abusive act carried out by the insider.

Dissertation Goal

There is not enough systematic, theory driven extant information systems (IS) literature that investigated the impact of affect and cognition on information security policy (ISP) violations. Affect may be more important in understanding ISP compliance behaviors considering that cognition may not be completely controlled. By integrating these two constructs, affect and cognition, this research evaluated the impact of affective and cognitive processes toward compliance with information security policies. Specifically, this research explored the impact of negative affect on cognitive processes in the context of attitude toward and compliance with ISPs. Emotions influence all forms of behavior and this influence is proportionate to the level of emotions. Additionally, strong emotions may be a recipe for an individual’s deviant behavior contrary to their self-interests (Willison & Warkentin, 2013) due to their deep involvement with their emotions. Furthermore, individuals that perceive they have been treated unfairly by their organization are likely to experience strong emotions, as fairness perceptions directly or

indirectly influence people's emotions. This rationale led to the primary research questions:

RQ1: Does negative affect (emotions) influence an individual's attitude and information security policy non-compliance behaviors?

RQ2: Do perceptions of injustice influence an individual's attitude and information security policy non-compliance behavior?

Specifically, this study addressed this gap by seeking to identify the nomological network of cognitive and affective constructs and their interrelationships relevant to understanding employees' unethical use and violation of ISPs.

Relevance and Significance

A major challenge for organizations is encouraging employees to comply with mandated information security policies, procedures and guidelines (D'Arcy & Greene, 2014). While security awareness is accepted as a means for increasing IS security compliance within an organization, the actual impact of both cognitive and affective behavior within the organization's end-users' intention to IS security compliance has not been clearly analyzed. In addition, the theories that explore cognitive reasoning such as theory of planned behavior, rational choice theory, and deterrence theory do not completely address IS policy abuse-related issues. Willison and Warkentin (2013) argued that pre-kinetic events like organizational injustice, neutralization, expressive motive or disgruntlement may be reasons why employees violate IS policies. Through evaluating both affective processes and cognitive processes in information security decision-making, we may have a more holistic understanding of compliance with organizational security policies.

Gonzalez and Sawicka (2002) described the human factor as the "Achilles heel" of information systems security. In an attempt to draft solutions for issues that emanate

from security policy violations and unauthorized systems breaches, the human factor must be taken into account because end-users will intentionally decide to circumvent security policies by lowering their value for systems security (Adams & Sasse, 1999). Prior studies on user behavior have concluded that employees make poor ISP choices for different reasons. Some of these reasons may be the lack of adequate training, absence of perception of a threat for violating security policies and procedures or a poor IS security culture of the organization (Hassanzadey et al., 2014; Hedstrom et al., 2011; Ifinedo, 2012; Renaud, 2011; Siponen et al., 2010; Siponen et al., 2014). Technical employees also present some issues with the use and access to their security service accounts. For example, the use of their service accounts on their personal computers or the sharing of credentials with other system users may render the system vulnerable to attack. While some authors have provided an account of the importance of human factor in ISP compliance, others have concluded that statistically, there is no correlation between ISP adoption and the prevention of ISP non-compliance and security breaches (Doherty & Fulford, 2005). Having an IS policy does not necessarily translate into prevention of ISP non-compliance.

This research offered additional insight into information systems security literature by first looking at how studying affective theories, together with cognitive theories, grants a holistic understanding regarding compliance attitudes and behavior. Secondly, exploring affective theories as a critical and necessary antecedent to understanding why deterrence mechanisms oftentimes fail and finally, capturing actual compliance behavior, rather than compliance intention, provided a richer and more meaningful findings regarding information security behaviors. This study also

contributed to theory as a unique measure of compliance with ISP by integrating constructs from rationality-based theories and concepts like rational choice theory, deterrence theory, theory of planned behavior and organizational injustice with affective and cognitive factors. This contribution diverges from prior studies that conceptualized employees' compliance with ISP from a strictly stable and reason-based approach. Practically, this study identified factors that influence affective reactions, and proposed avenues for organizations to develop strategies aimed at reducing non-compliance behavior.

Barriers and Issues

The determination of employees' ISP non-compliance behavior was based primarily on the definition of ISP non-compliance behavior and what methodology can be used to measure behavior. The human factor in ISP compliance studies in itself is a complex concept that renders the measurement of actual behavior difficult because multiple factors influence different types of behavior. For example, the severity level of ISP violation for a student on campus may be different from an employee on the same campus resulting to different security behavior. This is because the employee find the idea of ISP violation more catastrophic to them professionally than the student.

Attracting a valid number of participants in a web-based survey, the willingness of the participants to take the survey, and the generalizability of the findings can be daunting tasks. This study employed a web-based survey to collect data from participants in a college campus. Using a web-based survey is advantageous and for the purpose of this study, it will present the participants the option to take the survey at their own comfort. Another issue was the racial distribution of the participant population. The

intended participant pool is predominantly Hispanic and this raises issues with the generalizability of the research findings to other races.

Assumptions, Limitations, and Delimitations

Assumption is "what the researcher accepts as true without a concrete proof" (Ellis & Levy, 2009, p. 331). This study assumed that the survey participants will express sincerity when they respond to the survey. Secondly, this study assumed that each survey participant has violated the ISP of the institution at least once during his or her time on campus. To assess the validity and reliability of the constructs, a combined statistical method using confirmatory factor analysis (CFA), structural equation modeling (SEM) and Cronbach's Alpha was be leveraged. Subsequently, the assumptions and limitations that come with these approaches were applied to this study. Some of these assumptions include a reasonable size of survey participants, normal distribution of endogenous variables, identification of correlations or covariance in the model and model causality and specification (Kline, 2012).

The study of actual behavior in security is challenging (Vroom & von Solms, 2004). Behavior cannot be measured directly, and the primary source of data was self-reported data, subjecting the data to common method bias. Also, because the data was collected through an online survey, Rea and Parker (2014) stated that online surveys have a self-selection bias. Only participants with knowledge and idea of the subject matter were assumed to fully complete the survey, affecting the generalizability of the results.

One of the requirements for survey data collection is to keep the survey questions in scope and simple for respondents to understand. This may reduce the potential reluctance that participants may have in completing the study survey. As stated by

Houston and Tran (2001) “the problem facing researchers is how to encourage participants to respond, and then to provide a truthful response in surveys” (p. 70). The survey instrument was therefore developed following guidelines provided by Rea and Parker (2014).

Definition of Key Terms

A selection of key definitions has been provided below for the reader and researcher to have a consistent understanding of the concepts and discussions that follow in this research work.

Information security - Pfleeger and Pfleeger (2003) defined information security as “computer security attempts to ensure the confidentiality, integrity, and availability of computing systems’ components” (p. 29). Additionally, Whitman and Mattord (2009) defined information security as “the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information” (p. 8). Within the concept of information security are three critical elements of confidentiality, integrity and availability of information (CIA) which are considered the industry standard. Any improper maintenance of these three elements in information security may lead to the unauthorized release of sensitive information that may pose a potential threat to the organization.

Information security policy - Höne and Eloff (2002) defined information security policy as “a direction giving document for information security within an organization” (p. 402). Additionally, Bulgurcu et al., (2010) and Steinbart et al., (2016) defined information security policy as a set of established guidelines, roles and responsibilities that details the processes and procedures, including technical controls that employees need to follow in

order to help achieve the information security objectives of the organization. It is a process and procedure document that demonstrates commitment by top management in support of organization information security.

Information security policy (ISP) violation - Hu et al. (2011) defined information security policy violation as "any act by an employee using computers that is against the established rules and policies of an organization for personal gains" (p. 54). Accordingly, policy violations are not only restricted to the illicit access to data systems and the transfer of confidential information to third party, but also on any unauthorized activities on the organization IT systems that pose a threat to the organization.

Information security compliant behavior - The set of main information security activities that need to be performed by end-users in order to maintain and sustain organizational information security as established in the information security policy and procedures (Chan, et al., 2005). Demonstrating an information security compliance or ethical behavior requires that employees not only have the necessary skills to carry out a particular task, but also be motivated by the current organizational information security climate.

Summary

Employees' noncompliance with ISP is a valuable socio-organizational topic that presents an important information security threat to organizations. Unfortunately, employees have been proven the weakest link in attempts by the organization to achieve an effective management of the information security program. Prior studies have drawn upon cognitive processes while others have focused primarily on affective processes in an attempt to explain employees' unethical use of security policies and how these two

constructs influence employees' noncompliance with information security policies. Notwithstanding, the dearth of extant literature that integrates both affective and cognitive theories that could help shed more light on a more holistic understanding of information security compliance behaviors presents an opportunity for this study. These studies provide great insight into understanding why employees violate ISPs and procedures, but they do not provide any rationale of the abusive act carried out by the insider.

Events happening because of employees' unethical behavior towards ISPs and rules are increasingly becoming rampant, in great variety, and severity of threat. As a solution to this threat, through evaluating both affective processes and cognitive processes in information security decision-making, this study is designed to provide a more holistic understanding pertaining to compliance with organizational security policies. This study is organized using a five-chapter model. **Chapter 1** of this study presents the problem statement and research goal. The chapter also discusses the underlying theories that explain the cognitive and affective reasoning of individuals including a section on the relevance and significance of the research problem. The chapter concludes with definition of the key terms relevant to the current study. **Chapter 2** provided details on the literature review of key theories, constructs and topic areas that are used to establish the hypotheses and build the theoretical foundation for the research model. **Chapter 3** explained the methodology, which includes the study design, instrument development and measurement, data collection, and analysis with validation of the empirical approach. **Chapter 4** dwelled on data analysis and results with

discussion and presentation of these findings. Finally, **Chapter 5** discussed the conclusions, theoretical and practical implications and recommendations for future work.

Chapter 2

Review of the Literature

Overview

This chapter reviewed the relevant literature with the intention to provide more context and theoretical foundation as they relate to the topic of this research. Prior literature has described how cognitive processes influence an individual's rational decision-making and inclination to violate information security policies (ISPs) especially at the work place. These studies even though have made immense contributions to the information systems security literature, they are however not completely comprehensive because *affect*, an important factor in rational decision-making is more often overlooked. There is nevertheless sufficient literature that was explored to support the purpose of this research, which is to examine the combined influence of cognitive processes and *affect* on employees' misuse and non-compliance with IS security policies. There is an increasing need for efficient and more reliable information security measures that can be used to curb the growing cybercrime phenomenon (Bauer & van Eeten, 2009). According to Schultz (2005), there is a lack of sufficient experts with enough knowledge on how to deal with information systems issues caused by human factors, calling for more scholarly research that explore human behavior. Schultz (2005) further indicated that little emphasis is placed on the significance of human factors during the development and implementation of information security program.

Findings from the 2013 U. S. State of Cybercrime Survey conducted by the CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper (PwC) showed that the cost of non-malicious insider incidents outweighs the cost of damage caused by an external intruder (CSO Magazine et al., 2013). The cost of employee deviant behaviors on security systems may prove to be devastating with associated financial and reputational losses to the organization.

The remainder of this chapter is organized as follows. First, the chapter examines the underlying theories, which I use to build the model. Next, it discusses employee information security policy (ISP) compliance and the organizational justice frameworks that are associate with deviant behavior. Then it defines and discusses the role of affect and cognition in rational decision making with regards to ISP compliance behavior. The chapter concludes with the theory development and a discussion of the constructs' relationships and the proposed conceptual model and hypotheses to be tested.

Theoretical Foundation

A conceptual framework is a popular method in research that is used to explain attitudes and behaviors because it serves as part of an inductive process to improve upon the existing body of knowledge (Zivkovic, 2012). A conceptual framework includes concepts that define and establish relationships between certain variables (Abukhalifeh & Som, 2012) and uses constructs from a review of prior literature to support a study (Bansal & Corley, 2012).

The phenomenon of ISP misuse/deviant behavior can be evaluated based on competing cognitive and affective processes. Willison and Warkentin (2013) indicated

that reasons for abuse are a result of pre-kinetic events (e.g. neutralization, organizational injustice, disgruntlement, or expressive motives). These pre-kinetic events may influence cognitive processes. The role of cognition in employees' ISP compliance behavior is very significant. Providing an understanding of what cognitive processes influence ISP unethical behavior is therefore compelling to establish a foundation for this research. Because the framework for this study revolves around cognitive and rationality-based behavioral theories like neutralization, theory of planned behavior, deterrence, a review of the ISP compliance studies that describe and define individual cognitive processes as rooted in these theories is conducted in the sections that follow.

Neutralization Theory

The foundations to explain an individual's illicit/deviant behavior have been built upon the prominent Neutralization theory (Sykes & Matza, 1957). Neutralization can be defined as "a method whereby a person renders behavioral norms inoperative, thereby freeing himself to engage in behavior which would be otherwise considered deviant" (Rogers & Buffalo, 1974, p. 318). The theory states that individuals make rational decisions about their behavior by justifying their actions in order to subjugate the consequences (Sykes & Matza, 1957). Neutralization theory has been used by many scholars to study end users' ISP misuse and deviant behaviors (e.g., Barlow et al., 2013; Siponen et al., 2012). Siponen and Vance (2010) and Teh et al. (2015) demonstrated that neutralization is a significant predictor of ISP deviant behavior. These authors argued that neutralization positively affects intention to violate ISP more than sanctions could be used to deter misuse. For example, individuals carrying out unethical behavior justify their actions on grounds that there will not be any negative outcome from that behavior.

Consequently, the individual, on the premise that their actions are not criminal, feels no guilt. Neutralization therefore offers avenues where individuals render existing processes and procedures nonfunctional through justification and rationalization of their deviant behavior (Rogers & Buffalo, 1974).

Sykes and Matza (1957) used five cognitive techniques to explain the concept of neutralization: *denial of injury, denial of victim, denial of responsibility, condemnation of the condemners, and appeal to higher loyalties*. These techniques serve as the original five neutralization techniques. Klockars (1974) later suggested *metaphor of the ledger* as another neutralization technique, and Minor (1981) included *defense of necessity* in the neutralization taxonomy. Willison and Warkentin (2013) in a more recent study suggested 17 different techniques of neutralization that individuals use. A review of IS research provides a better understanding of how employees evoke these techniques of neutralization.

The *condemnation of the condemners'* technique as put forth by Sykes and Matza (1957) states that individuals will draw attention away from their unethical or undesirable behavior to focus on the actions and motives of employees condemning their actions. In the context of this study, employees neutralize their unethical ISP behavior through the *condemnation of the condemners* if they claim that the policy makes no sense (Siponen & Vance, 2010). Individuals vary in the way they accept responsibility for their actions especially in the workplace. The *denial of responsibility* explains that violators will justify their actions, deny responsibility of their actions, and avoid criticism from peers (Siponen et al., 2012). Results from Puhakainen and Siponen (2010) showed that

employees excused themselves of the responsibility to follow the company's secure email usage policy by the rationalized argument that the policy was not clear.

Defense of necessity refers to a situation where individuals do not have to be guilty when taking actions where necessary (Minor, 1981). Puhakainen and Siponen (2010) also exemplified *defense of necessity* technique by describing how employees opened up about their unusual ISPs deviant behaviors because certain requirements in the policies affect their productivity. Employees use *denial of injury* to defend their delinquent conduct or misuse behavior by claiming that the behavior does not cause harm to others (Thurman, 1984). *Appeal to higher loyalties* as put forth by Rogers and Buffalo (1974) is a technique in which when a person is in a situation of dilemma, he is forced to choose between two options of behavior: (1) in defiance of societal norms and (2) in breach of norms of a smaller group of population like friends. For example, Siponen and Iivari (2006) found that employees would be defiant to ISPs if they knew their action would benefit their colleagues.

When offenders rationalize their law-abiding acts with their criminal behaviors (Minor, 1981; Siponen et al., 2012), the *metaphor of the ledger* is used. For example, an employee can justify his or her deviant behavior by saying that "I have an important research project to be done for the organization so I need to search on any website for information" or "our project will not be completed on time if I don't share my password". In the IS context, employees may justify or rationalize their ISP unethical conduct to compensate for their compliance behavior (Siponen & Vance, 2010). Lim (2002) found that employees use the metaphor of the ledger to justify their cyberloafing behavior. Criminal offenders have also used other techniques of neutralization to justify their

deviant behavior. These techniques have been subsequently identified by IS researchers and are presented in Table 1. In addition, these techniques have been widely applied in criminology in order to address a variety of criminal or deviant behavior (Maruna & Copes, 2005). These criminal behaviors are summarized in Table 1. Considering that end users always rationalize or justify their non-compliance with ISP, it is important to understand the antecedents and factors that influence the decision to engage in deviant behavior.

Table 1

Neutralization Techniques as Applied in IS Studies

Technique	Definition	Example	Source
Denial of injury	Offenders claim their perceive actions have no harmful effects to people around them.	My actions don't hurt anybody.	Thurman, 1984; Sykes & Matza (1957)
Denial of the Victim	Perception of offenders that injury is the right form of retaliation.	They saw it coming.	Sykes & Matza (1957); Henry (2009)
Denial of responsibility	Offenders see their lack of responsibility for their deviant behavior justifiable because they think they are victims of the circumstance.	It was not intended	Sykes & Matza (1957); Siponen et al., 2012
Condemnation of the condemners	Offenders will draw attention away from their unethical behavior to focus on the actions of employees who oppose their actions.	A corrupt organization	Sykes & Matza (1957); Siponen & Vance (2010)
Appeal to higher loyalties	Offenders justify their misconduct as a moral value compared to those who disapprove of their behavior.	I did it for the team	Siponen & Iivari (2006)
Metaphor of the ledger	Offenders justify their deviant behavior as a compensation for their good deeds.	I am a hard-working employee	Henry (2009); Siponen & Vance (2010)

Table 1 (continued)

Neutralization Techniques as Applied in IS Studies

Defense of necessity	Offenders are not guilty when engaging in deviant behavior.	I had no other choice.	Minor, 1981; Puhakainen & Siponen (2010)

Table 2

Criminal Behaviors Employing Techniques of Neutralization

Behavior	Definition	Source
White-collar crime	Non-violent and financially motivated deviant decision-making behaviors that occur within the workplace.	Piquero et al. (2005)
Domestic violence	Deviant or aggressive and abusive behavior that typically involves an abuser within the home.	Dutton (1986)
Shoplifting	Taking property or merchandise from a place of business or store without permission.	Cromwell & Thurman (2003)
Tax evasion	The purposeful or deliberate act of under-reporting income or failure to pay taxes.	Thurman (1984)
Car theft	The criminal behavior of attempting to steal or break into a car without permission.	Copes (2003)

Rational Choice Theory

Rational choice theory (Becker, 1974) posits that during a decision-making process, individuals first make different alternative decisions and then consider the alternative decision with the best possible outcome. Individuals therefore make an assessment of the cost and benefits of each alternative in order to come up with the best option. Therefore, its focus is on evaluation of the effects of engaging in alternative courses of action (McCarthy, 2002; Paternoster & Pogarsky, 2009). In the context of this study, these alternative courses of actions are employees' compliance and noncompliance to ISPs. One stipulation of ISPs is the roles and responsibilities of employees in

protecting the information and technology assets of the organization. Thus, when an employee evaluates his or her compliance or noncompliance with ISP he considers the cost and benefit associated with his compliant or noncompliant behavior (Bulgurcu et al., 2010). In line with the rational choice theory, beliefs about the outcome of compliance behavior can be broken down into three categories: (1) perceived benefit of compliance (the expected benefits of ISP compliance to an employee), (2) perceived cost of compliance (the expected undesired consequences of compliance to ISPs), and (3) perceived cost of noncompliance (the expected undesired consequences of noncompliance to ISPs).

Most ISP compliance studies grounded in rational choice theory have ignored this important point, which lends credence to the inclusion of affect in ISP compliance/non-compliance studies. Rational choice theory explains that before engaging in deviant behavior, offenders weigh the costs and benefits of such behavior and try to maximize the benefits against the costs before engaging (D'Arcy & Herath, 2011; Li et al., 2010). Aytes and Connolly (2004) used the rational choice model to explain why university students engage in risky computing behavior such as opening email attachments without checking for viruses, failing to back up files, and disclosing passwords. They found that respondents continued to practice unsafe computing even when they were fairly knowledgeable on safe computing practices.

The decision to act in an offending manner becomes therefore a function of perceived cost and perceived benefits of the criminal behavior (Hu et al., 2011). Rational choice theory has been very important in explaining human behavior. But it has equally been heavily criticized because decisions are subjective and the costs and benefits of

these decisions vary (Paternoster & Pogarsky, 2009; Paternoster & Simpson, 1996). Therefore, people will make decisions based on their preferences. One key assumption of rational choice theory is that of *bounded rationality.* With bounded rationality, individuals make incomplete rational decisions due to the difficulties that would circumvent their ability to anticipate or calculate all relevant alternatives (Elster, 1986). This implies rationality is based on perceptions and not actual costs and benefits (McCarthy, 2002). Affective influences therefore will force individuals to make rational decisions about the same behavior that may vary over time, an assumption that is consistent with bounded rationality. For the purpose of this study, this assumption was adopted and used to account for employees' affective state from one moment to the other. This fits the concept of affective rationality as described by Finucane et al., (2000) and Slovic et al., (2004) in their decision-making literature.

Deterrence Theory

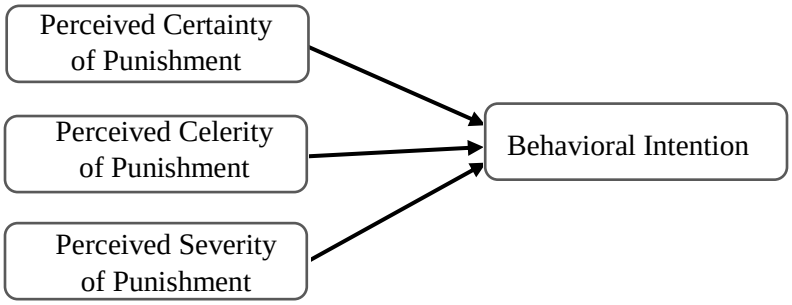
With the array of studies conducted on insider computer abuse, an area that has seen much focus and attention in IS research is deterrence (Willison et al., 2018). Deterring employees from the unethical use or violation of ISP follows prevention efforts that are designed to halt the ISP non-compliant behavior (Straub & Welke, 1998; Willison & Warkentin, 2013). The use of threat of sanctions by organizations to stop a behavior is therefore at the center of deterrence.

Deterrence theory has been used by organizations to explore ways to increase the costs of ISP non-compliant behavior in an attempt to divert or deter such behavior. Originally applied in criminology studies, deterrence theory has been primarily applied by IS researchers to explain dissuasion from non-compliant and deviant behavior. The

central tenet of deterrence theory is that potential wrongdoers exert a sufficiently rational influence through their understanding of the effects of criminal conducts (Straub & Welke, 1998). Accordingly, the theory posits that individuals weigh the costs and benefits before engaging in deviant behavior, and they chose to violate if the benefits outweigh the costs. The theory proposes three components: certainty of sanction, severity of sanction and celerity of sanction. Thus, if an individual comes to the conclusion that there is a high chance of being caught (certainty of sanction) and the punishment is severe (severity of sanction), they will not engage in defiant behavior (Siponen & Vance, 2010).

Figure 1

Deterrence Theory (Straub & Welke, 1998)

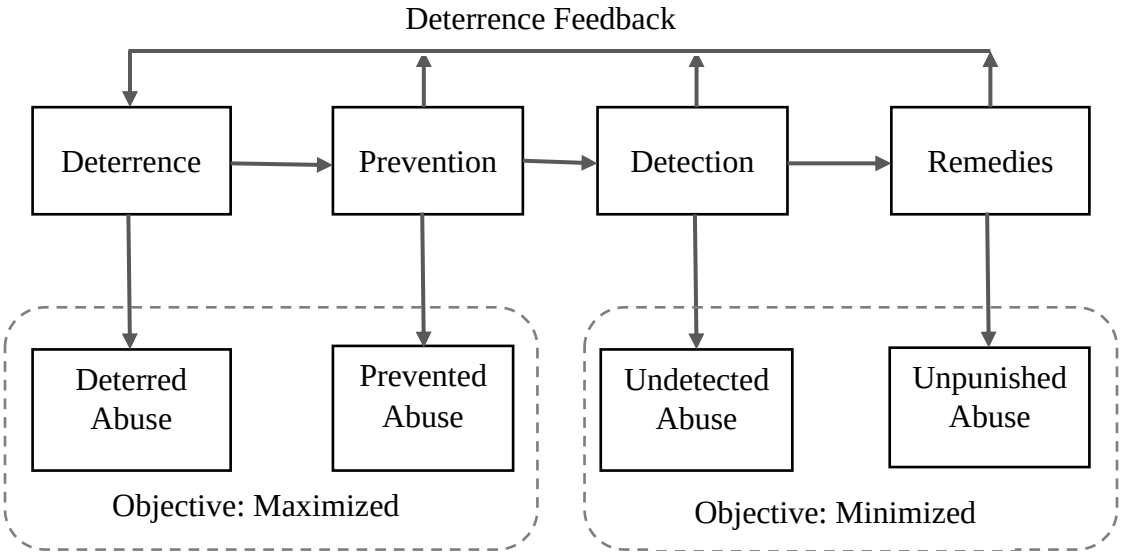


The security action cycle put forth by Straub and Welke (1998) suggests four stages of evaluation in order to achieve an effective information security management system: deterrence, prevention, detection, remedies (see Figure 2). The first stage of the cycle involves deterrence where organizations implement dissuasive measures like sanctions in order to dissuade employees from non-compliant and misuse behavior. When sanctions prove not successful, preventive measures like access controls are put in place to prevent non-compliance. When prevention fails, systems are put in place to detect any threat from intrusion. The final stage involves remediation, should detection fail. This

includes backup and restore systems where critical data and other important information can be restored. In order to effectively manage the security systems using these four stages, organizations can create countermeasure systems that give them the best possible options to use during an abuse (Straub & Welke, 1998).

Figure 2

Security Action Cycle (Straub & Welke, 1998)



The first stage of this cycle is very critical in that if violators are deterred from violating the ISPs, other stages of the security cycle would not be relevant. However, this has never been the case. Lessons learned from the four stages during a threat situation can be applied as a feedback in order to enhance the deterrence process.

Informal sanctions, formal sanctions and shame have been used by most deterrence studies to explain deviant behavior and deter ISP misuse (Nagin & Pogarsky, 2001; Siponen & Vance, 2010). Informal sanctions are sanctions impinged on an individual by peers, friends and family or reference group for a given undesired action (Anderson, et al., 1977). Formal sanctions Shame represents a self-imposed feeling of

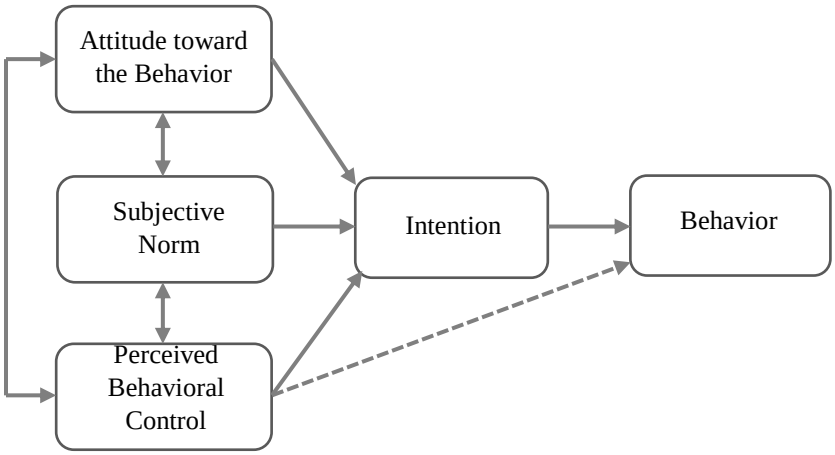
humiliation or embarrassment caused by one's conscious undesirable behavior (Paternoster & Simpson, 1996; Siponen & Vance, 2010). These constructs are more closely related in their deterrent influence on employees' ISP abuse and/or non-compliance.

Theory of Planned Behavior

One of the widely used models in IS research that emphasize decision-making is the theory of planned behavior (Ajzen, 1991). The theory posits that individual's intentions lead to behavior (Ajzen, 1991; Fishbein & Ajzen, 1975). At the center of TPB is the need to predict intentions. For the purpose of this study, that implicit presumption would be ISP non-compliant behavior. Intention represents an individual's willingness to express a certain type of behavior. Empirical studies have found a strong relationship between behavior and intention especially given a shorter time lapse between the intended behavior and actual behavior (Ajzen, 2011). In IS research, this strong relationship has also been found to be consistent (Lebek et al., 2014; Siponen et al., 2014). Three major factors: attitude, subjective norm and perceived behavioral control influence an individual's intended behavior (Newton et al., 2013).

Figure 3

Theory of Planned Behavior (Ajzen, 1991)



Attitude represents an individual's feelings about a behavior. It can be defined as the assessment of the potential outcome of showing a particular behavior (Safa et al., 2015). While attitude can be positive or negative, it can also be explicit or implicit. Implicit attitude affects our beliefs and behavior unconsciously. In explicit attitude, the surrounding environment influences an individual's behaviors and beliefs consciously (Albrechtsen & Hovden, 2010). Subjective norm is *"an employee's perceived social pressure[s] about compliance with the requirements of the ISP caused by behavioral expectations of such important referents as executives, colleagues, and managers"* (Bulgurcu et al., 2010, p. 529). Perceived behavioral control represent the assessment of the difficulties surrounding the performance of certain behavior based on past experience and potential obstacles. Ifinedo (2014) concluded that attitude, subjective norms, and perceived behavioral control influence employees' ISP compliance intention in the organization. The theory of planned behavior is further extended to include constructs like behavioral, normative, and control beliefs and their respective relationships to attitude, subjective norms, and perceived behavioral control.

However, the most ostensibly neglected factors in TPB are affect and emotions (Rapaport & Orbell, 2000; Richard et al., 1998; Wolff et al., 2011). This is in part because of a mistaken perception of the theory's assumption that people are rational and are not affected by emotions, and also on the methodology that is being applied by scholars during operationalization of the theory's constructs (Ajzen, 2011).

Table 3

Definition of Constructs Taken from Theory of Planned Behavior

Construct	Definition
Subjective norms	"An employee's perceived social pressure[s] about compliance with the requirements of the ISP caused by behavioural expectations of such important referents as executives, colleagues, and managers" (Bulgurcu et al., 2010, p. 529).
Compliance self-efficacy	"An employee's judgement of personal skills, knowledge, or competency about fulfilling the requirements of the ISP" (Bulgurcu et al., 2010, p. 529).
Attitude toward compliance with the ISP	An employee's evaluation of the positive or negative effects of showing a compliant behavior towards organization's ISP (Hu et al., 2011)
Compliance behavior	"Degree to which an employee protects the information technology assets of his or her organization by following its ISP" (D'Arcy & Lowry, 2019, p. 47).

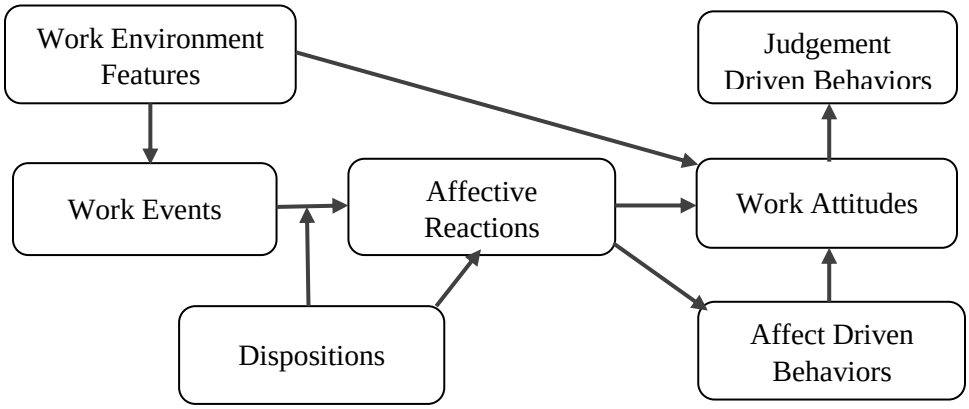
Affective Events Theory

Affective Events Theory (AET) is a significant addition to research on employees' experience at the workplace (Ashton-James & Ashkanasy, 2005; Humphrey, 2006; Walter & Bruch, 2009). AET, as proposed by Weiss and Cropanzano (1996) posit that workplace events that are perceived to impinge and/or promote employee wellbeing lead to affective events that influence affective responses (moods, emotions, feelings, etc). These affective responses in turn influence employees' attitudes and behavior

(Ashton-James & Ashkanasy, 2005). Essentially, the central tenet of AET is that workplace events will affect an employee's affective experiences (moods, emotions), attitudes and behaviors (Mitchell, 2011). AET emphasizes on (1) "the structure, causes, and consequences of affective experiences at work" (2) "events as proximal causes of affective reactions" (3) "time as an important parameter when examining affect and satisfaction" and (4) the structure of affective reactions as important as the structure of environments (Weiss & Cropanzano, 1996, p. 11). These four AET premises lend credence to current research that have applied AET with emphasis that affective and attitudinal events can cause certain work-related behaviors (Walter & Bruch, 2009).

Figure 4

Affective Events Theory (Weiss & Cropanzano, 1996)



Affect in Rational Decision-making

There is substantial theoretical evidence to support the fact that affect is a significant component in the rational decision-making process. As demonstrated in neuroscientific research, rational decision-making "is at best impractical, at worst impossible" (Djamasbi et al., 2010, p. 284) without affect. Affect is a simple, nonreflective neurophysiological state that is considered an integral blend of a feeling of

pleasure/displeasure (feeling of good or bad) and a feeling of engagement or value (Russell, 2003). It is an umbrella term that is influenced by everyday experiences and describes moods, emotions, or feelings (King et al., 2015; Zhang, 2013). Although cognition has been widely studied more than affect in the past decades, scholars in several disciplines have emphasized the importance of affect and its impact on attitude and behavior (Zang & Li, 2005). Studies in information systems and social psychology posit that even though affect comes before cognition, it also influences cognitive reactions (Norman, 2002; Russell, 2003).

Innate to rational choice theory (RCT) and theory of planned behavior (TPB), affect works in two ways to influence the process of rational decision-making: directly and indirectly. Directly, results from neuroscientific studies have shown that affect and cognition each have a contributing role in controlling thought and behavior (Forgas, 2008; Pessoa, 2008). Even though this direct pathway is yet to be confirmed by ISP compliance studies, prior research has proposed that affect directly influences compliance behavior (Baskerville et al., 2014; Pham et al., 2001; Yu et al., 2015). Indirectly, affect influences the cognitive judgement of an individual's cost-benefit appraisal (D'Arcy & Lowry, 2019). As conceptualized by rational choice theory, in this pathway, affect occurs before, and then directs the costs-benefits judgements of individuals. For example, an individual in a good state of feeling or mood will perceive higher benefits for showing a particular behavior than someone having a negative mood. Affect is very significant in explaining variance in a number of dependent constructs as used in information systems literature. It shows significant relationships between positive and negative emotions and constructs like intention to use, ease of use, attitude toward use, perceived usefulness,

use, and training (Bulgurcu et al., 2010; Djamasbi et al., 2010; Zhang & Li, 2005). In addition, findings from studies conducted in the information security context have equally confirmed the indirect influence of affect. Table 5 shows affect constructs as used in IS studies.

Table 4

Affect Concepts and Constructs as used in IS Studies

Construct	Source
Decision-making	Bahr and Ford (2011), Finucane et al. (2000), Slovic et al. (2004).
Online reviews	Yin et al. (2014).
Intention to use (behavioral intention)	Cenfetelli (2004), Djamasbi and Strong (2008), Moon and Kim (2001), Venkatesh and Speier (1999), Venkatesh et al. (2003), Zhang and Li (2007)
Masked affective priming	Comesaña et al. (2013)
Perceived ease of use	Cenfetelli (2004), Djamasbi et al. (2010), Venkatesh (1999), Venkatesh (2000), Zhang and Li (2005)
Website trust formation	Wakefield (2013), Lowry, Twyman, et al. (2014).
Cognitive absorption	Agarwal and Karahanna (2000)
Personal information disclosure	Wakefield (2013) and Yu, Hu, and Cheng, (2015)
Intrinsic motivation	Venkatesh and Speier (1999)
Deterrence	Willison and Warkentin (2013)
Computer abuse or deviant behavior	Posey, Bennett, Roberts, and Lowry (2011)
Privacy protection belief, privacy risk belief	Li et al. (2011)

Integrating Affect into Information Systems Research

The influence of affect on different IS constructs has been explored in information systems research (Zang, 2013). Considering that affect has consequences that reflect attitude and behavior (Weiss & Cropanzano, 1996), it has been used in IS studies to

explain variance in different related constructs. Significant relationships exist between negative emotions (like anger, stress, anxiety) and positive emotions (like enjoyment, satisfaction, pleasure) and IS constructs such as intention to use, perceived usefulness, ease of use, attitude toward use and training (see Table 5).

In the past decades, studies that focus on cognition have garnered more attention than affect-related studies. Recently, the importance of affect and emotion has drawn interest from scholars in different disciplines (Chen et al., 2013). Despite this significance, the exploration of affect in IS security-related behavioral studies is noticeably limited. Therefore, including affect in this study is very critical given the fact that it has not been given much attention in IS security research. The table below represents some constructs as used in a few behavioral IS research.

Table 5

Affect Constructs as used in IS Security Studies

Construct	**Study**
Perceived visual attractiveness	van der Heijden, 2003
Abuse-negative and abuse-positive affect	Kim et al. (2012)
Perceived risk	Ma and Wang (2009) and Zhang et al. (2013)
Perceived usefulness	Zang and Li (2005)
Online privacy protection belief	Li et al. (2011)
Work place deviance	Chen et al. (2013), Samnani et al. (2014)
Self-Disclosure	Yu et al. (2015)
Intention to disclose personal information	Wakefield (2013), Kehr et al. (2015)
Computer abuse or deviant behavior	Baskerville et al. (2010) and Posey et al. (2011)
Perceived lack of attributed trust	Posey et al. (2011)

Defining Affect

Generally, the term affect represents a combination of different moods, emotions, or feelings (King et al., 2015; Zhang, 2013) which are influenced by everyday experiences. It is a neurophysiological state of specific concepts including simple, non-reflective feelings. Affect represents "not so much the cool appraisal of what is out there but what the individual feels [at work], in terms of hedonic tones" (Organ & Near, 1985, p. 243). Moods are superficial and of longer duration than emotions (Lowry et al., 2014; Zhang, 2013). Therefore, in a day-to-day work life situation, employees may experience different moods that influence their perception of the organization and interactions at the workplace (Rothbard & Wilk, 2011). Affect can exert direct impacts on behavior (Yu, et al., 2015), in line with a dispositional view suggesting that affect motivates people to act in a particular way. Moods are influenced by daily events and interactions that happen at the workplace (Loiacono & Djamasbi, 2010). In this regard, researchers in the IS and other domains have conceptualized moods as an external antecedent used to predict attitude and rational behavior at the workplace (Lee et al., 2017; Loiacono & Djamasbi, 2010). Affect-related research has primarily focused on two main mood types; positive and negative affect.

Positive affect is the extent to which a person feels enthusiastic, alert, and active (King et al, 2015). It is the tendency for an individual to feel positive in their surrounding environment. In their meta-analytic study, Lyubomirsky et al. (2005) posited that positive affect plays a causal role and serves as an antecedent to desirable behavioral outcomes in different life domains. The central tenet of their study is that "positive affect engenders success" (Lyubomirsky et al., 2005, p. 803). Studies conducted in social psychology and

industrial organization reveal that employees with a high degree of experience in positive affect demonstrate higher organizational citizenship behavior (Crede et al., 2007) and overall higher job performance (Wright et al., 2007) thus ethical behavior.

Negative affect reflects the tendency to which a person experiences negative or distressing emotions characterized by sadness, fear, anxiety and lethargy (Samnani et al., 2014; Watson & Clark, 1984; Watson et al., 1988). Research that explored the relationship between negative affect and workplace unethical or counterproductive behaviors literature (e.g. Aquino et al., 1999; Chen et al., 2013; Douglas & Martinko 2001; Hershcovis et al., 2007; Samnani et al., 2014) has found that individuals who experience high negative affect have the proclivity to be very sensitive and more reactive to negative events. These individuals therefore have a high probability to engage in workplace deviant behavior including ISP noncompliance. Table 7 below shows the definition of different concepts as they relate to the construct of affect. However, for the purpose of this study, emphasis was placed on negative affect and how simultaneously with cognitive evaluations, it influences employees' ISP non-compliance behavior at the workplace.

Table 6

Definition of Concepts Related to Affect

Concept	Definition
Affect	A combination of specific concepts that includes moods, emotions, or feelings, which are influenced by everyday experiences (King et al., 2015; Zhang, 2013).
Core Affect	A two-dimensional affect construct that describes a person's moods and emotions (Russell, 2003).

Table 6 (continued)

Definition of Concepts Related to Affect

Concept	Definition
Affective Quality	The ability of a stimulus to change an individual's core affect (Russell, 2003).
Emotion	A mental or affective state of being ready as a result of the cognitive appraisals of one's environment (Bagozzi et al., 1999), a short-lived subjective feeling (Djamasbi, 2007; Loiacono & Djamasbi, 2010).
Feeling	The subjective emotional experience presumed to have an important monitoring and regulation function (Scherer, 2005).
Mood	The enduring predominance of certain subjective feelings that influence an individual's experience and behavior (Scherer, 2005).
Positive Affect	A mood-dispositional dimension that reflects pervasive individual differences in positive emotionality and self-concept (Watson & Clark, 1984).
Negative Affect	A mood-dispositional dimension that reflects pervasive individual differences in negative emotionality and self-concept (Watson & Clark, 1984).
State Affect	The mental state of preparedness emanating from cognitive appraisals of events or thoughts (Bagozzi et al., 1999).
Trait Affect	The relative tendency to experience more frequently certain moods or the ability to react with certain emotions, even with the slightest provocation (Judge, 1992; Russell, 2003; Scherer, 2005).

Affect can take two dimensions: state affect and trait affect (Carmichael & Piquero, 2004). State affect refers to emotions that can be defined as an individual's mental state of preparedness that results from the cognitive appraisal of their immediate environment (Bagozzi et al., 1999). Positive emotions lead to desirable behaviors like organizational citizenship behaviors while negative emotions may nurture deviant or unethical behaviors. For example, if an employee perceives they have been treated unfairly by their organization they develop anger and demonstrate unethical behaviors. One such behavior is non-compliance to ISPs, which is often detrimental to productivity

(D'Arcy et al., 2014; Posey et al., 2014; Puhakainen & Siponen, 2010). Trait affect drives an individual's mood and can be defined as the relative tendencies to experience more frequently certain moods or the ability to react with certain emotions, even with the slightest provocation (Judge, 1992; Russell, 2003; Scherer, 2005). These tendencies moderate the relationships between constructs like performance, output and job satisfaction (Judge, 1993; Weiss & Cropanzano, 1996). These affective states or emotions can therefore be said to influence behavior (Ilies & Judge, 2002).

Cognitive and affective dimensions have been confirmed to be associated with the construct of attitude (Ajzen & Fishbein, 2005; Eagly & Chaiken, 1993). In the affective dimension, attitude is understood to be a form of affective evaluation while in the cognitive dimension, attitude is conceptualized as reason-based, cognitive evaluation (Zhang, 2013). Weiss and Cropanzano (1996) argued that some workplace behaviors are a result of the affective experiences employees are submitted to at work while others represent the influence of cognitive evaluations by employees at work.

Organizational Injustice

Organizational justice has been used as a promising framework in IS research for understanding unethical behavior at the work place (Ambrose et al., 2002). Meta-analytic studies conducted on organizational justice (Cohen-Charash & Spector, 2001; Colquitt et al., 2007), and deviant behaviors (Berry et al., 2007; Hershcovis et al., 2007) have placed considerable value on unethical behavior and perceived justice literature. Researchers have used the term justice interchangeably with injustice to refer to employees' perceptions of fairness in the distribution of outcomes (Cohen-Charash & Spector, 2001), treatment from top management (Bies & Moag, 1986; Tyler & Bies, 1990), the execution

of processes (Cohen-Charash & Spector, 2001), and the availability of information that may influence outcome (Lim, 2002; Shapiro et al., 1994). Colquitt et al. (2001) define organizational justice as employee's perception of fairness of resource allocation and decision-making by top management in an organization. Justice, a synonym of "fairness" refers to managerial actions and decisions that correspond to the moral and ethical standards of the organization's laws and culture. This can be in forms like incentives, fairness in performance evaluation and job promotion procedures or fair pay (Yean & Yusof, 2016).

A number of organization behavioral researchers have widely examined the different relationships and types of injustice and how they lead to non-productive consequences at the workplace (Ambrose et al., 2002; Greenberg, 2006; Mitchell & Ambrose, 2007; Skarlicki & Folger, 1997). The seminal equity theory established by Adams (1963) deposed that *"inequity (injustice) aggravates individuals to make adaptive response in both cognitive and behavioral ways".* In addition, Adams (1965) posited that employees whose job compensation is not proportionate to their performance and effort experience some emotional reactions that exude signs of stress. Against this backdrop, I can therefore argue that organizational injustice nurture stressful conditions under which negative emotions and deviant behavior generate.

Also, Jones (2009) and Kwak (2006) noted that employees' perception of poor organizational justice is a regiment that leads to destructive behavior at the workplace. Subsequently, organizational injustice can be looked upon as a prominent predictor of employees' noncompliance with ISP. Relative to employees who receive appropriate reward for their job performance, those who feel unfairly treated display signs of

dissatisfaction and stress. These stressful situations can reflect their mood, emotion and daily complaints (Niedhammer et al., 2004). Therefore, understanding the fair practices shown to employees by their managers and how these practices influence individual employees' intention to engage in unethical behaviors could help organizations protect their resources and assets.

Organizational injustice literature differentiates three main constructs that can be used to explain different phenomena and how they influence employees' perceptions of injustice in organizations. These constructs include distributive injustice, procedural injustice and interactional injustice.

Distributive Injustice

Distributive injustice relates to employee's perceived beliefs that they do not receive benefits in proportion to the amount of effort they put on the job (e.g. perceived unfairness in performance evaluation). Adams (1965) argued that when employees perceive that they have been unfairly rewarded compared to their counterparts, they develop perceptions of unfair treatment and try to restore justice. One way of restoring justice is to develop an organization-targeted aggressive behavior or become counterproductive (Cohen-Charash & Spector, 2001). Aquino et al. (1999) argued 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" (p. 1075). Ultimately when an employee perceives unfair outcomes (distributive injustice), their affective reactions (e.g., anger, happiness, pride, or guilt), cognitions (e.g., cognitively distorted inputs and outputs), and behavior (e.g.,

misuse, performance or withdrawal) become influenced (Cohen-Charash & Spector, 2001).

Procedural Injustice

Procedural injustice (Colquitt et al., 2001), refers to employee's perceived beliefs that the procedures and processes put in place to determine outcome are unfair (e.g. perceived inequity in performance evaluation). As emphasis in distributive justice has shifted towards the process of resource allocation (procedural justice), research on organizational justice has also shifted (Cohen-Charash & Spector, 2001). No longer is perceived distributive injustice considered the main predictor of organizational injustice, but rather, the perceived procedural injustice of the processes that generate the outcome (Lind & Tyler, 1988). Results from extant literature show that not only perceptions of distributive injustice or inequity generate stress but also perceptions of procedural injustice. For example, Brotheridge (2003) showed that procedural injustice and distributive injustice both have a moderating influence on the effects of emotion that lead to different physiological and emotional behaviors. Furthermore, studies have concluded that reactions to stress because of the different injustices jointly manifest themselves. Tepper (2001) found that individuals who experienced high degree of procedural and distributive injustices showed more stress as their level of anxiety, depression and emotional exhaustion increased. Because procedures and processes determine resource allocation in organizations, procedural justice is determined to be a strong predictor of affective, cognitive and behavioral reactions toward the organization (Cohen-Charash & Spector, 2001). Leventhal (1980) has conceptualized that six rules (see Table 4) must be met in order to ensure fairness in procedures within the organization.

Table 7

Definition of Rules for Procedural Justice

Rule	Definition
The consistency rule	All procedures for allocation of resources should be consistent throughout the organization (Leventhal, 1980).
The bias-suppression rule	Self-interests should not be manifested in the decision-making process of resource allocation (Leventhal, 1980).
The accuracy rule	The accuracy of the process allocation information (Leventhal, 1980).
The correctability rule	Possibility to change an unfair decision from any existing opportunities (Leventhal, 1980).
The representativeness rule	Representation of the needs and values of all individuals affected by the process of allocation (Leventhal, 1980).
The ethicality rule	The process of resource allocation must be congenial with the ethical and moral values of the perceiver (Leventhal, 1980).

Interactional Injustice

Interactional injustice is a form of organizational injustice, which refers to employee's perceptions of the injustice, or unfair interpersonal treatment they receive from their managers when procedures are implemented (Colquitt et al., 2001). Because this reflects the human side of the organization, it relates to the process of communication between the management and employees as recipient of injustice. It is the unjust interpersonal relationship that employees have with figures in authority (Cropanzano et al., 2007), and determined by the interpersonal behavior of representatives from management. Therefore, interpersonal injustice is expected to strongly predict cognitive, affective, and behavioral reactions toward these managers who represent the source of justice (Bies & Moag, 1986; Masterson et al., 2000). Thus, during interactional injustice, the employee becomes dissatisfied and is expected to react negatively towards his or her manager (or the authority that is interactionally unfair to them) rather than react

negatively towards the organization, as predicted by distributive and procedural injustice. Similarly, the employee will be less committed and develop negative behaviors toward the manager and less so to the organization (Masterson et al., 2000). Interactional justice can be divided into two groups: (1) interpersonal justice which refers to the fairness of treatment (e.g. politeness, dignity, and respect) employees receive from the supervisors involved in process execution to determine outcomes (Colquitt et al., 2001) and (2) informational justice which refers to the availability of enough information (e.g. reasonable, timely, and specific) on how given procedures were used and outcomes distributed (Colquitt et al., 2001; Shapiro et al., 1994).

Even though organizations have invested a lot on ISPs to protect their information and computer assets from abuse, employees who experience any form of injustice at the workplace may render these systems and ISPs susceptible for violation and misuse. Employees who feel cheated and unfairly treated based on outcomes become dissatisfied, emotionally disconnected and develop feelings of resentment. These affective expressions motivate attitudes and deviant behavior, that may subsequently translate to feelings of retaliation on the organization through unethical use of ISP and procedures violation.

Employee Information Security Policy (ISP) Compliance

The extent of ISP misuse at the work place is alarmingly high and undeniable. In a survey conducted by Forbes Insight in 2017 on re-engineer information security in the age of digital transformation, 69% of company executives believe that advancements in information technology have provided them with platforms to reconsider and enhance their security policies (Forbes Insight, 2017). Due to the value placed on the behavioral

tenets of information security compliance, many studies have been conducted with focus on the issues of employees' information security policy (ISP) and procedure compliance (Chen et al., 2018; Ifinedo, 2012; Kraemer & Carayon, 2007; Post & Kagan, 2007; Siponen et al., 2014). Despite the strong theoretical foundation of these ISP compliance studies, many of these studies reported different findings on employees' ISP compliance/non-compliance behaviors (Chen et al., 2018). It is therefore imperative that employees make the right decisions when it comes to complying with IS policies.

IS policy represents a set of established guidelines that details the processes and procedures, including technical controls that employees need to follow in order to help achieve the information security objectives of the organization (Bulgurcu et al., 2010; Steinbart et al., 2016). Achieving these objectives and the effectiveness of this policy lies on the organization's need to focus on increasing employees' awareness of the policy (D'Arcy et al., 2009; Puhakainen & Siponen, 2010) through continuous training on the benefits associated with creating secured passwords, identifying phishing emails or shutting down workstations when not in use. The decision to embark on unethical use of computer systems thereby violating IS policies and procedures may result to significant financial risks and legal ramifications to the organization (Furnell & Thomson, 2009; Siponen et al., 2009, 2014). However, IS literature suggests that employees more often do not comply ethically with such processes and guidelines (Li et al., 2019). Instead, organizations are experiencing an increasing trend in the misuse, abuse, and destruction of its IS assets and resources by insiders (Ifinedo, 2014; Yoon et al., 2012).

There is a recent shift in approach of IS security studies with scholars moving from a more technical perspective to a sociotechnical norm, where emphasis is placed on

employee behavior as an important human factor of IS security that can be used to understand and predict employees' ISP compliance at the work place. This shift has resulted to an increased interest in the study of antecedents and factors that influence employees' ISP compliance/noncompliance behaviors, drawing upon rationality-based theories like protection motivation theory, general deterrence theory, theory of planned behavior and rational choice theory (D'Arcy & Lowry, 2019; Cheng et al., 2013). These theories describe individual cognitive processes that influence employees' ISP compliance behavior by examining the antecedents of ISP misuse behavior (D'Arcy et al., 2009; Hu et al., 2011; Siponen & Vance, 2010; Vance & Siponen, 2012; Willison & Warkentin, 2013), and factors leading to ISP compliance behaviors (Alotaibi1, Furnell1 & Clarke, 2016; Guhr, et al. 2018; Ifinedo, 2012; Johnston & Warkentin, 2010; Shropshire, et al, 2015).

Findings from many IS literature have provided guidelines that support the effective application and implementation of IS policies to encourage compliance behavior (Chen et al, 2012; Chu & Chau, 2014; Puhakainen & Siponen, 2010; Warkentin et al., 2011). However, insiders fail to "protect the integrity and privacy of the sensitive information of the organization and its partners, clients, customers, and others" (Warkentin & Willison, 2009, p. 102) due to lack of motivation, inadequate education and training or laziness. Consequently, numerous IS researchers have derived substantial interest in the study of employee compliance with IS policy by exploring antecedents to ISP compliance intention and behavior. Examples of such studies include cost-benefit of compliance/noncompliance (Bulgurcu et al., 2010; D'Arcy & Lowry, 2019), neutralization techniques (D'Arcy et al., 2014; Siponen & Vance, 2010; Teh et al., 2015),

self-efficacy (Warkentin et al., 2011), rationality-based decision-making processes (Hu et al., 2011; Vance & Siponen, 2012), perceived justice of punishment, punishment expectancy (Xue et al., 2010), severity and certainty of sanction of IS misuse (D'Arcy et al., 2009) and formal and informal antecedents of employee ISP unethical behaviors (Cheng et al., 2013). However, despite the attention devoted to ISP compliance behavior, and results from compliance studies, policy violations remain a top concern for information security management.

Rationality-based behavioral IS literature have used different frameworks to explain reason-based cognitive processing that influence rational decision-making. Hu et al. (2011) used the rational choice theory to test end users' ISP violation intention. Their results showed that benefit perception significantly influences employees' intended behavior, suggesting that punishment by itself is not effective in reducing employees' intended behavior to violate policy. Willison et al. (2018) proposed an integrated theoretical model based on rational choice theory and absolute and restrictive deterrence to explain how deterrence can be used to influence employees' participation in and frequency of insider computer violation intentions. They argued that deterrence theory can provide more opportunities for future research on insider threat behavior if scholars integrate it with the rational choice theory. This is because deterrence theory is a subset of rational choice theory with regards to the perceived cost section of rational decision-making process (Hechter & Kanazawa, 1997).

Consistent with findings from Hu et al. (2011) is the conclusion made by Siponen and Vance (2010). They posited that neutralization significantly predicts ISP compliance behavior, which in turn influences the effects of formal sanctions in an organization. In

addition, in order to understand the effects of benefits on ISP violation, Vance and Siponen (2012) tested a model based on rational choice theory. They concluded that perceived benefits, moral beliefs and informal sanctions are significant predictors of end user's violation of ISP.

Behavioral IS security research has shown that a number of factors either facilitate or hinder employees' compliance with ISP (e.g. Boss et al., 2015; Lebek et al., 2014; Sommestad et al., 2014). Even though non-rationality factors like reactance (Lowry & Moody, 2015; Lowry et al., 2015) and habit (Vance et al., 2012) have been used in some of these studies, they have been applied under a near pure rationality basis in the decision-making process (D'Arcy & Lowry, 2019).

Vance et al. (2012) applied the protection motivation theory (PMT) to explore how habit drives employees' ISP compliance in organizations. They found that nearly all components of PMT strongly predict employees' ISP use/misuse intentions. In the same framework using PMT, Johnston and Warkentin (2010) concluded that 'fear appeal' significantly predicts employees' intention not to violate ISP procedures. Meanwhile Siponen et al. (2009) found that response efficacy, threat appraisal and self-efficacy significantly influence employees' intention to comply with organizational ISP but coping appraisals have no significant influence on compliance attitudes (Siponen et al., 2010). Proponents of PMT argue that threat appraisals and coping appraisals significantly affect behavioral intention on ISP compliance (Cheng et al., 2013).

Threat appraisals assesses the degree to which an individual is threatened. There are two kinds of threats, perceived vulnerability and perceived severity. Coping appraisals (response efficacy, self-efficacy, and response cost) are constructs used to

assess an individual's ability to eliminate the threat. From a cost-benefit perspective of rational choice, results from Bulgurcu et al. (2010) show that the cost-benefit appraisal of compliance and non-complia0.nce significantly influence employees' ISP behavior and intentions. Similar results could be seen from Li et al. (2010) on employees' compliance intention of internet use policy. They concluded that formal sanctions, security risks and perceived benefits affect user compliance intention with internet use policy.

In summary, the extant literature reviewed in this section presents disparate findings that support different evaluative beliefs of cognitive influences as drivers of ISP compliance behavior. However, these studies are not commensurate with the importance of this problem due to the absence of an important concept - affect. Neys (2006), using the dual-process theory argued that a "rational thinking failure" such as unethical misuse of policy in the work place can be explained by two different human reasoning systems; affect and cognition. These reasoning systems can be used to evaluate employees' ISP non-compliance behavior. Therefore, in order to fully understand the prevalence of unethical violation of information security policies, an understanding of the combined role of both cognitive and affective processes in ISP compliance is imminent as they both influence rational decision-making.

Studies conducted under the organizational culture framework have explored the multidimensional aspect of attitude within workplace attitude, and research has considered the affective scope of workplace attitude, its precursors, and the consequences of affect on behavior (Ilies et al., 2006; Judge et al., 2006; Judge et al., 2009; Matta et al., 2017; Rodell & Judge, 2009). Supporting the affective dimension of workplace attitude, studies have shown that measuring this construct varies and that these variations predict

and can be predicted by variables like workplace events, daily feelings and job performance (Judge et al., 2012).

Secondly, there is the need for research that could reveal how affective events such as negative moods and emotions - created by organizational injustices - are associated with affective reactions of dissatisfaction, anger and frustration, and how these affective reactions lead to employees' cognitive cost-benefit appraisal and daily ISP non-compliance attitude. To respond to this issue, this study was designed with the application of ISP non-compliance in the same context. Essentially, this study conceptualized and measured affect-based and cognitive-related constructs and how they influence ISP non-compliance and unethical behavior.

Theory Development

Discussions from the previous sections in this chapter provided a succinct background and added perspective into the cognitive and affective processes, ISP non-compliance attitude and behavior as depicted in the conceptual model in Figure 5. This model is consistent with Weiss and Cropanzano's (1996) affective event theory, which described both cognitive and affective processes and their influence on attitude and behavior. In the model, this study proposed that perceived organizational injustice (i.e. fairness perception) is predicted to be negatively related to negative affect. Together, negative affect and perceived organizational injustice were also expected to be negatively related to individual's ISP non-compliance attitude and behavior.

Perceived Organizational Injustice

As discussed in the preceding sections, organizational injustice represents job stressors and influences negative emotions that result to non-compliance behavior at the

work place (Zohar, 1995). When individuals perceive they are not fairly treated while on the job, their cognitions, moods and emotions become affected and therefore force certain behavioral responses such as counterproductive workplace behavior and ISP non-compliance (Cohen-Charash & Spector, 2001; Greenberg, 1990). Essentially, employees' perception of unfair treatment is characterized by (1) experience of negative emotions and anger (Dupré et al., 2010; Willison & Warkentin, 2009), (2) deliberation on retaliating against the employer (Bennett & Robinson, 2000), and (3) rationalizing their unethical and/or deviant behavior including ISP non-compliance (Li et al., 2010; Lim, 2002). Individuals who experience a high level of injustice may become deeply involved in their emotions and this may lead to serious negative ramifications if the unfairness is not curtailed.

Perceived Distributive Injustice

Distributive injustice refers to the perceived unfairness of distribution or allocation decisions such as monetary rewards and recognitions due to outcomes (Aryee Budhwar, & Chen, 2002; Colquitt et al., 2001; Elovainio et al., 2004). It relates to employee's perceived beliefs that they do not receive benefits in proportion to the amount of effort they put on the job (e.g. perceived unfairness in performance evaluation). Skarlicki and Folger (1997) made a connection between negative emotions and perceptions of injustice. Perceived distributive injustice is judged when employees evaluate and compare the outcome to that of a co-worker, a standard or a past experience (Hubbel & Chory-Assad, 2005). Employees then develop perceptions by measuring if their distributive outcome meet their expectation and/or is proportional to that of their counterpart (Alder & Ambrose, 2005; Colquitt et al., 2006; Greenberg, 2006). Homans'

(1974) classic proposition stated that individuals who have been treated fairly tend to experience an upswing in positive emotions and those under-rewarded will experience anger and resentment. Hence, when employees perceive distributive injustice at the workplace, they develop feelings of dissatisfaction, resentment and anger. This feeling affects their attitude, commitment and output (Ambrose & Cropanzano, 2003; Sager, 1991) and influence their behavioral reaction. In light of this literature, the hypotheses:

H1A: *Perceived distributive injustice is negatively related to attitude toward specific information security policy.*

H1B: *Perceived distributive injustice is positively related to information security policy non-compliance intention.*

Perceived Procedural Injustice

Procedural injustice (Colquitt et al., 2001) refers to employee's perceived beliefs that the procedures and processes put in place to determine outcome are unfair (e.g. perceived unfairness in performance evaluation and promotion). Procedural injustice is associated with dissatisfaction, anger and resentment irrespective of how favorable the outcome is (Folger & Cropanzano, 1998) and these negative emotions may arise from organizational stressors. Task difficulty and procedural unfairness like organizational policy for performance evaluation and promotion based on employee's years of job experience instead of performance outcome represent examples of perceived controllable organizational stressors and can generate a feeling of negativity among employees. When an organization fails to conduct a fair performance or promotion procedure on an employee, the outcome may be a stressful appraisal of the situation by the employee, which in turn might lead to negative emotions. If the employee perceives they have been

unfairly treated, they hold the organization responsible for implementing the unfair procedure. Essentially, it is evident to state that the unfair enactment of procedures may force employees to develop negative feelings. Therefore, perceived procedural injustice is a predictor of employee non-compliance behavior at the workplace. Hence, the hypotheses:

H2A: *Perceived procedural injustice is negatively related to attitude toward specific information security policy.*

H2B: *Perceived procedural injustice is positively related to information security policy non-compliance intention.*

Perceived Interpersonal Injustice

Interpersonal injustice refers to the fairness of treatment (e.g. politeness, dignity, and respect) employees receive from the supervisors involved in process execution to determine outcomes (Colquit et al., 2001). Agent-system model states that the main source of interpersonal injustice/justice is from managers and supervisors (Bies & Moag, 1986). When an employee feels discontented because of rudeness, disrespect or any other form of mistreatment they receive, they tend to retaliate by directing their deviant behavior towards the entity they receive the mistreatment from (Robinson & Bennett, 1995). Hershcovis et al. (2007) concluded that interpersonal injustice (mistreatment from managers or supervisors) is a primary predictor of workplace counterproductive behavior. Consequently, when employees perceive interpersonal injustice through unfair treatment, they tend to counter the injustice by developing some cognitive, affective and unethical ISP non-compliance behavior towards the organization (Cohen-Charash & Spector, 2001; Greenberg, 1990). Therefore, the hypotheses:

H3A: *Perceived interpersonal injustice is negatively related to attitude toward specific information security policy.*

H3B: *Perceived interpersonal injustice is positively related to information security policy non-compliance intention.*

Perceived Informational Injustice

Informational justice refers to the availability of enough reasonable, timely, and specific information on how given procedures are used and outcomes distributed (Colquitt et al., 2001; Shapiro et al., 1994). It emphasizes the idea that in the decision-making process, those in position of authority should provide adequate information about processes and outcomes to those employees affected by their decisions (Sindhav et al., 2006). Employees comply with organizational policies when they are provided with detailed information about the consequences of violating such policies. For organization ISP compliance, informational injustice become apparent when employees perceive that authority figures in an organization are not open in their communication of why an ISP compliance is necessary and the processes and procedures put in place to detect and deter any non-compliance behavior (Li et al., 2014). When an employee perceives that incomplete or inadequate information is provided and used to arrive at an unfair decision, they develop cognitive, affective, and negative behavioral reactions as a result of the injustice (Cohen-Charash & Spector, 2001; Greenberg, 1990). Therefore:

H4A: *Perceived informational injustice is negatively related to attitude toward specific information security policy.*

H4B: *Perceived informational injustice is positively related to information security policy non-compliance intention.*

Attitude Toward Information Security Policy

In the premise of ISP compliance, attitude refers to ISP compliance attitude. Attitude toward information security policy represents the relative extend of an employee's favorable or unfavorable appraisal of ISP compliance (Ajzen, 1991; Herath & Rao, 2009b). The TPB posit that attitude, whether positive or negative, influences intended behavior (Azjen, 1991). In the same TPB framework, Bulgurcu et al. (2010) argue that beliefs surrounding the appraisal of consequences will affect an employee's overall compliance attitude and intended behavior. In other words, attitude is presumed to influence an employee's ISP compliance intentions. Other IS-related studies that employed the TPB model have also supported this argument (Karahanna et al., 1999). Accordingly, I anticipate that:

H5: *Attitude toward general information security policy is positively associated with attitude toward specific information security policy.*

H6: *Attitude toward specific information security policy is positively associated with information security policy non-compliance intention.*

Negative Affect at the Workplace

Negative affect is the tendency where individuals experience negative feelings and emotions like fear, anger, anxiety (Samnani et al. 2014; Watson et al. 1988). Behavioral studies that examine the link between negative affect and workplace deviant behavior have found that employees experiencing negative affect have a likelihood to engage in counterproductive or deviant workplace behavior (Hershcovis et al. 2007; Yang & Diefendorff, 2009). Cropanzano et al. (2003) and Penney and Spector (2005) suggested an explanation of the effect of negative affect on workplace deviant behavior.

They stated that employees experiencing negative affect perceive the world around them negatively and therefore are motivated to demonstrate behavior that will help them reduce the negative feeling.

The "affect management" (Dalal et al. 2009, p. 1053) further explains the relationship between negative affect and workplace deviant behavior. It posits that individuals who go through negative feelings and emotions will try to mend this negative affective state when they engage in deviant behavior at the workplace. In the ISP compliance context for example, when an employee perceives that the organization is making decisions that feed them with negative emotions, they reciprocate that negative feeling by engaging in the violation of the organization's IS policy and demonstrating other deviant behavior (D'Arcy & Lowry, 2019). In light of the above statements, this research study predicts that daily negative affect will influence employees' daily attitude towards ISP compliance. Compliance attitude in this context represents the affective appraisal of compliance with IS policy because this study focuses on the affective dimension of ISP compliance attitude. Therefore, when employees experience negative moods, they become engaged in negative and counterproductive tasks of their job (IIies & Judge, 2002; Rothbard & Wilk, 2011), one of which is the unethical use and violation of ISPs. Essentially, negative affect elicits negative emotions on ISP compliance and negative attitude towards this behavior. Hence the hypotheses:

H7: *Negative affect negatively influences attitude toward specific information security policy.*

H8: *Negative affect positively influences information security policy non-compliance intention.*

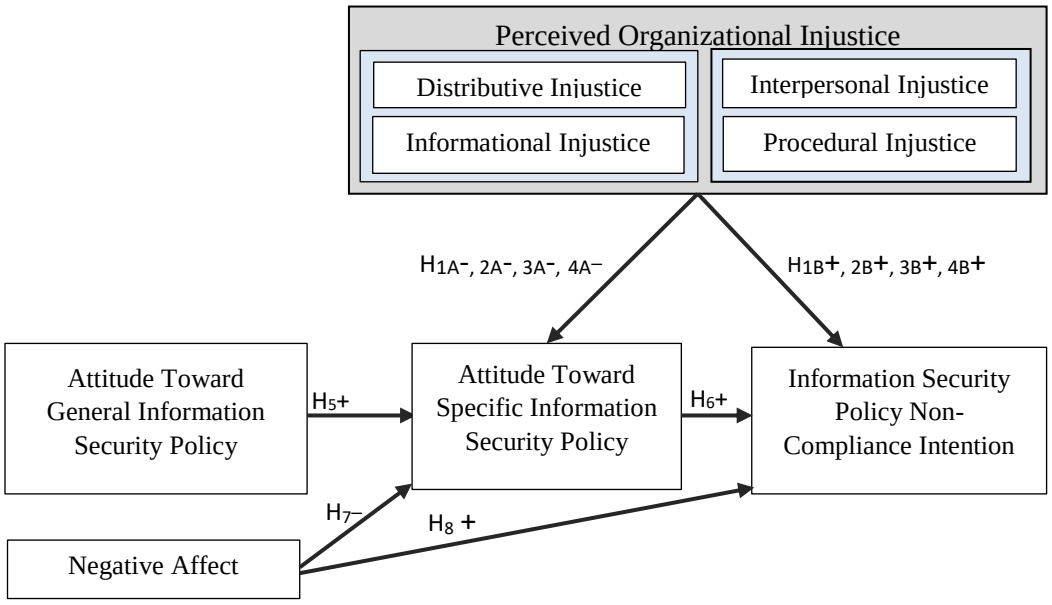
Table 8

Hypotheses and Structural Relationships

HO	Structural Relationship
H1A	Perceived distributive injustice is negatively related to attitude toward specific information security policy
H1B	Perceived distributive injustice is positively related to information security policy non-compliance intention.
H2A	Perceived procedural injustice is negatively related to attitude toward specific information security policy.
H2B	Perceived procedural injustice is positively related to information security policy non-compliance intention.
H3A	Perceived interpersonal injustice is negatively related to attitude toward specific information security policy.
H3B	Perceived interpersonal injustice is positively related to information security policy non-compliance intention.
H4A	Perceived informational injustice is negatively related to attitude toward specific information security policy.
H4B	Perceived informational injustice is positively related to information security policy non-compliance intention.
H5	Attitude toward general information security policy is positively associated with attitude toward specific information security policy.
H6	Attitude toward specific information security policy is positively associated with information security policy non-compliance intention.
H7	Negative affect negatively influences attitude toward specific information security policy
H8	Negative affect positively influences information security policy non-compliance intention.

Figure 5

Research Model and Hypotheses



When one considers the "instrumental nature of joining and remaining in an organization and the opportunities for appraisals of work conditions and outcomes" (Organ & Konovsky, 1989, p. 158), cognitive factors (e.g., employees' perceptions of workplace injustice) and affective reactions (e.g. moods, emotions) seem likely to play an equal, or perhaps greater, role in shaping both helpful and harmful behavior. A summary of the different constructs as used in this research, their definitions and sources is presented in Table 9 below.

Table 9

Definition and Sources of Constructs Employed in the Research Model

Construct	Definition
Distributive Injustice	Employee's perceived beliefs that they do not receive benefits in proportion to the amount of effort they put on the job e.g. perceived unfairness in performance evaluation (Adams, 1965).
Interpersonal Injustice	A form of interactional injustice that refers to the fairness of treatment (e.g. politeness, dignity, and respect) employees receive from the supervisors involved in process execution to determine outcomes (Colquitt, et al., 2001).
Informational Injustice	A form of interactional injustice that refers to the availability of enough information (e.g. reasonable, timely, and specific) on how given procedures were used and outcomes distributed (Colquitt, et al., 2001; Shapiro, et al., 1994).
Procedural injustice	Employee's perceived beliefs that the procedures and processes put in place to determine outcome are unfair e.g. perceived inequity in performance evaluation (Colquitt, et al., 2001).
Attitude toward general information security policy	General information security practices that demonstrate favorable or unfavorable beliefs and predispositions of IS compliant behavior (Ajzen 1991).
Attitude toward specific information security policy	Context-specific information security practices of a particular task for example password sharing, data encryption, shutting down your computer workstation when not in use (Bulgurcu et al., 2010).
Negative Affect	A mood-dispositional dimension that reflects pervasive individual differences in negative emotionality and self-concept (Watson & Clark, 1984).
Information Security Policy Compliance	Employee's intention to protect the organization's IT resources from potential threats of security violations (Ajzen 1991; Fishbein and Ajzen 1975).

Summary

This chapter provides definitions and discussions of constructs relevant to the study. The chapter also establishes the relationships among these constructs with regards to information security policy unethical use at the workplace. A literature review of relevant IS studies and their findings reveal the connections and missing links, regarding the unethical violation of information security policy. Extant literature conducted here indicates that cognitive-based theories have been predominantly employed to explain specific employee's unethical violation of information security policy and engagement in counterproductive behavior at the workplace. Meanwhile organizational literature have focused on affective events to explain deviant behavior. However, the limited IS literature has failed to address the need for research that could reveal how affective events such as negative moods and emotions - created by organizational injustices - are associated with affective reactions of dissatisfaction, anger and frustration, and how these affective reactions lead to employees' cognitive cost-benefit appraisal and many aspects of employee's daily unethical violation of information security policy and noncompliant behavior (Lee & Lee, 2002). This study integrates affective events with cognitive appraisals to explain employees' unethical use of ISP and counterproductive behavior at the workplace.

Chapter 3

Methodology

Overview of Research Design

Creswell (2014) stated that there are three types of research approaches, which include quantitative, qualitative and mixed. Among these approaches comes different designs. This research focused on a non-experimental, quantitative data collection with the objective to examine the relationship between affective and cognitive processes and their influence on employees' non-compliance with ISPs. Through the use of survey for data collection, this non-experimental study involved the assessment of relationships between variables and how these relationships influence the outcomes (attitude and non-compliance behavior). Despite the challenges associated with survey research (Pinsonneault & Kraemer, 1993), there are numerous reasons to conduct survey research: "(1) easy to administer, score, and code; (2) understand relationship among variables and constructs; (3) generalizable; (4) reusable and objective; (5) predictive tool; (6) test theoretical model; (7) confirm and quantify findings" (Newsted et al., 1998, p. 553).

Research Strategy

Given the level of difficulty associated with the study of actual acceptable behavior, a non-experimental scenario-based approach was explored to empirically

examine the stated hypotheses in this study and in turn attempt to answer the research questions. A panel of information technology (IT) experts from the organization was invited to validate the scenarios and questionnaire. The selection of this expert group was based on their familiarity with, and management experience of the organization's IS policies and procedures. Scenarios are nonintrusive and result in improved internal validity (Harrington, 1996). They may also provide a less intimidating way for participants to answer sensitive questions (Nagin & Pogarsky, 2001).

The scenarios in this design were used to induce continued negative affect in the subjects to determine the influence of negative affect on attitude towards and non-compliance with information security policy. Guidelines provided by Finch (1987) were used to create and/or modify the scenarios. Using this ethical approach, a hypothetical scenario web-based survey was distributed to participants who were encouraged to "role-play" and "behave as if he [or she] were a particular person in a particular situation" (Aronson & Carlsmith, 1968, p. 26). Following the scenario, participants then responded to a questionnaire which asked for the likelihood that they would demonstrate similar behavior as stated in the scenario under similar conditions (Vance & Siponen, 2012).

Prior IS research has employed this approach to study ethical issues that relate to IT and security policy violation (e.g. Ambrose et al., 2002; Banerjee et al. 1998; Chatterjee et al., 2015; D'Arcy & Lowry, 2019; Jasso, 2006; Thong & Yap, 1998). This approach allows "researchers to present concrete decision-making situations that approximate real-life situations" (Barnett et al., 1994, p. 473). This approach was chosen for the following reasons. Methodologically, employing a scenario-based approach provides an indirect way to measure undesirable or unethical behavior because ISP non-

compliance, like other unethical behaviors, cannot be measured directly through conventional methods (Harrington, 1996). This is because participants are "most probably not fully attentive to the manipulation" (Wallander, 2009, p. 506) and tend to respond to the questionnaire in a socially desirable manner (Trevino, 1992). Therefore, employing a scenario approach reduces any bias associated with social desirability (Chatterjee et al., 2015) because participants get less intimidated in recording their intentions (Vance & Siponen, 2012). Another advantage for employing a scenario-based approach is that it provides participants with information in a contextual manner that guides their decision-making process as to whether to commit unethical or deviant behavior to ISPs. Bachman et al. (1992) and Klepper and Nagin (1989) supported this methodology with a strong recommendation to include information that provides more specific context by describing the offense in the scenario.

Similar to related studies that have used employees as survey participants (e.g. Cappetta & Magni, 2015; D'Arcy & Lowry, 2019; D'Arcy et. al., 2014), this study beseeched the participation of employed, computer-using professionals of the organization for data collection (D'Arcy & Lowry, 2019). Given that this target population has a practical understanding of technology, are familiar with the organization's computer systems, IS policies and procedures, and are expected to have a general understanding of basic security concepts as well as interact with IT staff, they appear relevant to explore how their perception of unfairness engenders their retaliatory ISP non-compliance behavior. Finally, this population is deemed as an appropriate sampling frame because employees, just like everyone else, are subject to emotions,

moods, and feelings and were expected to abide by the institution's information security policies.

In the context of a higher education institution, using employee participants as a means to explore the non-compliance of IT and ISP can be explained by the fact that higher education accounts for a greater proportion of industry data and security breaches since 2005 (Ayyagari & Tyks, 2012). In addition, Oblinger and Hawkins (2006) reported that among the reported security violations assessed by Privacy Rights Clearinghouse between February 2005 and March 2006, nearly half were carried out in higher education institutions. This justifies the use of this industry in the context of this study.

Instrument Development and Measurement

The instrument design was adapted from Vance and Siponen (2012). To empirically examine employees' ISPs non-compliance intention, a scenario approach was employed. A scenario is a hypothetical situation where respondents are asked to "role play" as if they are in a real-life situation as depicted in the scenario. The scenario is then followed by a series of questions that ask the likelihood that respondents would act under same conditions as depicted in the scenario (Nagin & Paternoster, 1993). For this research, four scenarios were designed describing different ISP violations that represent actual experiences to participants (Piquero & Hickman, 1999). To do so, each member of the IT security team from the organization was contacted via email and asked to state at least four common security policy violations at the organization, by using the organization's information security program manual and annual security incident report. A list of security policy violations was generated from the security team members' responses, and using content analysis, the list was ranked and categorized. The top four

common consequential security policy violations (service account and password sharing, use of work computers for personal business, unfair workplace treatment, and failure to shut down workstations while away) were used to design the scenarios and questionnaire. A web-based questionnaire was sent out to all participants where they were required to read each scenario before proceeding to the questionnaire.

All items for the seven constructs in this study were adapted through modification of instruments that have already been developed, validated, and adopted for use by information security researchers in order to maintain efficiency and higher reliability of results (Colquitt et al., 2001; Herath & Rao, 2009a; Workman et al., 2008). To establish content and construct validity, the scenarios were refined through expert pretest prior to full data collection. By conducting these preliminary procedures, common method bias was reduced and instrument validity increased by ensuring reliability. Convergent and discriminant validity met expected cutoffs.

Organizational injustice, negative affect, attitude toward general information security policy, and attitude toward specific information security policy, represent latent variables which are "research abstractions that cannot be measured directly" (Gefen & Straub, 2005, p. 91). Additionally, because attitude determines behavior and behavior can be directly measured through ISP non-compliance, behavior was captured through participants' responses in the questionnaire. Organizational injustice, attitude toward general information security policy, and attitude toward specific information security policy construct items were measured using a calibrated five-point Likert-type scale that ranged from 1= strongly disagree, and 5= strongly agree. Negative affect construct items

were also measured using a five-point Likert scale that ranged from 1 = very slightly or not at all to 5 = extremely.

Organizational Injustice Measure

A reversed scale of Colquitt's (2001), Moorman's (1991), and Turel et al,'s (2008) organizational justice and Francis's (2005) organizational injustice measures were used to evaluate respondents' perceptions of organizational injustice. Their measures assess perceptions using distributive (in)justice, procedural (in)justice, interpersonal (in)justice and informational (in)justice dimensions. For the purpose of this study, the organizational justice scales items were reworded and reversed by converting the original Colquitt et al.'s (2001), Moorman's (1991) and Turel et al.'s (2008) scale items into negative statements. Scale items adapted from Francis and Barling (2005) were not reversed because the study measured injustice frameworks. Instead, they were reworded to suit the context of this study. This way, measures with higher scores would represent higher levels of perception of organizational injustice and not organizational justice as represented by Colquitt et al.'s (2001), Moorman's (1991) and Turel et al. (2008) original scales.

Procedural injustice was assessed using a 7-item scale that measured employees' perceived beliefs that the procedures and processes put in place to determine an outcome are unfair. For example, injustice in performance evaluations. A sample procedural injustice scale item is 'If someone lays a complaint, my organization would not follow the necessary standards and procedures to determine the outcome'. Higher scores suggest that the participant's perception of injustice with regards to the procedures put in place to determine outcome is high.

Distributive injustice was assessed using a 4-item scale. This measured the injustice employees perceive related to the belief that they do not receive benefits in proportion to the amount of effort they put on the job (outcome). For example, injustice related to pay or job promotion. A sample distributive injustice scale item is 'I am not fairly rewarded for the amount of effort I have contributed to this organization'. Higher scores suggest that the participants perceive a high injustice because the amount of benefit they receive is not proportionate to their output at work.

Interpersonal injustice was assessed using a 4-item scale. Interpersonal injustice measured the unfair treatment (e.g., politeness, dignity, and respect) employees receive from their supervisors. High scores suggest that participants are not treated with dignity or respect by their superiors.

Informational injustice which measures the availability of enough information (e.g. reasonable, timely, and specific) on how given procedures were used to determine outcomes was assessed using a 4-item scale. High scores suggest that participants do not receive enough information on how certain outcomes are determined. The table below shows the organizational injustice items and the sources where they are adapted.

Table 10

Measurement of Organizational Injustice Items

Original Item	Item for this study	Source
	Perceived Procedural injustice items	
Have those procedures been based on accurate information?	If someone in my workplace lays a complaint, my organization would not collect all accurate information necessary for decision making.	Colquitt et al., (2001); Francis, (2005); Moorman, (1999)

Table 10 (continued)

Measurement of Organizational Injustice Items

Original Item	Item for this study	Source
Have those procedures been applied consistently?	If someone in my workplace lays a complaint, my organization would be inconsistent in applying the necessary standards and procedures to arrive at the decision.	
Have those procedures been free of bias?	If someone in my workplace lays a complaint, my organization would be biased in following standards and procedures during decision-making.	
Have you had influence over the (outcome) arrived at by those procedures?	If someone in my workplace lays a complaint, my organization would not allow those affected to have influence over the decision arrived at using procedures in place.	
Provide useful information regarding the decision and its implementation.	If someone in my workplace lays a complaint, my organization would not provide useful feedback regarding the decision and its implementation.	
Allow requests for clarification about the decision.	If someone in my workplace lays a complaint, my organization would not allow for requests for clarification or additional information about the decision.	
Provide opportunities to appeal or challenge the decision.	If someone in my workplace lays a complaint, my organization would not provide opportunities to appeal or challenge the decision.	
	Perceived Distributive injustice items	
Does your (outcome) reflect what you have contributed to the organization?	I am not fairly rewarded for my contribution to this organization.	Colquitt et al., (2001); Francis, (2005); Moorman, (1999)
Is your (outcome) justified, given your performance?	I am not fairly rewarded in view of the work I have done well.	
Fairly rewarded for the stresses and strains of your job.	I am not fairly rewarded for the stresses and strains of my job.	

Table 10 (continued)

Measurement of Organizational Injustice Items

Original Item	Item for this study	Source
Does your (outcome) reflect the effort you have put into your work?	I am not fairly rewarded for the amount of effort I have put into my work.	
	Perceived Interpersonal injustice items	
The service representative treated you in a polite manner?	My supervisor does not treat me in a polite manner.	Colquitt et al., (2001); Turel et al. (2008)
The service representative treated you with dignity?	My supervisor does not treat me with dignity.	
Has (he/she) treated you with respect?	My supervisor does not treat me with respect.	
Has (he/she) refrained from improper remarks or comments?	My supervisor does not refrain from using improper remarks or comments towards me.	
	Perceived Informational injustice items	
Has (he/she) been candid in (his/her) communications with you?	My supervisor has not been candid in (his/her) communications with me.	Colquitt et al., (2001); Turel et al. (2008)
Has (he/she) explained the procedures thoroughly?	My supervisor does not explain procedures to me thoroughly.	
Were (his/her) explanations regarding the procedures reasonable?	My supervisor's explanations of the procedures to me are not reasonable.	
Has the service representative communicated details in a timely manner?	My supervisor does not communicate details to me in a timely manner.	
Has the service representative seemed to tailor communications to individuals' specific needs?	My supervisor does not seem to tailor communications to my specific needs.	

A confirmatory factor analysis (CFA) for the injustice variables was performed to ensure they are separate constructs. Overall model fit of the injustice variables was assessed using multiple fit indices - standardized root mean square residual (SRMR), normed fit index (NFI) and chi-square.

Negative Affect Measure

The Positive and Negative Affect Schedule (PANAS) scale (Watson et al. 1988) was used to assess the dispositional tendency where employees experience negative or distressing emotions characterized by sadness, fear, anxiety and lethargy discomfort across time and situation – negative affectivity. Findings from prior studies have demonstrated the validity of negative affectivity construct in measures of psychological distress (Chen et al., 2013; Panaccio et al., 2014; Salami, 2010; Thatcher & Perrewé, 2002; Watson et al., 1988). The PANAS scale consists of 10 items (words) that describe negative emotions (e.g. distressed, irritable, nervous, and jittery). Participants were asked to state the extent to which they have experienced any negative emotion at the organization over a period of time using a 5-point Likert scale from 1 = very slightly or not at all to 5 = extremely.

Table 11

Negative Affect Items

Indicate the extent to which you have felt this way since you started working at this organization.	
1. Distressed	6. Upset
2. Guilty	7. Scared
3. Hostile	8. Irritable
4. Ashamed	9. Nervous
5. Jittery	10. Afraid

Attitude Toward General Information Security Policy Measure

Attitude is an important variable that determines behavioral intentions and behavior. Ajzen (1991) defined a behavioral attitude as "the degree to which a person has a favorable or unfavorable evaluation or appraisal of the behavior in question". In the context of information security, Hu et al. (2011) expanded this definition to represent an employee's evaluation of the positive or negative effects of showing a compliant behavior towards the organization's ISP. Attitude toward general ISP was assessed using a 4-item scale adapted from Bulgurcu et al.'s (2010) attitude scale and Herath and Rao's (2009b) security policy attitude scale. The items for this construct and their source of adaptation are shown in the table below.

Table 12

Attitude Toward General Information Security Policy Items

Original item	Items for this study	Source
Adopting security technologies and practices is beneficial.	Complying with my organization's information security policy requirements is beneficial.	Bulgurcu et al. (2010) & Herath and Rao (2009b)
Adopting security technologies and practices is helpful.	Complying with my organization's information security policy requirements is helpful.	
Adopting security technologies and practices is important.	Complying with my organization's information security policy requirements is important.	
To me, complying with the requirements of the ISP is useless…useful	Complying with my organization's information security policy requirements is useful.	

Attitude Toward Specific Information Security Policy Measure

Attitude toward specific information security policy refers to context-specific practices of a particular task for example password sharing, data encryption, shutting down your computer workstation when not in use. As in the previous section, attitude

toward specific ISP was assessed using a 4-item scale adapted from Bulgurcu et al.'s (2010) attitude scale and Herath and Rao's (2009b) security policy attitude scale. For the two attitude constructs, participants were asked to indicate the extent to which they agree with each item. Scale items range from 1 = strongly disagree to 5 = strongly agree.

Table 13

Attitude Toward Specific Information Security Policy Items

Original item	Items for this study	Source
Adopting security technologies and practices is beneficial.	It is beneficial that I shut down/put to sleep my computer while temporarily away from my desk.	Bulgurcu et al. (2010) & Herath and Rao (2009b)
Adopting security technologies and practices is helpful.	It is critical that before I share any data I should encrypt (password-protect) any personal identifying information.	
Adopting security technologies and practices is important.	It is important that I do not share my password while on the job.	
To me, complying with the requirements of the ISP is useless…useful	It is important that I do not use my organization's computer for personal business.	

Information Security Policy Non-compliance Measure

The conceptual research model in this study suggests that organizational injustice, affect, and attitude toward general ISP frameworks determine ISP behavior. Because attitude determines an individual's intention and intention determines behavior, and because this study hypothesized that attitude toward specific information security policy is positively associated with information security policy compliance, the dependent variable, ISP compliance was determined directly through analysis of the four five-point Likert scale items adopted from Bulgurcu et al. (2010) and Chen et al. (2012). Scale items range from 1 = strongly disagree to 5 = strongly agree as shown on Table 14.

Table 14

Information Security Policy Non-compliance Items

Original item	Items for this study	Source
It is possible that I will follow iCorp's security policies.	I do not intend to comply with the requirements of the information security policies of my organization.	Bulgurcu et al. (2010) & Chen et al. (2012)
If I follow iCorp's security policies, the chance I would get rewarded is high.	Complying with my organization's information security policies does not increases the chances of me being rewarded.	
I intend to protect information and technology resources according to the requirements of the ISP of my organization in the future.	Protecting the IT resources according to the information security policies requirements of my organization is not very imperative for me.	
I intend to carry out my responsibilities as prescribed in the ISP of my organization when I use information and technology in the future.	It is not important that I carry out my responsibilities as prescribed in the information security policies of my organization when I use information and technology resources.	

A summary of the variables adopted for this study, with their definitions and sources, is presented in the table below.

Table 15

Summary of Variables Adopted for this Study

Variable	Definition
Independent variables	
Distributive injustice	An employee's perception of unfairness (injustices) in the distribution resources or allocation of decisions such as monetary rewards and recognitions based on outcomes (Aryee, et al., 2002; Colquitt, et al., 2001)

Table 15 (continued)

Summary of Variables Adopted for this Study

Variable	Definition
Independent variables	
Procedural injustice	An employee's perceived beliefs that the procedures and processes put in place to determine outcome are unfair e.g. perceived inequity in performance evaluation (Cohen-Charash & Spector, 2001; Colquitt et al., 2001).
Interpersonal injustice	The fairness of treatment (e.g. politeness, dignity, and respect) employees receive from the supervisors involved in process execution to determine outcomes (Colquitt et al., 2001; Turel et al., 2008)
Informational injustice	The availability of enough information (e.g. reasonable, timely, and specific) on how given procedures were used and outcomes distributed (Colquitt et al., 2001; Shapiro et al., 1994).
Attitude toward general information security policy	The relative extend of an employee's favorable or unfavorable appraisal of all information security policies (Ajzen, 1991; Herath & Rao, 2009b)
Negative affect	This reflects the tendency to which a person experiences negative or distressing emotions characterized by sadness, fear, anxiety and lethargy (Samnani et al., 2014; Watson & Clark, 1984)
Dependent variables	
Attitude toward specific information security policy	The relative extend of an employee's favorable or unfavorable appraisal of specific information security policies (Ajzen, 1991; Herath & Rao, 2009b)
Information security policy compliance intention	An employee's intention to protect the information and technology assets of the organization from potential security breaches by complying with its ISPs (Bulgurcu et al., 2010; D'Arcy & Lowry, 2019).

Instrument Validity and Reliability

Instrument validity refers to the actual measurement of what needs to be measured (Salkind, 2012). Reliability refers to "the degree to which measures are free from error and, therefore, yield consistent results" (Zikmund, 1988, p. 260). Creswell (2002) stated

that, instrument validity and reliability provide “an accurate assessment of the variable and enable the researcher to draw inferences to a sample or population” (p. 180). Subsequent research has emphasized the importance of validity and reliability by arguing that studies that lack instrument validation are not trustworthy and their findings, interpretation and conclusions lack rigor (Boudreau, et al., 2001; Straub, et al., 2004).

Instrument Validity

Straub (1989) stated that the validity of a survey instrument refers to a “prior and primary process in confirmatory empirical research” (p. 162). He further emphasized that an “instrument valid in content is one that has drawn representative questions from a universal pool” (p. 150). Meanwhile Creswell (2002) contended that, “content validity is the extent to which the questions on the instrument and the scores from the questions are representative of all the possible questions that could be asked about the content or skills” (p. 184). The importance of content validity can be justified by the fact that it removes items from variables that rely on understandable phenomenon without lowering the instrument rigor (Diamantopoulos & Winklhofer, 2001). Construct validity, on the other hand, refers to “a determination of the significance, meaning, purpose, and use of scores from an instrument” (Creswell, 2002, p. 184). It emphasizes on “whether the scores serve a useful purpose and have positive consequences when they are used in practice” (Creswell, 2014, p. 159). Meanwhile Trochim and Donnelly (2008) contended that, construct validity is the “degree to which inferences can legitimately be made from the operationalizations in your study to the theoretical constructs on which those operationalizations are made" (p. 56). For this research, an expert panel was used to validate items in the instrument and the constructs assessed. Their feedback and

recommendations were used to adjust the instrument accordingly. Construct validity was established through the factor analysis procedures.

Convergent and discriminant validity of the measurement quality of the constructs was established by analyzing pre-validated scales of the different measurements in the model (Barclay & Harland, 1995). Discriminant validity of constructs was confirmed by examining both the loading and cross-loading matrix and the correlation matrix of constructs. This research assessed discriminant validity by confirming that, (1) items on respective constructs load much higher than the items loadings on the other theoretical constructs (Chatterjee et al., 2015), and (2) by comparing the square root of the average variance extracted (AVE) for each construct with the correlation scores between any pair of construct in the correlation matrix (Bulgurcu et al., 2010; Gefren & Straub, 2005). In other words, the AVE for each construct should be higher than the correlations between that construct and any other constructs (Fornell & Larcker, 1981). Convergent validity assessed the consistency across multiple items. Gefren and Straub (2005) stated that convergent validity "is shown when *t*-values of the Outer Model Loadings are above 1.96" (p. 97), and when factor loadings are 0.60 or higher and each item loads significantly on its latent construct. This research assessed convergent validity by examining items loadings (*t*-value) on their corresponding latent construct.

Instrument Reliability

Reliability is "the consistency with which a measuring instrument yields a certain result when the entity being measured hasn't changed" (Leedy & Ormrod, 2005, p. 31). Straub (1989) stated, "reliability is a statement about the stability of individual measures across replications from the same source of information" (p. 160). Straub (1989) further

stated that, “findings based on a reliable instrument are better supported, and parameter estimates are more efficient” (p. 160). Cronbach's Alpha was used to measure the model’s internal consistency of every construct. Values for Cronbach’s Alpha range from 0.0 to 1.0, with 1.0 indicating a higher reliability of the construct. The composite reliability was confirmed if Cronbach's Alpha exceed the acceptable threshold of 0.7 (Hair, et al., 2010).

Data Collection

Ellis and Levy (2012) stated that data refers to “the purposive collection of perceived facts” (p. 407). According to Sekaran (2002), “data collection methods are an integral part of research design” (p. 223), and King and Jun (2005) deposed that, “survey research is a major presence in Information Systems (IS)” (p. 881). This research used Qualtrics as a data collection service to gather data from the sample population. The sampling approach requires several steps that include: (1) defining the population; (2) determining the sample frame; (3) determining the sampling design; (4) determining the appropriate sample size; (5) executing the sampling process (Sekaran & Bougie, 2013). For the purpose of this study, the sampling frame, which represents elements of the population required for sampling, was full-time employees of Texas Southmost College (TSC). TSC is a public two-year higher education institution located south of the state of Texas. This population is deemed necessary for this research because TSC employees use IT resources for their daily work tasks and therefore are familiar with IT security policies and procedures of the institution.

This research employed a convenience sampling technique for data collection. According to Etikan et al. (2016), convenience sampling is a “nonprobability or

nonrandom sampling where members of the target population that meet certain practical criteria, such as easy accessibility, geographical proximity, availability at a given time, or the willingness to participate are included for the purpose of the study" (p. 2). Because this technique makes assumption of a homogeneous target population, there would not be any difference in the results obtained if using a random sampling technique (Hu & Qin, 2018).

An anonymous quantitative web-based survey was distributed to employees through their TSC emails and their responses were captured in Qualtrics. One of the issues researchers deal with is how to encourage participants to fully complete and provide honest responses to a survey (Houston & Tran, 2001). This research adopted a non-probability snowball process (Eddy, et al., 2010) whereby employees who completed the survey were encouraged to request their friends to do so and the process repeated until the desired response count was achieved.

Data collection was done in three phases. Phase I involved a review and validation of the instrument by an expert panel. The selection of this expert group was based on their familiarity with, and management experience of the organization's IS policies and procedures. Direct emails and messages through the organization were sent to IS experts soliciting their participation on the expert panel to further validate the survey instrument. This panel included faculty members from the Computer Sciences and Computer Information Systems departments, as well as IT members from the organization. Instrument review and validation is a recommended approach in IS research because there is a lack of "clear consensus on the methods and means for determining content validity" (Straub et al., 2004, p. 387). The research instrument was sent to the

expert panel where they were tasked with validating observed items or variables that were used for data collection. Their assessment determined whether the items reflect the construct being measured (Skinner et al., 2015) and the feedback received was used to improve the research instrument.

Following modifications to the instrument using feedback from the expert panel review, phase II was launched, and it constituted a pilot study using the modified survey instrument. The pilot test was conducted on a selection of 20 employees representing a cross-section of the target population. Emails were sent through their organization accounts soliciting participation in the pilot test. As recommended by Anderson and Gerbing (1991), Hinkin (1998) and Milne and Bahl (2010) following an expert panel review, a pilot study can further establish the "content validity of scores on an instrument and to improve questions, format, and scales" (Creswell, 2014, p. 161). Feedback received from participants of the pilot study was used to make improvements on the survey instrument.

Phase III was the main data collection phase where the survey was administered to participants through Qualtrics. Upon approval from Nova Southeastern University's Institutional Review Board (IRB), and the survey site's IRB, an email invitation, which include a consent form, was sent to participants. Ensuring a sufficiently large sample size was preeminent in this study. Determining the necessary sample size in this study adopted the statistical power analysis as recommended by Cohen (1992), and the a priori analysis method using *G*Power* software (Mayr et al., 2007). The statistical power analysis method is more appropriate for research involving more than two variables (Cohen, 1988), thus a convenient tool for this study. It examines the relationship between

variables like sample size (N), significance criterion (α), effect size of the population (ES), and the statistical power.

Faul et al. (2009) stated that "the necessary sample size is computed as a function of user-specified values for the required significance level α, the desired statistical power 1-β, and the to-be-detected population effect size" (p. 1149). Though Weston and Gore (2006) concluded that "there is no consensus [in sample size], except to suggest that missing or nonnormally distributed data require larger samples than do complete, normally distributed data" (p. 734), Pinsonneault and Kraemer (1993) argued that exploratory research need a sample size "sufficient to test categories in the theoretical framework with statistical power" (p. 12). Subsequently, using the medium effect size convention ρ of 0.3 (Cohen, 1988), significance level α of 0.05, and a desired statistical power 1-β of 0.95, would guarantee a desired sample of at least 111 participants from a pool of 397 employees. This minimum sample was sufficient for this research.

Data Analysis

In an attempt to address the research questions, a number of statistical analyses were performed. Partial Least Square-Structural Equation Modelling (PLS-SEM) was used to explore the relationships between the dependent and independent variables. PLS-SEM is the technique of choice for IS research especially where the main objective is to predict and explain the outcome construct (Gefen & Straub, 2005; Hair et al., 2014; Levy & Danet, 2010). PLS-SEM is a "collection of statistical techniques that allow a set of relationships between one or more independent variables (IVs), either continuous or discrete, and one or more dependent variables (DVs), either continuous or discrete to be examined" (Ullman & Bentler, 2003, p. 661). SEM consist of the measurement model

and structural (regression) model (Hair et al., 2017). It is used to measure the overall data fit to the model and to determine the relationships that exist amongst variables. While "the measurement specifies how latent variables (or constructs) are measured, the structural model shows how the latent variables are related to each other" (Hair, et al., 2017, p. 13). PLS was used to determine the significance of relationships (variance) and their resulting R-squared (R^2) (coefficients of determination). Path analysis examined the relationship between perceived organizational injustice constructs, attitude towards general information security policy, negative affect (IVs) and their impact on attitude toward specific information security policy, and its impact on information security policy non-compliance behavior (DV).

Resources

This study needed an institutional review board (IRB) approval from the Nova Southeastern University IRB because human subjects were involved for data collection. Access to the survey instrument required a select group of IT security experts to review and validate the appropriateness of the survey instrument from a security perspective. The Alvin Sherman Library of Nova Southeastern University was used as the main source for journal articles, peer-reviewed articles and other relevant sources of literature that were used to support this research. Qualtrics was also leveraged for survey administration and data collection, access to a computer with Word, Excel, PowerPoint, Visio, SPSS®, Smart PLS 3.0. and G*Power for statistical data analysis and presentation.

Summary

This chapter discussed the methodology that was used to conduct this research, as well as the quantitative approach used for data collection, analysis and interpretation.

This chapter also discussed the three-phase approach that was adopted for this research which include an expert panel review, development and validation of the survey instrument including measures that were drawn from existing literature (Sekaran & Bougie, 2013) (phase 1), a pilot test of the survey instrument to identify any potential problems that may arise during the main data collection (Rea & Parker, 2014; Zikmund, 2013) (Phase 2), and the data collection, analysis and interpretation (phase 3). This chapter also discussed different statistical analyses techniques like path analysis in PLS that were used to analyze the data in order to establish the relationships between the constructs as well as answer the research questions. Finally, the resource requirements for the research were discussed as a conclusion to this chapter.

Chapter 4

Results

Overview

This chapter dealt with data collection, statistical and empirical analyses of survey responses, and the results obtained for employee's information security policy non-compliance intention as affected by perceived organizational injustice, attitude towards general information security policy, attitude towards specific information security policy and negative affect. This study seeks to examine the combined influence of negative affect (negative changes in moods and emotions) and cognitive factors (e.g., employees' perceptions of workplace injustice) on employees' misuse and non-compliance with information security policies. This study examined the following questions:

RQ1: Does negative affect (emotions) influence an individual's attitude and information security non-compliance intention?

RQ2: Do perceptions of injustice influence an individual's attitude and information security non-compliance intention?

A total of eight constructs and twelve paths as embodied in the research model examined the relationships among the constructs. Organizational injustice frameworks such as perceived distributive injustice (PDI), perceived procedural injustice (PPI), perceived interpersonal injustice (PII), and perceived informational injustice (PINJ), attitude toward general information security policy (ATG), attitude toward specific information security policy (ATS), and negative affect (NAF) represent the unobservable

(latent) variables, while ISP non-compliance intention (ISPC) represent the dependent variable. Altogether 38 items were used to measure the latent variables. According to Safa et al. (2016), a structural model examines the relationships between latent variables and a measurement model measures the relationships between the dependent variable and the independent variables. These two models were assessed for validity and overall fitness of the research model in this study.

Phase 1 - Expert Panel Validation of Survey Instrument

Phase 1 of the study employed the Delphi approach, which tasks experts with assessing the validity of the survey instrument (Olson, 2010). Saunders, Lewis, and Thornhill (2009) argued that before a survey is administered to the target population, the questionnaire should be tested for any inaccuracies, biases, vagueness, dual meaning, and built-in or systematic errors. To ensure validity, a team of experts was requested to vet the survey instrument by exploring the operational representations of the model's theoretical constructs and providing feedback on the clarity, conciseness, content, and ease of understanding the items in the answer choices (Dolnicar, 2003). The team of 15 professionals constituted a Vice President of Information Technology, an Associate Vice President of Instruction, a Chief Information Officer, Information Security and Network Specialists (3), an Executive Director of Institutional Research and Compliance, Computer Science faculty members (3), Human Resource Employee Relations Specialists (2), and Doctoral Students (3). The expert panel identified potential issues with phrasing in some of the item statements, the reversed scale in the instrument, wording and structure of the scenarios, and recommended some changes. Further recommendations by the panelists included the following:

- To remove doubt from the survey taker perhaps you may want to add in the narrative what is an “information security policy”.
- You might consider using gender neutral names to combat gender biases that other researchers have found when asking questions with male or female names.
- Please use the scale below to rate the extent to which you agree or disagree with the statements as follows: List out the entire numeric scale beginning with “5”, not “1”.

Based on their feedback and recommendations, the required changes were made to the survey instrument.

Phase 2 - Pilot Study

Following Lewis-Beck et al. (2003) recommendations, a pilot survey was conducted to test for the internal consistency reliability of the latent variables before any data collection. The pilot study also tested whether all participants responded to the questions in a similar manner. Kieser and Wassner (1996) suggested the use of between 10 – 20 participants for a pilot sample size in order to achieve meaningful differences among groups. For this research, a convenience sample of 20 participants was conducted. The 20 participants included a cross-section of the population of interest from the data collection sites, friends, family relations and professional colleagues working as administrators at other higher education institutions. The survey was sent to participants through email and participants were asked to provide feedback after taking the survey on the clarity, comprehension, ambiguity, wording and length of the survey. Results from the pilot test indicated that participants had a good understanding and interpretation of the questionnaire. In addition, one response from the pilot study was submitted with a

missing data value. Consequently, all questions in the survey were marked as ‘forced response’ in order to avoid having any missing data values. Other changes and adjustments were made to the survey with grammatical and wording mistakes corrected. Feedback from participants also indicated that the estimated completion time falls within 10 minutes or less as earlier anticipated.

Data obtained from the pilot survey were analyzed using IBM SPSS v27, and Cronbach's Alpha was used to measure the model’s internal consistency of every construct. Gefen et al. (2000) and Straub et al. (2004) indicated that a Cronbach Alpha of 0.700 is considered acceptable. Results of the reliability analysis of the pilot study showed that items in the instrument measured consistently for each of the following scales: perceived distributive injustice (PDI) = 0.893, perceived procedural injustice (PPI) = 0.859, perceived informational injustice (PINJ) = 0.875, perceived interpersonal injustice (PII) = 0.747, attitude towards general ISP (ATG) = 0.848, and negative affect (NAF) = 0.887. The Cronbach’s Alpha for attitude towards specific ISP (ATS) and ISP non-compliance (ISPC) were 0.662 and 0.676 respectively, and therefore deemed not acceptable. The Cronbach’s Alphas of ATS and ISPC were affected by a low inter-item correlation of ATS2 and ISPC1. Removing these two items from their measures raised the Cronbach Alpha values to 0.712 and 0.705 respectively.

Phase 3 - Data Collection

The main data collection for this study was conducted using a survey hosted by Qualtrics and administered online through convenience sampling. The data collection lasted two months, from December 2020 to January 2021. Prior to the main survey distribution, the IT office was contacted and informed of the scheduled survey distribution after IRB request for approval was granted (Appendix B). The IT Systems Administrator then sent out an email blast to all participants on the list informing them of the scheduled survey delivery, and to clarify any concerns that may be raised about the authenticity of the email. A day after the email from the Systems Administrator, an email invitation to participate in the survey was sent to 397 full-time employees of the organization with the web-based survey link attached to the email. The cross-sectional approach was used for data collection and deemed appropriate for this research because, unlike the longitudinal approach, the data was not collected at different points in time.

Different authors and industry reports have provided baseline data with respect to expected participant response rates during survey administration. Fryrear (2015), from SurveyGizmo, stated that a 10-15% response rate is an expected average response rate for an external survey, while Baruch & Holtom (2008) reported high rates of 35.7%. There were 135 participants who responded to the survey, giving a response rate of 34%. Because all questions in the survey were marked as “forced response” (required), some participants exited the survey after accepting to participate. Upon further review, 18 of the 135 responses were deemed unusable and therefore were not considered for analysis, leaving us with 117 valid responses. The valid 117 responses represent a 5.4% increase

from the projected 111-sample population using statistical power analysis test from *G*Power* tool and the size of the organization.

Of the 117 participants, two records with extreme outliers were deleted, leaving us with 115 records for analysis. Amongst the 115 records remaining, a significant number of them (71, 61%) were males and 44 (38.2%) were females. Most of the respondents (65%) fall within the 30 – 39 and 40 – 49 age groups and majority of them (71.8%) hold a bachelor's and master's degree. Descriptive statistics of the respondents' demographics are shown in Table 16

Table 16

Respondents' Demographics

Variables		Frequency	Percent
Gender	Male	71	60.7%
	Female	44	38.2%
Age Group (Years)	20 -29	7	6.1%
	30 - 39	32	27.4%
	40 - 49	44	37.6%
	50 - 59	17	14.5%
	60+	15	13.0%
Highest Level of Education	Some College	4	3.5%
	Associate Degree	12	10.4%
	Bachelor's Degree	40	34.2%
	Master's Degree	44	37.6%
	Doctoral Degree	14	12.0%
	Professional Degree	1	0.9%

N = 115

Pre-Analysis Data Screening

According to Levy (2006), "pre-analysis data preparation deals with the process of detecting irregularities or problems with the collected data" (p. 150). Levy suggested four reasons why pre-analysis data screening is important: ensure data accuracy,

eliminate missing data, eliminate response set biases, and to mitigate outliers. Mertler and Vannatta (2013) emphasized the significance of conducting a pre-analysis of the collected data in order to ensure its accuracy before any statistical analysis is performed. Before analyzing the main data, a pre-analysis process was performed where the data were reviewed for any missing data. A visual inspection of the data was conducted to make sure there are no response-set biases that could lead to invalid conclusions (Mangione, 1995). All items that have 100% of responses with the same value were deleted. Because all items on the survey were marked as required, the possibility of having responses with missing data was also eliminated. Using IBM SPSS, descriptive statistics were performed to identify any missing values, analyze outliers, calculate the mean, mode, median, standard deviation and check for normality. Detailed results of skewness and Kurtosis and the descriptive properties of the dataset are presented in Appendix C.

A multivariate reliability test using Mahalanobis distance was conducted to identify any multivariate outliers. Mahalanobis distance is defined as the distance of a case from the centroid of the remaining cases where the centroid is a point created by the means of all variables (Levy, 2006, p. 152).

Mahalanobis Distance and Box Plot

The Mahalanobis distance methodology differentiates groups of multivariable data by a univariate distance measure, calculated from the assessment of multiple parameters. The Mahalanobis distance value is determined by normalizing performance parameters and their coefficients of correlation (Taguchi et al., 2001). The Mahalanobis distance test measures the distance between a distribution and a point using a Chi-square

(χ^2) distribution (Mahalanobis, 1936). The degree of freedom (df) represents the number of independent variables (Tabachnick et al., 2007). An average function was used to create a subset of independent variables by aggregating all items to their respective independent variable.

The Mahalanobis distance test was performed to detect and eliminate any multivariate outliers. This study examined 7 independent variables (used as the degree of freedom, *df*) to calculate the critical value. Mertler and Reinhart (2017) stated that "the accepted criterion for outliers is a value for Mahalanobis distance that is significant beyond $p < .001$, determined by comparing the obtained value for Mahalanobis distance to the Chi-square critical value" (p. 31). Using a Mahalanobis distance test in SPSS, data were assessed to identify any multivariate outliers. The critical value of the Chi-square at $p < .001$ and degree of freedom (df) = 7 yields a Mahalanobis distance of 24.322 based on the Chi-square distribution table (Appendix D). Results from the first Mahalanobis distance test showed that there were 10 outliers from five cases (Case Number 44, 39, 29, 104, and 66). Upon further review, two records (Cases 39 and 44) with a Mahalanobis distance greater than 24.322 were identified and considered for removal from the study. However, Mertler and Vannatta (2001) stated that due to their potential significance in the study, some outliers should not be automatically eliminated from the study but should be reassessed for inclusion in further analysis. A rerun of the Mahalanobis distance with the remaining 115 cases generated eight extreme values in cases 29, 104, 66, 51, and 56 (see Appendix E).

Normality test

A test of normal distribution was conducted using standard Skewness and Kurtosis following the analysis of outliers. During the first Mahalanobis distance analysis, Skewness and Kurtosis values were 1.820 and 4.155 respectively. Guidelines established by Hair et al. (2017) showed that the acceptable threshold for a distribution to be normal is if the Skewness and Kurtosis results fall between -1 and +1. Results from the first Mahalanobis test showed that the data were not normally distributed. A rerun of Mahalanobis distance after the two extreme outliers were deleted reduced the Skewness and Kurtosis values to 1.297 and 1.325 respectively. To continue the test for normality, Tabachnick and Fidell (2019) suggested that a visual assessment of graphical and statistical outputs not limited to values of Skewness and Kurtosis should be conducted to check for normality. The bell-shaped curve on the histogram (Appendix F) indicates the curve of data normality. In addition, cases close to the diagonal line of the normal Q-Q plot (Appendix E) and P-P plot of regression standardized residuals (Appendix F) certainly follow the line of regression, and the rectangular shape of the scatter plot (Appendix E) all confirm normality of the data distribution (Ghasemi & Zahediasl, 2012).

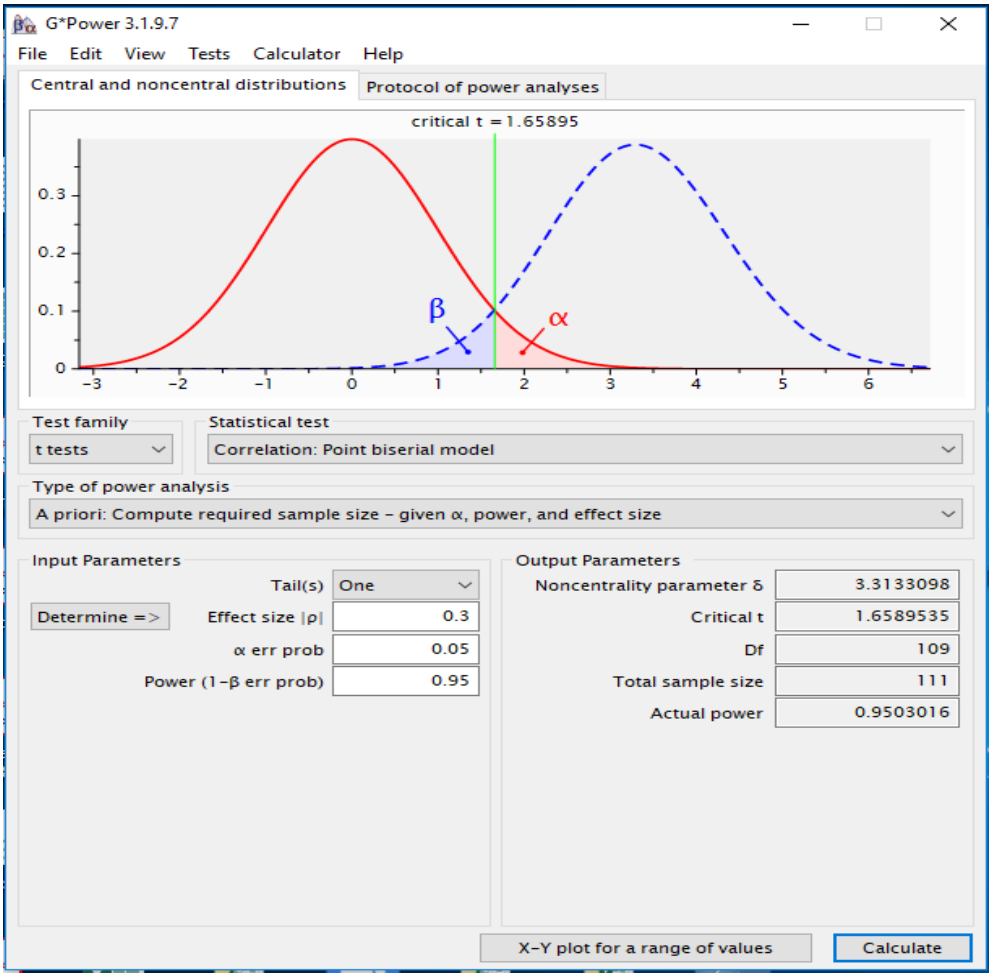
Data Analysis

Data analysis for Partial Least Square Structural Equation Modeling (PLS-SEM) was conducted with the use of Smart PLS 3.0 as described by Hair et al. (2019) and Wong (2013). Hair et al. (2014) noted that PLS-SEM is a widely used statistical approach in IS studies because of its ability to assess the measurement of constructs, while evaluating causal relationships. Gefen et al. (2000) also pointed out that PLS-SEM is a valuable technique for prediction-oriented and theory building research as it is designed

to explain variance among variables and their resulting R-squared (R2) or coefficients of determination. Li et al. (2011) stated that, "PLS requires a much smaller sample size than other structural equation modeling (SEM) techniques" (p. 439). To validate this statement, the projected sample population needed for PLS analysis was calculated using *G*Power 3.1.9*. The minimum projected sample was 111 and was calculated using effect size of 0.5, significance of 0.05, and desired power level of 0.95. Results from the analysis are shown in Figure 6.

Figure 6

*Results of Sample Size Analysis in G*Power*



Construct Reliability and Validity

Assessing the measurements in this research required the use of Smart PLS algorithm to conduct tests on discriminant validity, construct validity and reliability, outer loadings, cross-loadings, model fit, bootstrapping and path coefficients. Average variance extracted (AVE) and Cronbach's Alpha were used to measure convergent validity and internal reliability consistency respectively. Straub et al. (2004) stated that "reliability assesses the confidence that the measuring instrument will yield the same results when subjected to the same measurement" (p. 426). According to Sekaran and Bougie (2013), Cronbach Alpha (*a*) is a "reliability test that examines the consistency of respondent's answers to all the items in a measure" (p. 229). Values of Cronbach alpha range between 0.0 to 1.0, with 1 indicating a higher reliability of the construct. The composite reliability will be confirmed if Cronbach's alpha exceeds the acceptable threshold of 0.7 (Hair et al., 2010). Cronbach's alphas were run to ensure scale reliability with results. All measures, except PII (0.643) and ISPC (0.619) which were not considered reliable, produced a strong reliability score with a significant Cronbach alpha above the acceptable 0.7 (see Appendix H). The Cronbach alpha for PII increased to 0.9405 when latent variables PII1 (-0.026) and PII2 (0.009) were deleted. However, the Cronbach alpha for ISPC (0.628) remained below 0.7 even after ISPC4 (0.401) was deleted and the algorithm reran. Hair et al. (2014) posited that the internal consistency reliability is often underestimated because Cronbach's alpha is strongly related to the number of items in each scale, and that exploratory research consider Cronbach alpha of 0.60 to 0.70 acceptable values. Conversant with this shortcoming, composite reliability was used to measure the internal consistency reliability. A rerun of the PLS algorithm

improved composite reliability of the constructs to acceptable values above 0.7 (Appendix J) as proposed by Bagozzi and Yi (1988).

Results of the PLS algorithm were also used to determine if values of factor outer loadings were acceptable. Hair et al. (2017) stated that for an indicator to account for more than 50% of variance, the value of its factor outer loading should be higher than 0.7. Subsequently, loadings greater than 0.7 were considered reliable for this research. However, to improve on the validity and reliability of this research, the following indicators ISPC4 (0.401), NAF2 (0.584), NAF3 (0.677), PII1 (-0.026), and PII2 (0.009) were deleted and the algorithm was run again. Results of the measurement show that all factor outer loadings were greater than 0.7 as shown in Table 17, except for ISPC2 with a factor loading of 0.530. Deleting ISPC2 would inadvertently reduce the rho_A reliability coefficient of ISP non-compliance to below the acceptable value of 0.7. In addition, Hulland (1999) concluded that for a latent construct to be reliable, its indicators loading should be greater than 0.5. Against this backdrop, ISPC2 was considered reliable for this research.

Table 17

Factor Outer Loadings

	ATG	ATS	ISPC	NAF	PDI	PINJ	PII	PPI
ATG1	0.912							
ATG2	0.919							
ATG3	0.875							
ATG4	0.932							
ATS1		0.735						
ATS2		0.769						
ATS3		0.864						
ATS4		0.823						
ISPC1			0.839					
ISPC2			0.530					
ISPC3			0.856					

Table 17 (continued)

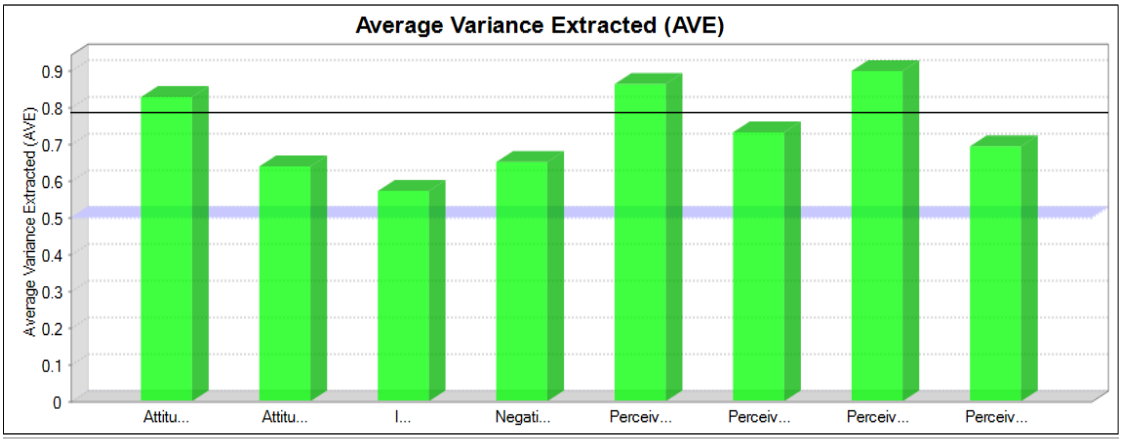
Outer Loadings

	ATG	ATS	ISPC	NAF	PDI	PINJ	PII	PPI
NAF10				0.726				
NAF4				0.718				
NAF5				0.749				
NAF6				0.741				
NAF7				0.905				
NAF8				0.895				
NAF9				0.885				
PDI1					0.931			
PDI2					0.954			
PDI3					0.909			
PDI4					0.922			
PINJ1						0.778		
PINJ2						0.897		
PINJ3						0.788		
PINJ4						0.884		
PINJ5						0.920		
PII3							0.946	
PII4							0.950	
PPI1								0.768
PPI2								0.797
PPI3								0.810
PPI4								0.923
PPI5								0.844
PPI6								0.847
PPI7								0.835

Convergent validity is established when the scores obtained with two different instruments measuring the same concept are highly correlated (Sekaran & Bougie, 2013, p. 227). Trochim and Donnelly (2008) defined convergent validity as "the degree to which concepts that should be related theoretically are interrelated in reality." (p .68). According to Chin et al. (2003), when the AVE of items' loadings is 0.5 or higher, convergent validity is acceptable. As shown in Figure 7, the minimum threshold values for AVE were all surpassed, confirming convergent validity.

Figure 7

Average Variance Extracted



Further analysis of results of construct reliability and validity test showed that AVE values for all constructs were above 0.5 and therefore considered reliable. Results from AVE, composite reliability, and Cronbach's alpha support the convergent validity of measurement items used in this study (see Table 18 below, and Appendices I and J).

Table 18

Construct Reliability and Validity

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Attitude towards General ISP	0.931	0.942	**0.951**	0.828
Attitude towards Specific ISP	0.812	0.828	**0.876**	0.639
ISP Non-Compliance	0.628	0.707	**0.794**	0.572
Negative Affect	0.911	0.958	**0.928**	0.651
Perceived Distributive Injustice	0.947	0.952	**0.962**	0.863
Perceived Informational Injustice	0.918	0.918	**0.932**	0.732
Perceived Interpersonal Injustice	0.888	0.889	**0.947**	0.899
Perceived Procedural Injustice	0.932	1.141	**0.941**	0.694

After deleting indicators ISPC4 (0.401), NAF2 (0.584), NAF3 (0.677), PII1 (-0.026), PII2 (0.009)

Discriminant Validity

Discriminant validity is the extent to which constructs in a model are not related. Henseler et al. (2015) deposed that "discriminant validity ensures that a construct measure is empirically unique and represents phenomena of interest that other measures in a structural equation model do not capture" (p. 116). Discriminant validity is determined when the value for cross-loading for each variable is greater than the cross-loading value with other variables (Chin, 1998). Cross-loadings and the Fornell-Larcker criterion, including the Heterotrait-Monotrait (HTMT) test, were used to assess for discriminant validity. The Fornell-Larcker criterion compares the square root of AVE with the correlation of latent variables. This method depicts that a latent variable should express a high variance of its own indicator when compared to the variance of other variables (Hair et al., 2014). Therefore, the square root of a construct's AVE should be greater than the values of inter-construct correlation (Fornell & Larcker, 1981). Results of the Fornell-Larcker criterion are presented in Table 19.

Table 19

Fornell-Larcker Criterion

	ATG	ATS	ISPC	NAF	PDI	PINJ	PII	PPI
Attitude towards General ISP (ATG)	**0.910**							
Attitude towards Specific ISP (ATS)	0.643	**0.800**						
ISP Non-Compliance (ISPC)	-0.370	-0.300	**0.756**					
Negative Affect (NAF)	-0.205	-0.004	0.381	**0.807**				
Perceived Distributive Injustice (PDI)	-0.070	-0.050	-0.119	0.200	**0.929**			
Perceived Informational Injustice (PINJ)	-0.059	0.043	-0.128	0.150	0.379	**0.856**		

Table 19 (continued)

Fornell-Larcker Criterion

	ATG	ATS	ISPC	NAF	PDI	PINJ	PII	PPI
Perceived Interpersonal Injustice (PII)	0.319	0.254	-0.351	-0.120	-0.034	0.068	**0.948**	
Perceived Procedural Injustice (PPI)	0.036	0.132	-0.069	0.206	0.387	0.465	0.078	**0.833**

Guidelines provided by Fornel and Larcker (1981) were used to assess discriminant validity by comparing the correlation coefficients of each construct with the square root of each AVE in the diagonal. Results referenced in Table 18 showed that the square root of AVE for each construct exceeded the higher value of the inter-construct correlations between that construct and any other construct in the model. Overall, discriminant validity was evident among the measurement items in this model and therefore supports discriminant validity between the constructs.

Cross-loadings were also assessed for discriminant validity and the results showed that scale items were more strongly loaded on their respective constructs than other indicators (Gefen & Straub, 2005). Examining Table 18 and Appendix K it can be seen that the square root of AVE and cross-loading values are higher than their inter-construct and inter-item correlations. This therefore depicts discriminant validity in the measurement items of this study (see Table 18 and Appendix K).

A more innovative and unique approached that is used to assess discriminant validity in PLS is the Heterotrait-Monotrait (HTMT) ratio of correlations. This superior performance approach was proposed by Henseler et al. (2015) through a Monte Carlo simulation research where they concluded that HTMT can be highly specific (97% to

99%) compared to the Fornell-Lacker and cross-loadings criterion. According to Hair et al. (2019), HTMT denotes the mean of the items' cross-construct correlation relative to the mean of the average inter-item correlation for the same construct. Applying HTMT requires the use of a predefine threshold. Any HTMT values greater than this threshold will indicate a lack of discriminant validity. Some authors suggest a threshold of 0.85 (Kline, 2011), whereas others propose a value of 0.90 (Teo et al., 2008). Results of HTMT as shown in Table 20 depict discriminant validity, with acceptable HTMT values less than 0.90.

Table 20

Heterotrait-Monotrait Ratio (HTMT)

	ATG	ATS	ISPC	NAF	PDI	PINJ	PII	PPI
Attitude towards General ISP (ATG)								
Attitude towards Specific ISP (ATS)	0.723							
ISP Compliance (ISPC)	0.438	0.402						
Negative Affect (NAF)	0.204	0.090	0.450					
Perceived Distributive Injustice (PDI)	0.094	0.098	0.154	0.244				
Perceived Informational Injustice (PINJ)	0.085	0.072	0.196	0.183	0.411			
Perceived Interpersonal Injustice (PII)	0.343	0.302	0.455	0.127	0.049	0.086		
Perceived Procedural Injustice (PPI)	0.071	0.138	0.154	0.276	0.421	0.494	0.092	

Model fit

According to Levy and Green (2009), SEM is a valid approach that should be considered for confirmatory factor analysis and testing for model fit. To determine the model fit, a PLS algorithm was run and the data analyzed. A standardized root mean square residual (SRMR) is an acceptable measure used to evaluate a model fit (Hair et al., 2014), and an SRMR value less than 0.08 is indicative of a good model fit (Hu & Bentler, 1998). As noted by Hooper et al. (2008), an SRMR value of 0 is indicative of a perfect model fit; however, using a larger sample size with many parameters could lower the SRMR value below 0. Results of the PLS algorithm for model fit of this study showed that the SRMR value was 0.074 which is below the 0.080 value, thus indicating a good model fit (Hair et al., 2017) (see Table 21 and Appendix J).

Table 21

Model Fit Summary

	Saturated Model	Estimated Model
SRMR	0.074	0.074
d_ULS	3.604	3.624
d_G	1.992	1.995
Chi-Square	1180.941	1181.500
NFI	0.695	0.695

Findings

This section presents the results of data analysis in an attempt to determine if the hypotheses in this study were supported or not supported. The Smart PLS 3.0 tool was used to run a PLS-SEM data analysis through bootstrapping. Bootstrapping with a 5000 sub-sampling was conducted to assess the significance of the research model's paths, and to examine the path coefficients. The *t*-statistics (*t*-values) produced from bootstrapping

depict the degree of significance in the structural paths (see Appendix L). Path coefficients determine the strengths of relationships amongst constructs in the causal model, while R^2 values estimate the predictive strength of the model (Hair et al., 2014; Mertler & Vannatta, 2013). Values of path coefficients range from -1 to +1, with values closer to +1 depicting strong positive relationships and those closer to -1 indicating strong negative relationships. Variables with values closer to zero are generally considered to have weak relationships (Hair et al. 2014).

A PLS bootstrap was executed to test the significance of a structural path using the following recommended settings: 5000 subsamples that are drawn randomly from the original data set; bias-corrected and accelerated bootstrap; complete bootstrapping; one-tailed test type as recommended for coefficients with positive or negative sign reflected in the hypotheses; and a significance level of 0.05 (Kock, 2015). Results of bootstrapping as shown in Appendix L show that the coefficient of determination, R^2, for latent variables attitude towards specific ISP and ISP non-compliance is 0.446 and 0.344 respectively. This means that the independent variables exhibited variance towards the dependent variables with attitude towards specific ISP showing that 44% variance explained by perceived organizational injustice frameworks (perceived distributive injustice, perceived procedural injustice, perceived interpersonal injustice, and perceived informational injustice), attitude towards general information security policy, and negative affect. ISP non-compliance intention showed 34% variance that can be explained by attitude towards specific information security policy, perceived distributive injustice, perceived procedural injustice, perceived interpersonal injustice, perceived informational injustice, and negative affect (see Appendix J for the R-square output).

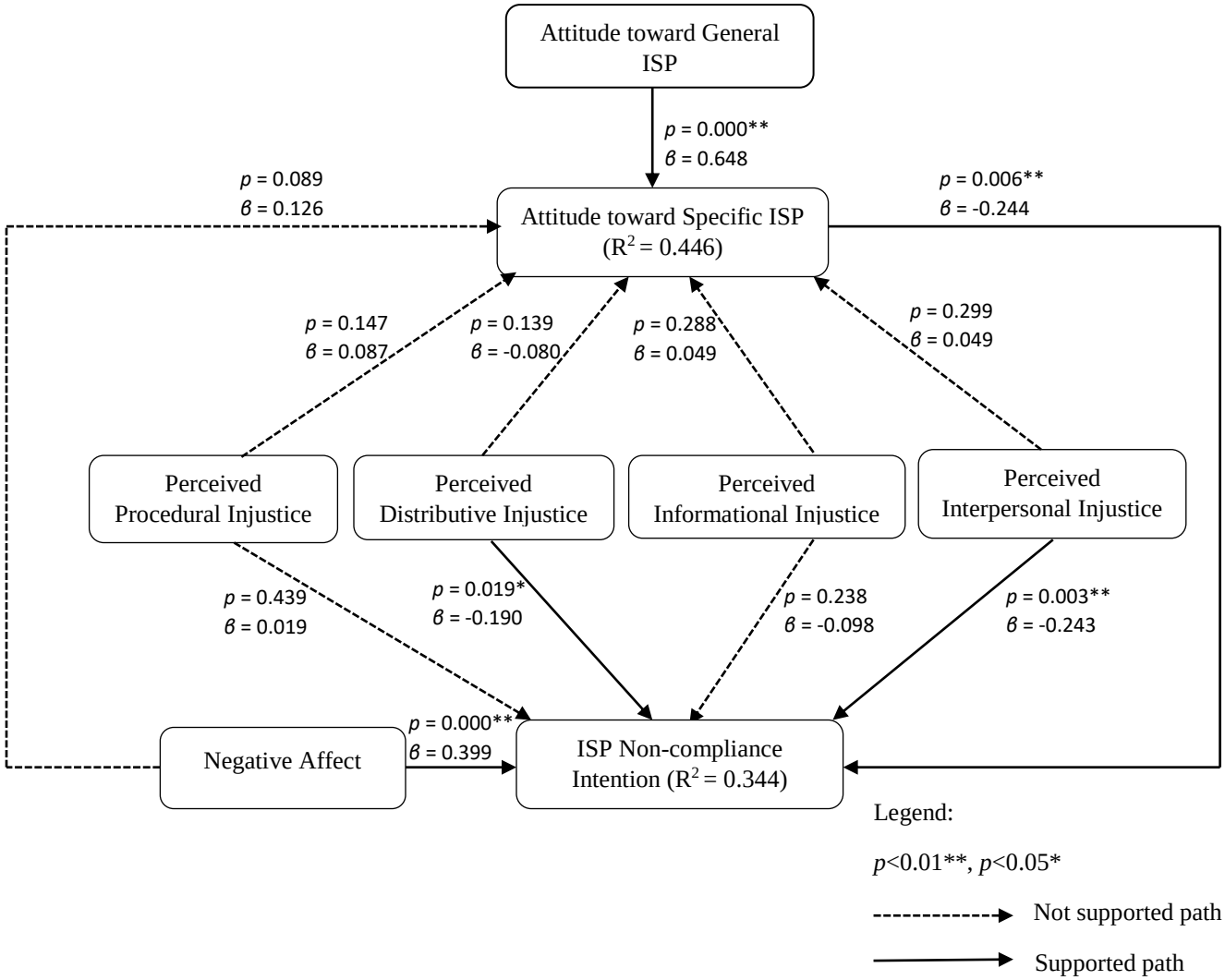
Path analysis was also performed after running PLS algorithm. Results were used to evaluate the significance of the relationships between constructs by examining path coefficients. The size of the path coefficients showed that negative affect (β = 0.399) has the strongest effect on ISP non-compliance intention, followed by perceived procedural injustice (β = 0.019), perceived informational injustice (β =-0.098), perceived distributive injustice (β = -0.190), attitude towards specific ISP (β = -0.244), and perceived interpersonal injustice (β = -0.243). Meanwhile attitude towards general ISP (β = 0.648) commanded the strongest effect on attitude towards specific ISP, followed by negative affect (β = 0.126), perceived procedural injustice (β = 0.087), perceived informational and perceived interpersonal injustices (β = 0.049), and finally perceived distributive injustice (β = -0.080). Paths with low positive values indicate weak positive relationships and paths with negative values indicate weak negative relationships (Appendix I).

Based on path analysis and results of the hypotheses testing as shown in Table 20, it can be stated that attitude towards specific ISP was not positively influenced by negative affect (t=1.348, p=0.089), perceived distributive injustice (t=1.085, p=0.139), perceived informational injustice (t=0.560, p=0.288), perceived interpersonal injustice (t=0.526, p=0.299), and perceived procedural injustice (t=1.048, p=0.147). Only attitude towards general ISP (t=6.713, p=0.000) showed to positively influence attitude towards specific ISP. On the other hand, ISP non-compliance was negatively influenced by perceived informational injustice (t=0.714, p=0.238), and perceived procedural injustice (t=0.154, p=0.439). However, attitude towards specific ISP (t=2.501, p=0.006), negative affect (t=5.269, p=0.000), perceived distributive injustice (t=2.070, p=0.019), and perceived interpersonal injustice (t=2.735, p=0.003) all exhibited positive relationships

and influence towards ISP non-compliance. Results of the PLS analysis consisting of constructs, *p*-value, *t*-statistic, and R-squared values are shown in Figure 8 below.

Figure 8

Results of PLS Path Analysis for ISP Non-Compliance Intention



Hair et al (2011) pointed out that "the individual path coefficients of the PLS structural model can be interpreted as standardized beta coefficients of ordinary least squares regressions" (p. 147). Results of bootstrapping in SmartPLS 3.0 showed that perceived distributive injustice (β = -0.080, $p < 0.05$) has a direct but non-significant influence on attitude towards specific ISP, thus **H1A** is not supported. However, when it

comes to ISP non-compliance intention, perceived distributive injustice (β = -0.190, p < 0.05) showed a significant but negative contribution, supporting **H1B.** In addition, path parameters showed that organizational injustice frameworks - perceived procedural injustice (β = 0.087, p < 0.05), perceived interpersonal injustice (β = 0.049, p < 0.05), perceived informational injustice (β = 0.049, p < 0.05), and negative affect (β = 0.126, p < 0.05), had no significant effect on attitude towards specific ISP. Therefore, **H2A, H3A**, **H4A,** and **H7** were not supported. Nevertheless, attitude towards general ISP (β = 0.648, p < 0.001) showed a strong positive influence on attitude towards specific ISP, thus supporting **H5.** In addition, the direction of the effect of perceived procedural injustice (β = 0.019, p < 0.05), and perceived informational injustice (β = -0.098, p < 0.05), on ISP non-compliance were not significant. Hence, **H2B** and **H4B** were not supported. Also, perceived interpersonal injustice (β = -0.243, p < 0.01), and attitude towards specific ISP (β = -0.244, p < 0.05) both had significant negative contributions on ISP non-compliance. Thus, **H3B** and **H6** were fully supported. Finally, results further suggested that negative affect (β = 0.399, p < 0.001) had a significant and direct positive influence on ISP non-compliance intention. Therefore, **H8** was fully supported. Summary of results of the hypotheses testing are shown in Table 22.

Table 22

Summary of Hypotheses Tests

HO	Path	Path Coefficient (β)	*t*-Values	*p*-Values	Supported
H1A	Perceived Distributive Injustice -> Attitude towards Specific ISP	-0.080	1.085	0.139	No
H1B	Perceived Distributive Injustice -> ISP Non-Compliance Intention	-0.190	2.070	0.019	Yes
H2A	Perceived Procedural Injustice -> Attitude towards Specific ISP	0.087	1.048	0.147	No
H2B	Perceived Procedural Injustice -> ISP Non-Compliance Intention	0.019	0.154	0.439	No
H3A	Perceived Interpersonal Injustice -> Attitude towards Specific ISP	0.049	0.526	0.299	No
H3B	Perceived Interpersonal Injustice -> ISP Non-Compliance Intention	-0.243	2.735	0.003	Yes
H4A	Perceived Informational Injustice -> Attitude towards Specific ISP	0.049	0.560	0.288	No
H4B	Perceived Informational Injustice -> ISP Non-Compliance Intention	-0.098	0.714	0.238	No
H5	Attitude towards General ISP -> Attitude towards Specific ISP	0.648	6.713	0.000	Yes
H6	Attitude towards Specific ISP -> ISP Non-Compliance Intention	-0.244	2.501	0.006	Yes
H7	Negative Affect -> Attitude towards Specific ISP	0.126	1.348	0.089	No
H8	Negative Affect -> ISP Non-Compliance Intention	0.399	5.269	0.000	Yes

Summary

This chapter presented the results of analysis conducted on the primary data collected from the measurement instrument, and the structural analysis conducted using IBM SPSS for pre-analysis of the data, and SmartPLS for the main data analysis. Instrument validation included an expert panel review and validation of the research

instrument through a Delphi approach, and a pilot study to ensure reliability of the survey instrument. Results of the pilot study showed that the instrument was reliable, and no further modifications of the instrument were made. Finally, the main data collection and results of analysis for measures that addressed the hypothesized relationships was presented, including tests for the reliability and validity of the constructs, as well as establishing a fit for the model. The measurement model was tested to be an acceptable fit, and the structural model was tested using latent variable scores generated though PLS algorithm.

Based on initial results of validity and reliability, two items were deleted from the model and the refined model was tested for measurement and structural relationships using SmartPLS. Of the twelve hypotheses in this research, results from running a PLS bootstrapping procedure showed that five had a significant influence on employees' attitude towards specific ISP and ISP non-compliance, and therefore were fully supported. The remaining seven hypotheses showed no significant influence on attitude and non-compliance behavior, hence they were not supported. Detailed discussions of these findings and conclusions are presented in the next chapter.

Chapter 5

Conclusions, Implications, Limitations, and Summary

Overview

Many institutions consider their employees to be a great assert in their efforts to mitigate risks associated with information security threats and policy non-compliance. Findings from numerous information security studies have demonstrated that information security violations caused by the unethical actions of disgruntled employees and other insiders with legitimate access rights to information systems pose an even greater financial burden and the costliest risks to an organization (Cole, 2015). Given that employees with legitimate access privileges have a good knowledge of organizational processes (Willison & Warkentin, 2013), the question becomes therefore how to mitigate insider threats posed by these employees. The main objective of this study was to examine the influence of organizational injustice and negative affect on employees' non-compliance with IS policies. Specifically, the researched focused on perceived injustice frameworks and negative changes in moods and emotions and their relationship with attitude towards specific ISPs and ISP non-compliance behavior. Findings from the data collected (see Table 20) are discussed in this chapter. This chapter also discussed the study limitations and practical implications.

Discussion

This research empirically examined the combined influence of perceived organizational injustice frameworks (distributive injustice, procedural injustice,

informational injustice, and interpersonal injustice), and negative affect on employees' attitude and non-compliance behavior with organizational information security policy. Based on data collected from 115 employees who have sufficient knowledge and familiarity with requirements of their institution's ISPs, results of this study are presented in Table 20. As depicted from results of the survey, perceived distributive injustice was not found to be negatively related to attitude towards specific ISP (**H1A**). This result contradicts Sulu et al. (2010) who found a weak but rather positive relation between distributive injustice and employee's intended attitude towards safeguarding certain specific ISPs of the organization. This lack of support as hypothesized in **H1A** can be explained by the fact that distributive injustice is more related to an individual's perception of the ratio of their job contributions and performance rewards to the outcome ratio of their colleague (Willison & Warkentein, 2013), and not necessarily to any specific ISP. Another interpretation of the lack of support could be that some employees react to perceived distributive injustice by adopting a less cynical attitude toward the organization's specific ISPs.

Furthermore, consistent with prior studies, the results of analysis showed that employees with strong perceptions of distributive injustice demonstrate higher ISP non-compliance and abusive behavior (**H1B**). The study by Syed, Naseer and Bouckenooghe (2020) on "the unfairness in stressful job environments…." found that employees with strong perceptions of distributive injustice relatively have greater ISP non-compliance and unethical behavior. Similarly, Khattak et al. (2020) on "the combined effect of perceived organizational injustice and perceived politics on deviant behaviors", also showed that employees who perceive high distributive injustice (unfair treatment) from

their immediate leadership are more susceptible to engage in unethical and deviant behaviors such as ISP non-compliance aimed at their organization. This employee response is significant in that supervisors who promote these feelings of injustice, and organizational actions which create employee distributive injustice and motivate aggression, could equally feel the brunt of retaliation from disgruntled employees. Thus, consistent with findings highlighted in prior studies, this finding emphasizes the position that perceived distributive injustice is a more significant antecedent in employees' ISP non-compliance attitude and behavior (Aryee et al., 2002; Colquitt et al., 2001; Elovainio et al., 2004).

Perceived procedural injustice was also found to have no significant influence on attitude toward specific ISP (**H2A**) and subsequently on ISP non-compliance intention (**H2B**). This result was contrary to findings from Cohen-Charash and Spector (2001), and Sarwar and Mohamed (2020) who argued that procedural injustice has a negative but significant influence and therefore a job stressor to employees' performance. The interpretation here is that perceived procedural injustice has no influence in altering the relative extend of an employee's favorable or unfavorable attitude of appraisal towards ISP non-compliance (Ajzen, 1991; Herath & Rao, 2009b). One probable reason for the insignificant relationship between perceived procedural injustice on attitude toward specific ISP and subsequently on ISP non-compliance from this study can be explained by the significant influence perceived distributive injustice has on employees' ISP compliance intention. Hence their focus on equity of resource distribution and not on procedures. Employees may believe they are being compensated through perks and rewards based on their job contribution (ability and capability), and not necessarily on

their attitude towards the organization's IS policy. Therefore, if they perceive any procedural injustice, they believe their performance may not be affected by their feeling of dissatisfaction or resentment towards the organization irrespective of how favorable the outcome is, but rather on their perceived beliefs that they do not receive benefits in proportion to the amount of effort they put on the job (Hubbel & Chory-Assad, 2005).

Contrary to results from prior studies (Khattak et al., 2020), this study found that perceived interpersonal injustice had no significant influence on attitude toward specific ISP (**H3A**). One possible explanation of this finding is that employees' beliefs of interpersonal injustice, same as procedural injustice, may have no influence on their feeling of resentment and rage towards their supervisors and the organization and their intention to demonstrate unwanted and unethical behavior at the workplace. Results from the agent-system model by Masterson et al., (2000), showed that procedural injustice, amongst other forms of organizational injustice, accounted for the most variance in counter-productive workplace behavior, and of the three organizational justice frameworks, perceived interpersonal injustice has a significantly strong effect on negative attitudes (Colquitt, 2001). It is obvious from this result that employees' attitude towards ISP outweighs their perceived belief of interpersonal injustice. It can thus be inferred from this result that when employees are confident of their attitude, their perception of any unfair treatment from their supervisors involved in process execution to determine outcomes (Colquitt et al., 2001) will have no significant influence on their intended ISP attitude.

However, there was a significant influence of interpersonal injustice on ISP non-compliance behavior (**H3B**), which was consistent with findings from theoretical studies

(Jones, 2009; Mitchel & Ambrose, 2007; Lavelle et al., 2007) and meta-analytic research on the effects of injustice on organizational citizenship behavior (Fassina et al., 2008). For example, this result corroborated findings from Jones (2009) when they found that interpersonal injustice strongly predicts counter-productive workplace behavior, and Lavelle et al. (2007) demonstrated that interpersonal injustice accounted for more unique variance in employee behavior than other forms of injustices.

Perceived informational injustice as shown by the results, did not influence employees' attitude toward specific ISP (**H4A**), simply for the same reasons mentioned in the previous sections on the insignificant influences of distributive, procedural and interpersonal injustices on attitude towards specific ISP. Likewise, from an ISP non-compliance perspective, perceived informational injustice was found not to have a significant influence on employees' ISP non-compliance behavior (**H4B**). This outcome is very much consistent with previous studies. Li et al. (2014) in "exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance" found out that informational injustice has no direct significant impact on employees' internet use policy compliance intention. Li et al. (2014) noted that the absence of any statistical significance of perceived informational injustice could be attributed to the shallow relationships and limited daily interactions between employees and managers who are responsible for enforcing IS security policies. Previous marketing research suggest that the effect of informational injustice could be subdued by that of distributive injustice in the presence of a limited employee-manager relationship (Hoffman & Kelley, 2000). That is, the consequences of informational injustice relating to ISP misuse were not perceived by employees to be severe.

Results from the analysis also indicated that, for disgruntled employees, attitude toward general ISP leads to attitude, whether positive or negative, toward specific ISP (a significantly direct positive influence), as well as intended ISP non-compliance behavior (**H5 and H6**). These results were found to be in conformity with findings from prior literature. Bulgurcu et al. (2010) deposed that the effects of attitude on employees' IS policies non-compliance intention are incredibly significant. Based on a TPB framework, Bulgurcu et al. (2010) argued that beliefs surrounding the appraisal of consequences will affect an employee's overall compliance attitude and intended behavior. In other words, attitude is presumed to influence an employee's ISP non-compliance intentions. Still from a TPB perspective, Hu et al. (2012) found a stronger support of individual attitude towards behavioral intention to comply with IS policies. Puhakainen and Siponen (2010) observed that supervisor participation in employees' attitude has a direct significant impact on employee ISP compliance behavior. Thus, attitude is highly influenced by personal and direct communications between employees and managers, and this affects employees' compliance intention with IS policies.

Apparent from this research is the finding that employees who experience negative affect (negative feelings and emotions like fear, anger, anxiety) have a likelihood to engage in counterproductive or deviant workplace behavior **(H8)**. The results provide evidence that negative affect positively influences ISP non-compliance behavior, which is consistent with findings from prior studies (Chen et al., 2013; D'Arcy & Lowry, 2019; Samnani et al. 2014). Chen et al. (2013) in their examination of the relationship between employees' negative affect and workplace deviance, concluded that negative affect has a strong positive effect on employees' workplace deviant behavior.

Similarly, D'Arcy and Lowry (2019) found that negative affect had a strong significant relationship with employees' attitude and subsequent behavior with IS policies compliance. According to Dalal et al. (2009), individuals who go through negative feelings and emotions will try to mend this negative affective state when they engage in deviant behavior at the workplace. Thus, explaining the strong positive influence of negative affect on employees' ISP non-compliance as found in this study. However, it was found that negative affect did not influence attitude toward specific ISP as expected **(H7)**. This lack of significant support between negative affect and attitude toward specific ISP may be attributed to, irrespective of an employee's emotional state, the fact that an employee may consider ISPs to be particularly important. However, their actions "speak louder than their words" on grounds that they do not comply with these policies because of the emotional experiences at work.

Conclusions

This study empirically examined the behavioral influences of organizational injustice and negative affect on employees' information security policy compliance behavior. Employees' compliance with information security policies is an important socio-organizational topic (Boss & Kirsch, 2007) that represents a key information security problem for organizations. Despite the implementation of SETA and other technical and managerial programs, employees' IS policies non-compliance is still a growing concern. This research argued that employees that perceive they have been treated unfairly by their organization are likely to experience strong emotions as fairness perceptions directly or indirectly influence their emotions. Thus, strong emotions may be a recipe for an individual's deviant behavior contrary to their self-interests due to their

deep involvement with their emotions. Using pre-kinetic and rationality-based behavioral theories like neutralization, theory of planned behavior, deterrence, and organizational injustice, this research introduced a theoretical conceptual model to help with understanding how organizational injustice frameworks and negative affect influence employees' attitude and non-compliance behavior with IS policies.

The conceptual model of ISP non-compliance was measured using perceived organizational injustice frameworks like distributive injustice, procedural injustice, informational injustice, and interpersonal injustice, as well as items established for the negative affect and attitude towards IS policy constructs. Validating the theoretical model required the application of Partial Least Square Structural Equation Modeling (PLS-SEM) technique through the use of SmartPLS and Confirmatory Factor Analysis (CFA). PLS was used to determine the significance of inter-item relationships (variance) and their resulting R-squared (R^2) (coefficients of determination). Path analysis was used to examine the relationships between constructs by examining their path coefficients. Results from the data analysis revealed that organizational injustice constructs, negative affect, and attitude towards general IS policy are better suited in explaining a degree of variance in attitude towards specific IS policy. However, negative affect, distributive injustice, interpersonal injustice, and attitude towards specific IS policy were better suited in influencing employees' ISP non-compliance behavior. Furthermore, additional support reveled that negative affect and attitude towards specific ISP were the two rationality-based constructs that showed a strong significant relationship with employees' IS policy non-compliance.

This study presents some theoretical contributions. Beyond the findings that answer the research questions, this study contributes to literature in the IS security body of knowledge. First, although negative affect is an important component in the decision-making process, no significant progress has been made theoretically that amplifies the essential role of negative affect in judgement and decision-making in the realm of ISP non-compliance behavior. Previous IS research have considered dispositions of affect that are constant over time. This focus has been explicitly emphasized in the conceptualization of state-based affect in employees' decision to violate IS policies (D'Arcy & Lowry, 2019), or implicitly as established in cross-sectional studies that are designed to capture affective constructs at a point in time (Boss et al., 2015; Posey, Roberts, & Lowry, 2015). This study empirically contributes to theory development on the examination and unique measure of non-compliance with ISP by integrating organizational injustice constructs alongside negative affect and other cognitive factors. This contribution will diverge from prior studies that conceptualized employees' compliance with ISP from a strictly stable and reason-based approach.

Theoretical and Practical Implications

Theoretically, this research focused on actual ISP non-compliance behavioral intention and this adds to extant literature by demonstrating that employees' non-compliance with IS policies is a concept of intention and not necessarily actual behavior. Ajzen (1991), in the TPB stated that intention leads to behavior and that users are expected to carry out their intentions, it is worthwhile to state that attitude determines an individual's intention and intention determines behavior. Prior IS studies have applied behavioral intention as dependent variable (Anderson & Agarwal, 2010; Dinev & Hu,

2007; Johnston & Warkentin, 2010; Yoon & Kim, 2013). This research contributes to prior studies and extant literature by introducing ISP non-compliance as a dependent variable that emphasizes actual non-compliance behavior. The over reliance on intentions rather than actual behavior by previous IS studies is a shortcoming to the development and validation of theory (Crossler et al., 2013). Boss et al. (2015) also posited that "actual behaviors are important for ISec research because the end goal is to change security behaviors, not just security intentions" (p. 46).

Practically, it is obvious that employees' attitude and behavior towards compliance with ISPs vary daily. Amid these day-to-day fluctuations, there are blunt episodes of ISP unethical behavior that may coincide with prior experiences. Given that a single episode of non-compliance behavior can inadvertently pose security threats to the organization, it becomes imperative for organizations to stamp on these unwanted behaviors by implementing additional security measures that can predict and deter such behaviors. This research found that changes in negative mood and injustices in the distribution of resources and unfair interpersonal treatment employees receive from their managers are somewhat significant in this regard. Hence, organizations are called to foster and encourage a pleasant and positive work environment by implementing employees' mood management, equal resources distribution and fair interpersonal treatment strategies as an avenue to enhance ISP compliance behavior.

Additionally, employees' unethical or deviant workplace behaviors have consequences for ISP compliance management, and organizations need to be on the lookout for that. This amplifies the value that IS have on other functional areas when they work in tandem to tackle non-compliance with IS policies. Additionally, this study's

finding that disgruntled employees look to their supervisor's unfair treatment or injustices as triggers to ISP non-compliance behavior suggests that organizations must make a concerted effort to call out injustice practices and publicly reward employees who demonstrate compliant behavior, irrespective of the injustice. Such rewards can be in the form of official recognition of best security policy compliant employees or perks for excellence in security compliance.

Furthermore, this research found no significant influence of organizational injustice on attitude towards ISP. Because attitude determines behavior and employees' perception of poor organizational justice is a regiment that leads to destructive behavior at the workplace (Jones, 2009; Kwak, 2006), organizations are recommended to acknowledge that all employees may be liable to unwanted behavior in the context of ISP compliance. This acknowledgement could be through reinforcing the culture of transparency and fairness in treatment resource distribution from top management to lower-level employees.

Limitations and Directions for Future Research

The data was collected from participants in a predominantly Hispanic community, imposing limits to the generalizability of the results. Any inference drawn from this research will most directly apply to employees from a Hispanic background. Hence, culture and race might have influenced the direction of outcome from the results. Future research can replicate this study with focus on other ethnic/racial backgrounds. However, understanding these results from a racial and cultural perspective still renders them valid because understanding ISP compliance from a racial and cultural standpoint is particularly important.

Participants were offered no incentives to participate in the data collection exercise. As earlier anticipated, this became a factor limiting the response rate. The request for participation was articulate, detailing the objectives of the study as a means to encourage and promote participation. Another limitation that affected the response rate was that over 2000 of the emails sent with the survey link were flagged as fishing by some employees. This was a critical factor and a lesson for future studies conducting surveys by email to consider cybersecurity programs within the study organizations and other security measures such as spam filters.

In the context of information security policy non-compliance, this study was limited to organizational injustice constructs, compliance attitude, and negative affect. Hence, the inclusion of distributive injustice, procedural injustice, informational injustice, interpersonal injustice, attitude towards IS policy compliance, and compliance related behaviors. Surprisingly, two new negative affect processes, negative affective absorption (the disposition for an individual to be deeply involved with their negative emotions) and negative affective flow (an individual's state of deep involvement with their negative emotions) were omitted from this study. Future IS research that focus on compliance behavior can leverage these two negative affect constructs in examining ISP compliance behavior. The findings of this research showed that the four organizational injustice frameworks have no direct relationship with an employee's attitude towards specific information security policies. Likewise, two of the four (procedural injustice and informational injustice) showed no positive relationship with ISP non-compliance intention. Further research is recommended to identify and examine if there are any

potential mediating or moderating variables that could influence the outcome of the relationships from both an attitude and ISP non-compliance intention perspective.

Finally, this research used a web-based survey for data collection therefore the data was self-reported. This comes with limitations associated with self-reported data which includes self-selection bias, risks to validity and accuracy, and the desire for the participant to be considered kind, encouraging, and supportive (Rosenbaum et al., 2006). In addition, it is difficult for the researcher to verify self-reported data, rendering the honesty of participants' response choices questionable (Emerson et al., 2013). Due to security and confidentiality concerns, participants may not be willing to report certain behavioral observations for fear of retaliation against them (Knapp and Kirk, 2003).

Summary

With persistent efforts from organizations to curb employees' ISP non-compliance behaviors, threats from insiders' deliberate violations of IS policies is still on the rise. A possible explanation for this predicament is that ISP non-compliance is subject to different organizational injustice and affective influences. This research explored organizational injustice and negative affect constructs in an attempt to identify and define existing gaps in the IS literature field. From where the empirical examination of the impact of organizational injustice and negative affect in the premise of attitude and ISP non-compliance behavior. This study presented a background on the area of research interest, and with the use of extant literature, this study attempted to examine organizational injustice frameworks and negative affect and the impact they have on defining employees' attitude and ISP non-compliance behavior. A synthesis of prior literature relevant to the subject matter was presented, and based on that synthesis,

research questions and hypotheses were developed. Based on cognitive and rationality-based theories like rational choice, TPB, affect event theory, a conceptual model was proposed that includes cognitive and affective antecedents to attitude and non-compliance behavior.

A review of the literature from prior studies that highlighted information security threat avoidance and security policy compliance behavior, was conducted to assess and develop constructs for this research. The chosen foundational framework based on cognitive theories was perceived organizational injustice with its four constructs: distributive injustice, procedural injustice, informational injustice, and interpersonal injustice. Negative affect and attitude towards IS policy were also adopted for theory development. Prior studies have used the term justice interchangeably with injustice to refer to employees' perception of poor organizational justice as a regiment that leads to non-productive workplace behavior (Jones, 2009; Kwak, 2006). Negative affect reflects the tendency to which a person experiences negative or distressing emotions characterized by sadness, fear, anxiety and lethargy (Samnani et al., 2014; Watson & Clark, 1984; Watson, Clark, & Tellegen, 1988). Attitude toward information security policy represents the relative extend of an employee's favorable or unfavorable appraisal of ISP compliance (Ajzen, 1991; Herath & Rao, 2009b). Synthesis of prior literature presented findings and conclusions, and the identified gaps were used as a premise for this study.

The strategy adopted under the research methodology was a non-experimental scenario-based quantitative survey approach. Methodology also discussed the survey instrument development and validation (which include reliability and validity), sample

population, and data collection. A nonprobability convenience sampling approach was used to collect data from full-time employees at 2-year higher education institutions. Validity and reliability of the instrument was tested through the use of a panel of fifteen IS subject matter experts. This step was followed by a pilot study where 20 participants were invited to participate. The data collected was pre-analyzed to identify any outliers using Mahalanobis distance in SPSS. A test for normality was also run in SPSS after the pre-analysis step. SmartPLS 3.0 was used to run a PLS algorithm. The initial run was to identify items whose path coefficients were below the required 0.70. A rerun of the PLS algorithm produced *t*-statistics of structural model paths with their associated level of significance.

Finally, a discussion of results of hypotheses tests was presented under conclusion, with key empirical evidence to support the results. Theoretical and practical implications of key findings were discussed, and the limitations and directions for further research concluded the study.

Appendices

Appendix A

Survey Questionnaire

Information Security Policy (ISP) Non-Compliance Survey Instrument

Research Title: *An Empirical Examination of the Impact of Organizational Injustice and Negative Affect on Attitude and Non-Compliance with Information Security Policy*

Dear research participant,

Thank you for your time and willingness to participate in this survey. My name is Celestine Kemah and I am a doctoral student at the College of Computing and Engineering at Nova Southeastern University in Florida. I am conducting research for my doctoral dissertation where I seek your anonymous participation in a survey. The research will primarily examine the combined influence of affect and cognitive processes on employees in the context of misuse and noncompliance with information security policies. My doctoral advisor is Dr. Ling Wang, Professor of Information Systems, Information Assurance and Cybersecurity Management in the College of Computing and Engineering at Nova Southeastern University. My dissertation title is An Empirical Examination of the Impact of Organizational Injustice and Negative Affect on Attitude and Non-Compliance with Information Security Policy.

You will be taking a one-time survey that will last approximately 15 minutes. Please also note that:

Your identity, survey responses, and assessment scores will be kept anonymous. No personally identifiable information will be collected from you. The information that you provide in the survey will be completely anonymous. All your responses will be completely anonymous, aggregated and used only for academic purposes. Your participation in this survey is voluntary and, you may exit (i.e., opt-out) the survey at any time.

The survey is divided into sections with each section starting with a scenario that reflects employee treatment at the workplace. After the scenario, you will be prompted to answer the questionnaires that follow.

If you agree with the information provided above, please click on the "I Accept" button below to begin the survey. If you have any questions, you can contact me via ck641@mynsu.nova.edu or at +1240-278-1315.
Again, thank you for your time and participation in this research.

Research Background

Employees' non-compliance with information security policy is an important social and organizational topic that represents a key information security problem for organizations. It equally poses major concerns for information security management. Cognitive processes are very significant in providing an understanding as to why employees do not comply with policies and procedures. However, they do not completely explain the abusive insider's motivations. Affect is a necessary and important regimen of rational decision-making and often influences some cognitive processes such as judgments and decisions. The purpose of this study is to examine the combined influence of affect (negative changes in moods and emotions) and organizational injustice (cognitive) processes on employees in the context of misuse and non-compliance with information security policies.

Research Consent and Authorization

Your participation in this survey is voluntary and you may choose to exit the survey at any time. If you have read the above information and consent to participate in this research study, please click on the "I Accept" button below that will give you access to the survey. If you need a copy of this consent form, please click on this Link

- I Accept
- I Do not Accept

Perceived Distributive Injustice Scenario

Jael has been working at SkyNet for over ten years. His effort and commitment to the company have resulted in an increase in business output for each of the last five (5) years. Last year, SkyNet celebrated its employees with different awards including salary increases. Jael was promised a salary increase, but he was never rewarded despite the stressful nature of the job and his work performance above other system analysts. The firm explained that Jael was intentionally ignored because of his supervisor's frequent change despite the availability of records that prove his eligibility for a raise. Subsequently, Jael grew furious and started demonstrating negative behavior towards his superiors.

Given this hypothetical scenario and assuming you were Jael, please specify the extent to which you would agree or disagree with the following four statements.

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I am not fairly rewarded for my contribution to this organization	○	○	○	○	○
I am not fairly rewarded given the work I have done well.	○	○	○	○	○
I am not fairly rewarded for the stresses and strains of my job.	○	○	○	○	○
I am not fairly rewarded for the amount of effort I have put into my work.	○	○	○	○	○

Perceived Distributive Injustice Scenario

Jael has been working at SkyNet for over ten years. His effort and commitment to the company have resulted in an increase in business output for each of the last five (5) years. Last year, SkyNet celebrated its employees with different awards including salary increases. Jael was promised a salary increase, but he was never rewarded despite the stressful nature of the job and his work performance above other system analysts. The firm explained that Jael was intentionally ignored because of his supervisor's frequent change despite the availability of records that prove his eligibility for a raise. Subsequently, Jael grew furious and started demonstrating negative behavior towards his superiors.

Given this hypothetical scenario and assuming you were Jael, please specify the extent to which you would agree or disagree with the following four statements.

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I am not fairly rewarded for my contribution to this organization	○	○	○	○	○

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I am not fairly rewarded given the work I have done well.	○	○	○	○	○
I am not fairly rewarded for the stresses and strains of my job.	○	○	○	○	○
I am not fairly rewarded for the amount of effort I have put into my work.	○	○	○	○	○

Perceived Procedural Injustice Scenario

Reilly is an analyst at a financial institution where she analyzes investment candidates for her firm. She performed the same job as other analysts in the company. According to the company policy, if an employee receives two consecutive service awards, they are eligible for promotion. Reilly has received this award consecutively in two of the past five years. However, she did not receive promotion in favor of Michael, a close friend of Reilly's supervisor. Reilly did not believe the promotion process was fair, so she decided to find out why she did not get promotion despite believing that her work was as good as Michael's. She decided to take her concern to human resources who did not provide any concrete explanation why she was passed on for promotion.

Given this hypothetical scenario and assuming you were Reilly, please specify the extent to which you would agree or disagree with the following 7 statements.

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If someone at my workplace files a complaint, my organization does not collect all accurate information necessary to make decision.	○	○	○	○	○

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If someone at my workplace files a complaint, my organization would be inconsistent in applying the necessary standards and procedures to arrive at a decision.	○	○	○	○	○
If someone at my workplace files a complaint, my organization would be bias in following standards and procedures during the decision-making process.	○	○	○	○	○
If someone in my workplace files a complaint, my organization would not allow those affected to follow the established procedures in order to influence the decision.	○	○	○	○	○
If someone at my workplace files a complaint, my organization would not provide useful feedback regarding the decision and its implementation.	○	○	○	○	○
If someone at my workplace filess a complaint, my organization would not allow for requests for clarification or additional	○	○	○	○	○

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
information about the decision.					
If someone at my workplace filess a complaint, my organization would not provide opportunities to appeal or challenge the decision.	○	○	○	○	○

Perceived Interpersonal and Informational Injustice Scenario

Avery is a shift worker at Pier Traditions, a manufacturing company in North East United States. He mostly works the second of three work shifts. He had made arrangements to celebrate their 10th wedding anniversary. Two days prior, Avery submitted a request to leave work early on the day of their anniversary but he was accused by his supervisor of trying to leave work early and was ordered to return to the factory floor pending the arrival of his replacement. Avery's supervisor was not polite and failed to provide sufficient details as to why his request was rejected at the last minute.

Given this hypothetical scenario and assuming you were Avery, please specify the extent to which you would agree or disagree with the following 9 statements.

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
My supervisor does not treat me in a polite manner.	○	○	○	○	○
My supervisor does not treat me with dignity.	○	○	○	○	○
Complying with my organization’s information security policy requirements is essential.	○	○	○	○	○

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Complying with my organization's information security policy requirements is useful.	○	○	○	○	○
My supervisor has not been candid in (his/her) communications with me.	○	○	○	○	○
My supervisor does not explain procedures to me thoroughly.	○	○	○	○	○
My supervisor's explanations of the procedures to me are not reasonable.	○	○	○	○	○
My supervisor does not communicate details to me promptly.	○	○	○	○	○
My supervisor does not seem to tailor communications to my specific needs.	○	○	○	○	○

Information Security Policy Compliance Scenario

Charlie works at SkyNet. He is aware that SkyNet enforces its information security policy compliance by having its IT department monitor and record security policy compliance and violations on a regular basis. Each year the IT department sends out security policy compliance and violations reports to each department. SkyNet follows up by conducting an unscheduled assessment of its employees on information security policy compliance and violations. During one of the assessments, a coworker offered to help Charlie with the backlog of security tickets. However, in order to receive help from his coworker to clear the tickets, Charlie had to share his service account and password. Meanwhile, after the unscheduled assessments, those who had complied with the policy will be orally commended and have 1 to 5 points added to their merits (100-point base) based on the degree of compliance, while those who had violated the security policies will be orally

censured and have 1 to 5 points deducted from their merits based on the severity of violations. These merit points are directly linked to their annual bonus that is added to their salary. These merit points also have implicit influences on promotion and other benefits.

Given this hypothetical scenario and assuming you were Charlie, please specify the extent to which you would agree or disagree with the following statements.

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Complying with my organization's information security policy requirements is beneficial to me as an employee.	○	○	○	○	○
Complying with my organization's information security policy requirements is helpful to me as an employee.	○	○	○	○	○
Complying with my organization's information security policy requirements is important to me as an employee.	○	○	○	○	○
Complying with my organization's information security policy requirements is useful to me as an employee.	○	○	○	○	○
It is beneficial that I shut down/put to sleep my computer while temporarily away from my desk.	○	○	○	○	○

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
It is critical that before I share any data I should encrypt (password-protect) any personal identifying information.	○	○	○	○	○
It is important that I do not share my password while on the job.	○	○	○	○	○
It is important that I do not use my organization's computer for personal business.	○	○	○	○	○
I do not intend to comply with the requirements of the information security policies of my organization.	○	○	○	○	○
Complying with my organization's information security policies does not increases the chances of me being rewarded.	○	○	○	○	○
According to my organization's information security policy requirements, protecting the IT resources is not very imperative for me.	○	○	○	○	○
It is not important that I carry out my responsibilities as	○	○	○	○	○

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
prescribed in the information security policies of my organization when I use information and technology resources.					

Given these hypothetical scenarios above and assuming you were , Jael, Reilly, Avery or Charlie please indicate the extent to which you have felt since you started working at this organization.

	Very slightly or not at all	A little	Moderately	Quite a bit	Extremely
Distressed	○	○	○	○	○
Guilty	○	○	○	○	○
Hostile	○	○	○	○	○
Ashamed	○	○	○	○	○
Jittery	○	○	○	○	○
Upset	○	○	○	○	○
Scared	○	○	○	○	○
Nervous	○	○	○	○	○
Afraid	○	○	○	○	○
Irritable	○	○	○	○	○

Gender

- ○ Male
- ○ Female

Age Group

20 -29	30 - 39	40 - 49	50 - 59	60+
○	○	○	○	○

Highest Level of Education

High School graduate/GED	Some College	Associate Degree	Bachelor's Degree	Master's Degree	Doctoral Degree	Professional Degree
○	○	○	○	○	◉	○

Appendix B:

IRB Approval Letter

NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To: **Celestine Kemah**

From: **Wei Li, Ph.D,**
Center Representative, Institutional Review Board

Date: **June 16, 2020**

Re: **IRB #: 2020-294; Title, "An Empirical Examination of the Impact of Organizational Injustice and Negative Affect on Attitude and Non-Compliance with Information Security Policy"**

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

1) CONSENT: If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE EVENTS/UNANTICIPATED PROBLEMS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and Wei Li, Ph.D, respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

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

Cc: Ling Wang, Ph.D.
Ling Wang, Ph.D.

Appendix C:

Pre-analysis test Results with Descriptive Statistics, Skewness, and Kurtosis

Descriptive Statistics

	N	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
PDI1	117	4.06	1.003	-1.218	.224	1.163	.444
PDI2	117	4.02	1.008	-1.112	.224	.877	.444
PDI3	117	3.79	1.071	-.950	.224	.528	.444
PDI4	117	3.95	1.082	-1.103	.224	.697	.444
PPI1	117	3.26	1.100	-.448	.224	-.586	.444
PPI2	117	3.35	1.101	-.499	.224	-.485	.444
PPI3	117	3.34	1.092	-.233	.224	-.751	.444
PPI4	117	3.15	1.119	-.047	.224	-.856	.444
PPI5	117	3.58	1.161	-.536	.224	-.723	.444
PPI6	117	3.33	1.114	-.161	.224	-.833	.444
PPI7	117	3.19	1.137	-.091	.224	-.786	.444
PII1	117	3.51	1.250	-.676	.224	-.629	.444
PII2	117	3.34	1.247	-.378	.224	-.914	.444
PII3	117	4.07	.935	-1.039	.224	1.260	.444
PII4	117	3.93	1.081	-1.113	.224	1.025	.444
PINJ1	117	3.74	1.109	-.882	.224	.113	.444
PINJ2	117	3.61	1.137	-.645	.224	-.273	.444
PINJ3	117	3.50	1.047	-.492	.224	-.262	.444
PINJ4	117	3.82	1.103	-.890	.224	.128	.444
PINJ5	117	3.56	1.086	-.579	.224	-.208	.444
ATG1	117	4.21	.927	-1.300	.224	1.328	.444
ATG2	117	4.13	.915	-1.152	.224	1.082	.444
ATG3	117	4.15	.916	-1.066	.224	.791	.444
ATG4	117	4.07	.888	-1.263	.224	1.960	.444
ATS1	117	4.26	.800	-1.422	.224	3.413	.444
ATS2	117	4.21	.972	-1.245	.224	1.108	.444
ATS3	117	4.44	.951	-1.858	.224	2.905	.444
ATS4	117	4.26	.832	-1.153	.224	1.495	.444
ISPC1	117	1.94	1.234	1.236	.224	.480	.444
ISPC2	117	2.49	1.277	.332	.224	-1.103	.444
ISPC3	117	1.86	.999	1.335	.224	1.475	.444
ISPC4	117	2.50	1.369	.543	.224	-1.029	.444

NAF1	117	2.74	1.192	-.061	.224	-.999	.444
NAF2	117	1.93	1.032	.714	.224	-.763	.444
NAF3	117	2.02	1.152	.792	.224	-.480	.444
NAF4	117	1.81	1.129	1.257	.224	.606	.444
NAF5	117	2.05	1.121	.758	.224	-.393	.444
NAF6	117	2.72	1.351	.145	.224	-1.255	.444
NAF7	117	2.09	1.149	.732	.224	-.538	.444
NAF8	117	2.30	1.212	.644	.224	-.542	.444
NAF9	117	2.12	1.190	.857	.224	-.198	.444
NAF10	117	2.61	1.332	.311	.224	-1.090	.444
Valid N (listwise)	117						

Appendix D:

Mahalanobis Distance and Stem & Leaf Plot

Descriptives

			Statistic	Std. Error
Mahalanobis Distance	Mean		6.9401709	.48680627
	95% Confidence Interval for Mean	Lower Bound	5.9759898	
		Upper Bound	7.9043521	
	5% Trimmed Mean		6.4372785	
	Median		5.6979952	
	Variance		27.727	
	Std. Deviation		5.26561494	
	Minimum		.47121	
	Maximum		30.88376	
	Range		30.41255	
	Interquartile Range		5.30662	
	Skewness		1.820	.224
	Kurtosis		4.155	.444

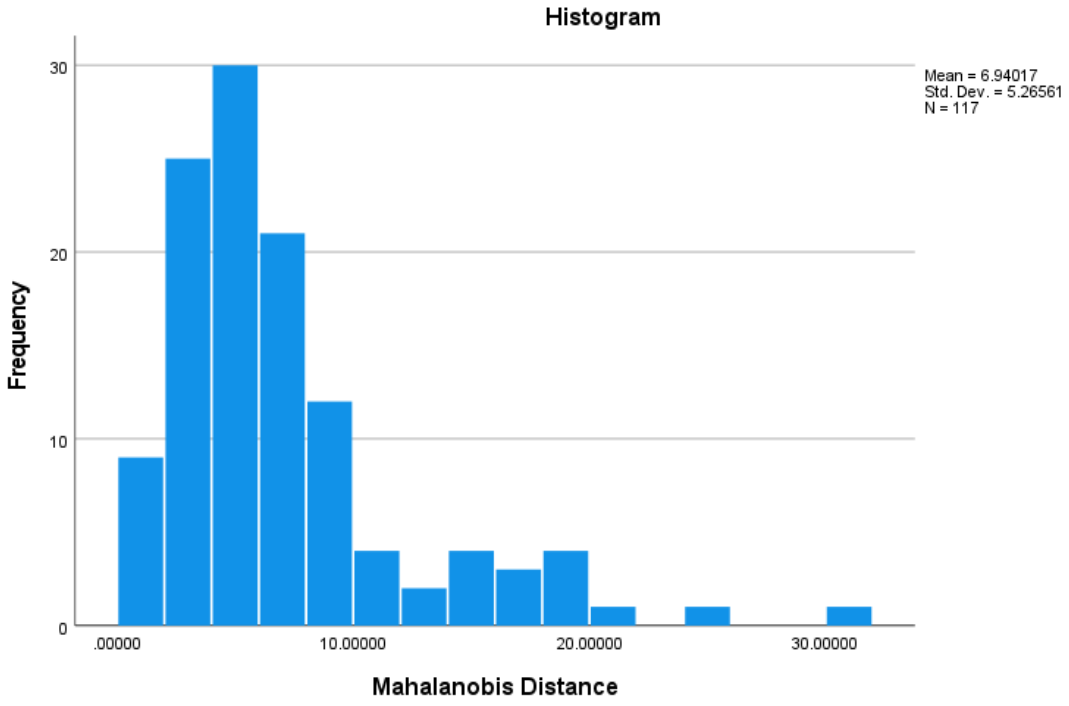
Extreme Values

			Case Number	Value
Mahalanobis Distance	Highest	1	44	30.88376
		2	39	25.04404
		3	29	20.67579
		4	104	18.80049
		5	66	18.50962
	Lowest	1	41	.47121
		2	110	.51287
		3	79	.68874
		4	32	.91866
		5	71	1.05051

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Mahalanobis Distance	.177	117	.000	.835	117	.000

a. Lilliefors Significance Correction

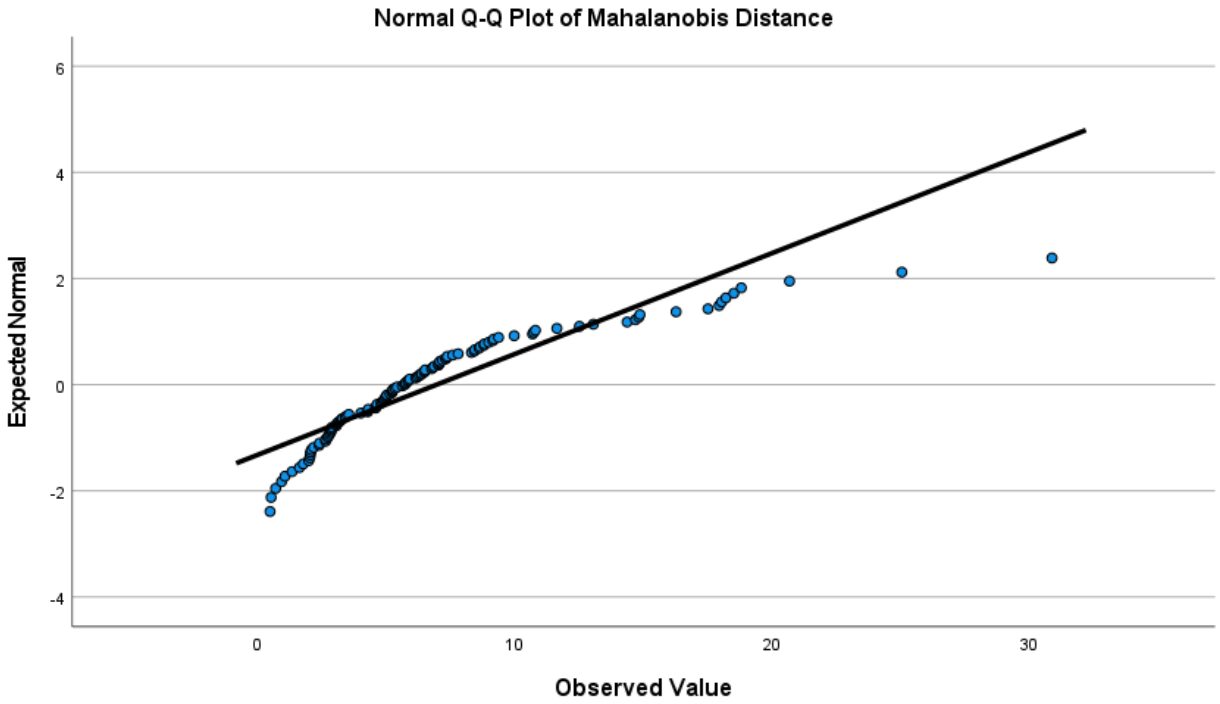


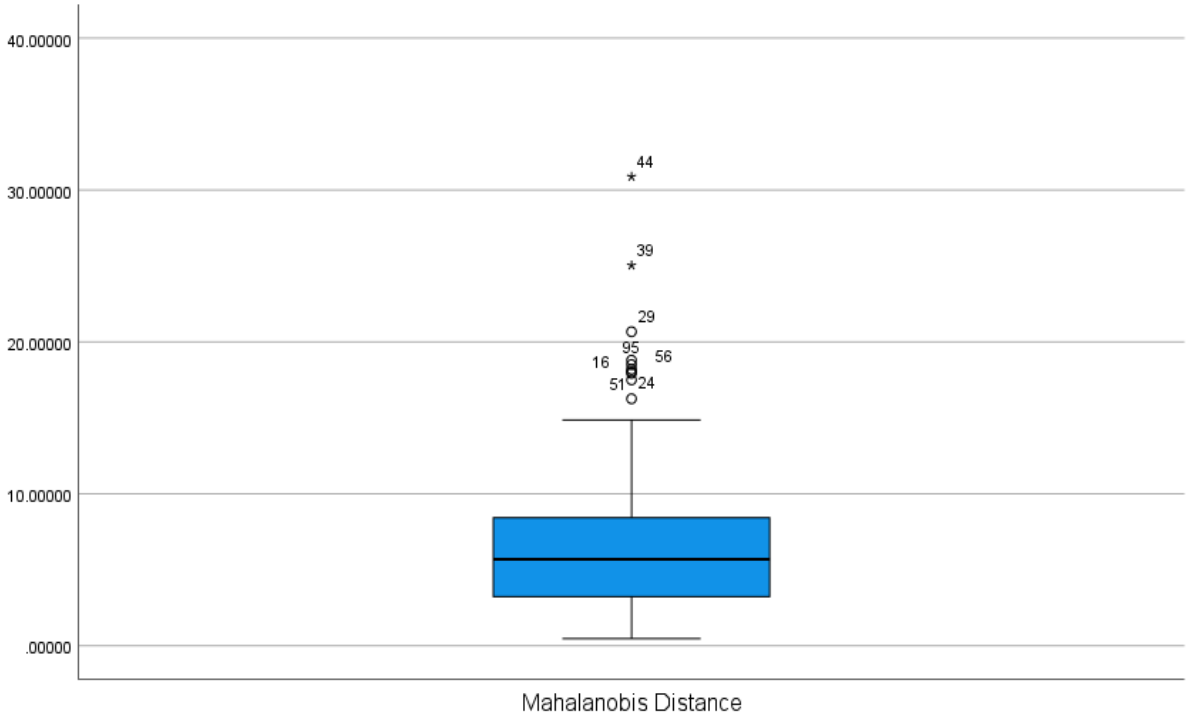

```
Mahalanobis Distance Stem-and-Leaf Plot

 Frequency     Stem &  Leaf

     4.00        0 .  4569
     5.00        1 .  03679
    16.00        2 .  0000133667778888
     9.00        3 .  001122345
    14.00        4 .  02225666788999
    16.00        5 .  0012222346677889
    11.00        6 .  11233445788
    10.00        7 .  0000123357
     8.00        8 .  34456789
     4.00        9 .  1139
     3.00       10 .  677
     1.00       11 .  6
     1.00       12 .  5
     1.00       13 .  0
     4.00       14 .  3688
    10.00 Extremes    (>=16.3)

 Stem width:   1.00000
 Each leaf:        1 case(s)
```


Normal Q-Q Plot of Mahalanobis Distance
Expected Normal
6
4
2
0
-2
-4
0
10
20
30
Observed Value


40.00000
30.00000
20.00000
10.00000
.00000
44
39
29
95
16
56
51
24
Mahalanobis Distance

Appendix E:

Rerun of Mahalanobis Distance and Stem & Leaf Plot after Deleting 2 Extremes

Descriptives

			Statistic	Std. Error
Mahalanobis Distance	Mean		6.5745408	.41884277
	95% Confidence Interval for Mean	Lower Bound	5.7448165	
		Upper Bound	7.4042651	
	5% Trimmed Mean		6.2198885	
	Median		5.6108204	
	Variance		20.174	
	Std. Deviation		4.49158834	
	Minimum		.47121	
	Maximum		20.67579	
	Range		20.20458	
	Interquartile Range		5.22906	
	Skewness		1.297	.226
	Kurtosis		1.325	.447

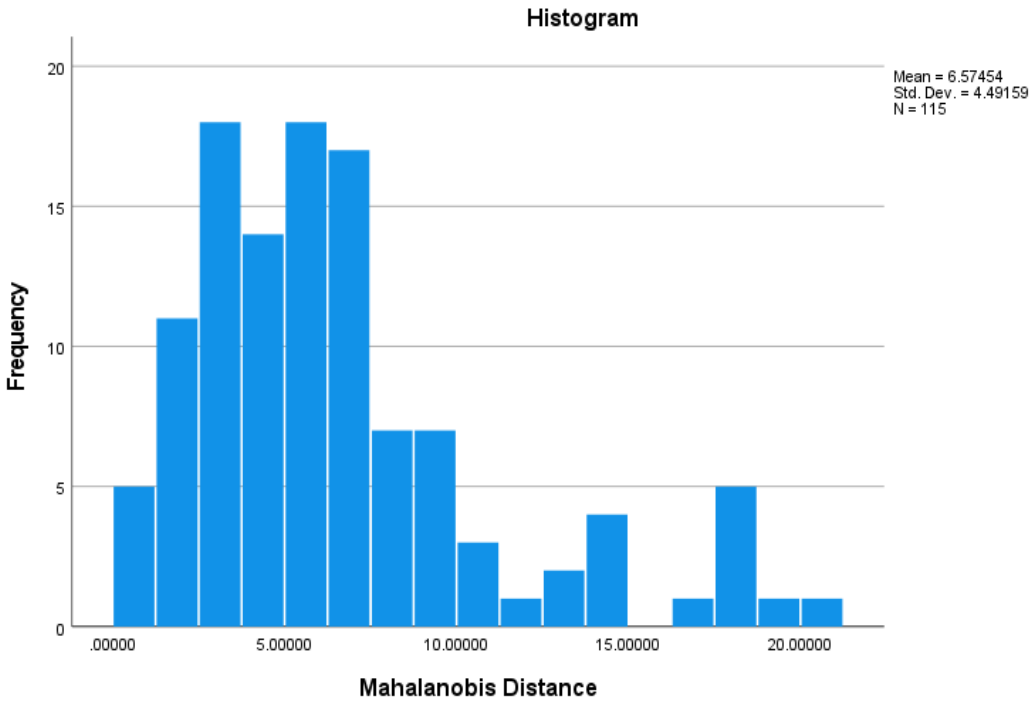
Extreme Values

			Case Number	Value
Mahalanobis Distance	Highest	1	29	20.67579
		2	104	18.80049
		3	66	18.50962
		4	51	18.20100
		5	56	18.03625
	Lowest	1	41	.47121
		2	110	.51287
		3	79	.68874
		4	32	.91866
		5	71	1.05051

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Mahalanobis Distance	.152	115	.000	.879	115	.000

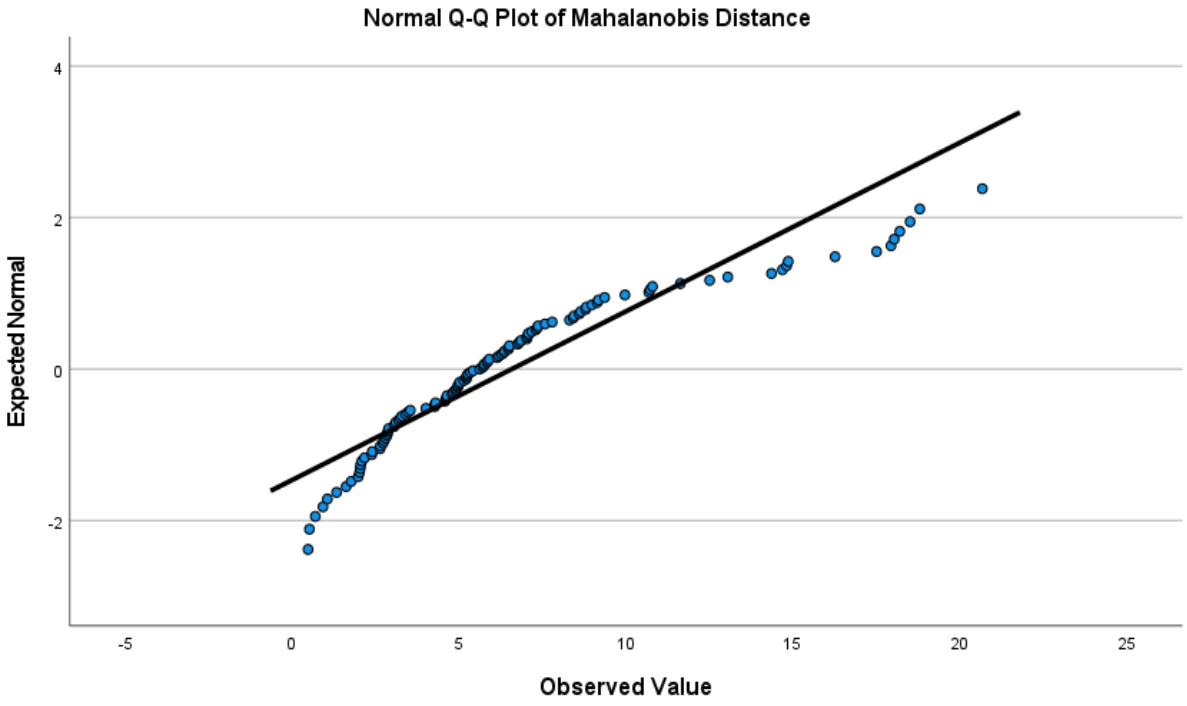
a. Lilliefors Significance Correction

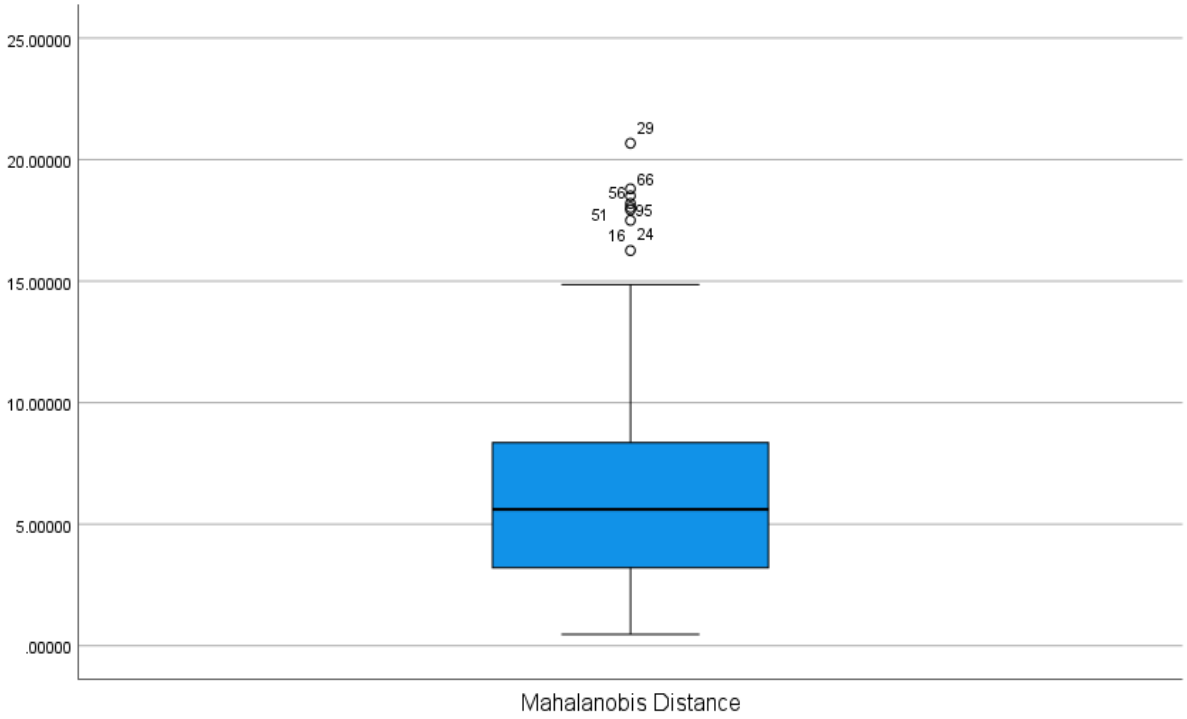


Mahalanobis Distance Stem-and-Leaf Plot

Frequency	Stem &	Leaf
4.00	0 .	4569
5.00	1 .	03679
16.00	2 .	0000133667778888
9.00	3 .	001122345
14.00	4 .	02225666788999
16.00	5 .	0012222346677889
11.00	6 .	11233445788
10.00	7 .	0000123357
8.00	8 .	34456789
4.00	9 .	1139
3.00	10 .	677
1.00	11 .	6
1.00	12 .	5
1.00	13 .	0
4.00	14 .	3688
8.00	Extremes	(>=16.3)

Stem width: 1.00000
Each leaf: 1 case(s)


Normal Q-Q Plot of Mahalanobis Distance
Expected Normal
4
2
0
-2
-5
0
5
10
15
20
25
Observed Value


25.00000
20.00000
15.00000
10.00000
5.00000
.00000
29
66
56
95
51
16
24
Mahalanobis Distance

Appendix F:

Test Results of Normality and Scatter Plot

Correlations

		ISPC	PDI	PPI	PII	PINJ	ATG	ATS	NAF
Pearson Correlation	ISPC	1.000	-.051	-.093	-.208	-.079	-.398	-.297	.303
	PDI	-.051	1.000	.465	.355	.448	-.032	-.004	.224
	PPI	-.093	.465	1.000	.378	.463	-.016	.085	.305
	PII	-.208	.355	.378	1.000	.549	.173	.175	.174
	PINJ	-.079	.448	.463	.549	1.000	-.027	.101	.233
	ATG	-.398	-.032	-.016	.173	-.027	1.000	.562	-.178
	ATS	-.297	-.004	.085	.175	.101	.562	1.000	-.027
	NAF	.303	.224	.305	.174	.233	-.178	-.027	1.000
Sig. (1-tailed)	ISPC	.	.294	.160	.013	.201	.000	.001	.001
	PDI	.294	.	.000	.000	.000	.366	.485	.008
	PPI	.160	.000	.	.000	.000	.431	.182	.000
	PII	.013	.000	.000	.	.000	.032	.031	.031
	PINJ	.201	.000	.000	.000	.	.386	.141	.006
	ATG	.000	.366	.431	.032	.386	.	.000	.028
	ATS	.001	.485	.182	.031	.141	.000	.	.388
	NAF	.001	.008	.000	.031	.006	.028	.388	.
N	ISPC	115	115	115	115	115	115	115	115
	PDI	115	115	115	115	115	115	115	115
	PPI	115	115	115	115	115	115	115	115
	PII	115	115	115	115	115	115	115	115
	PINJ	115	115	115	115	115	115	115	115
	ATG	115	115	115	115	115	115	115	115
	ATS	115	115	115	115	115	115	115	115
	NAF	115	115	115	115	115	115	115	115

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.524[a]	.275	.227	.758

a. Predictors: (Constant), NAF, ATS, PDI, PII, PPI, ATG, PINJ

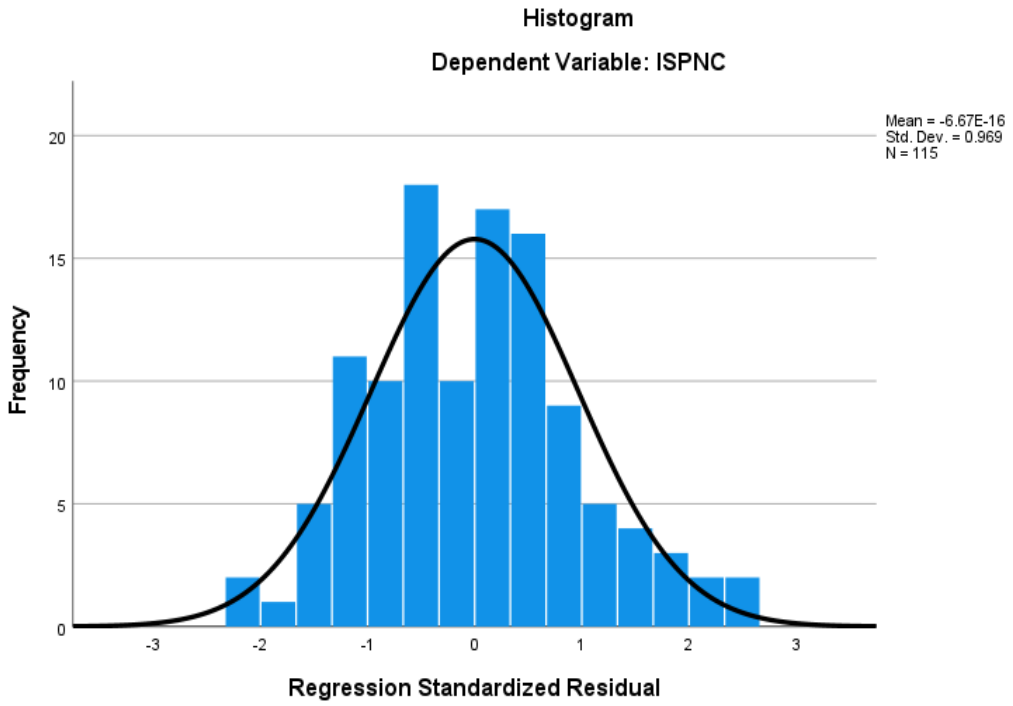
b. Dependent Variable: ISPC

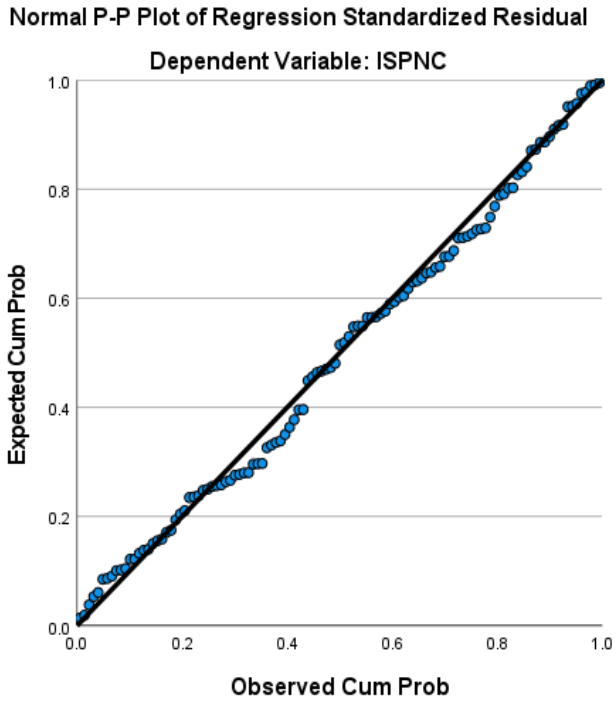
ANOVA[a]

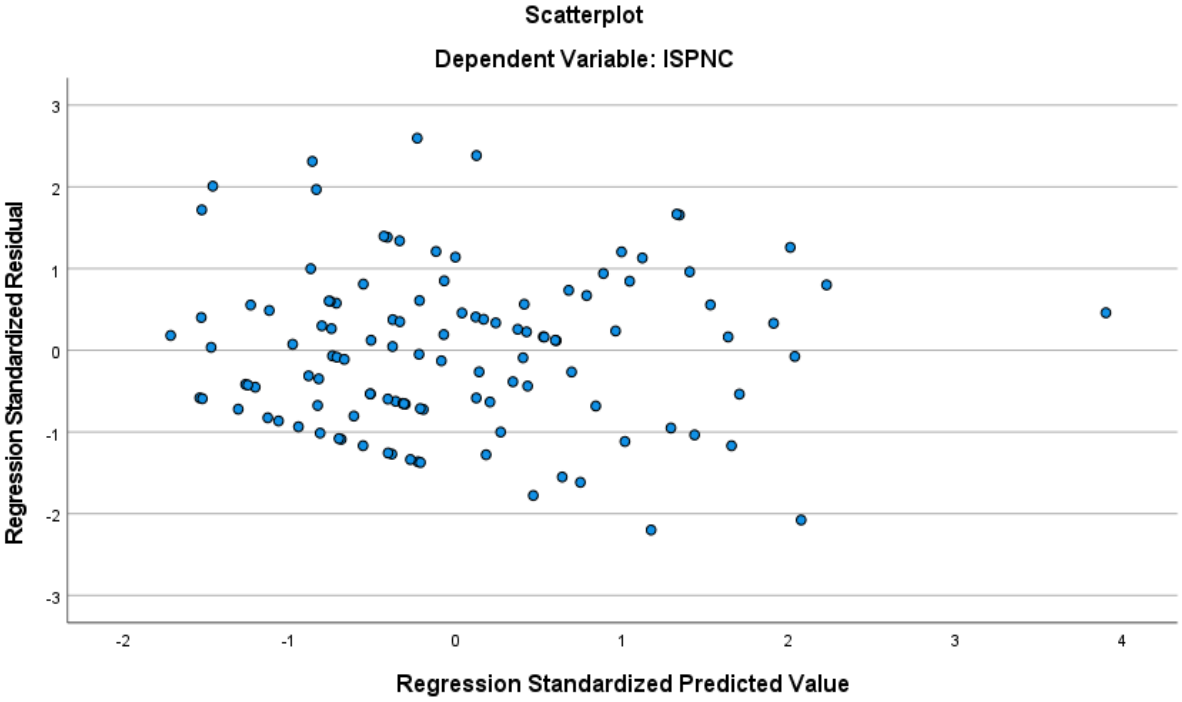
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	23.287	7	3.327	5.789	.000[b]
	Residual	61.493	107	.575		
	Total	84.780	114			

a. Dependent Variable: ISPC

b. Predictors: (Constant), NAF, ATS, PDI, PII, PPI, ATG, PINJ

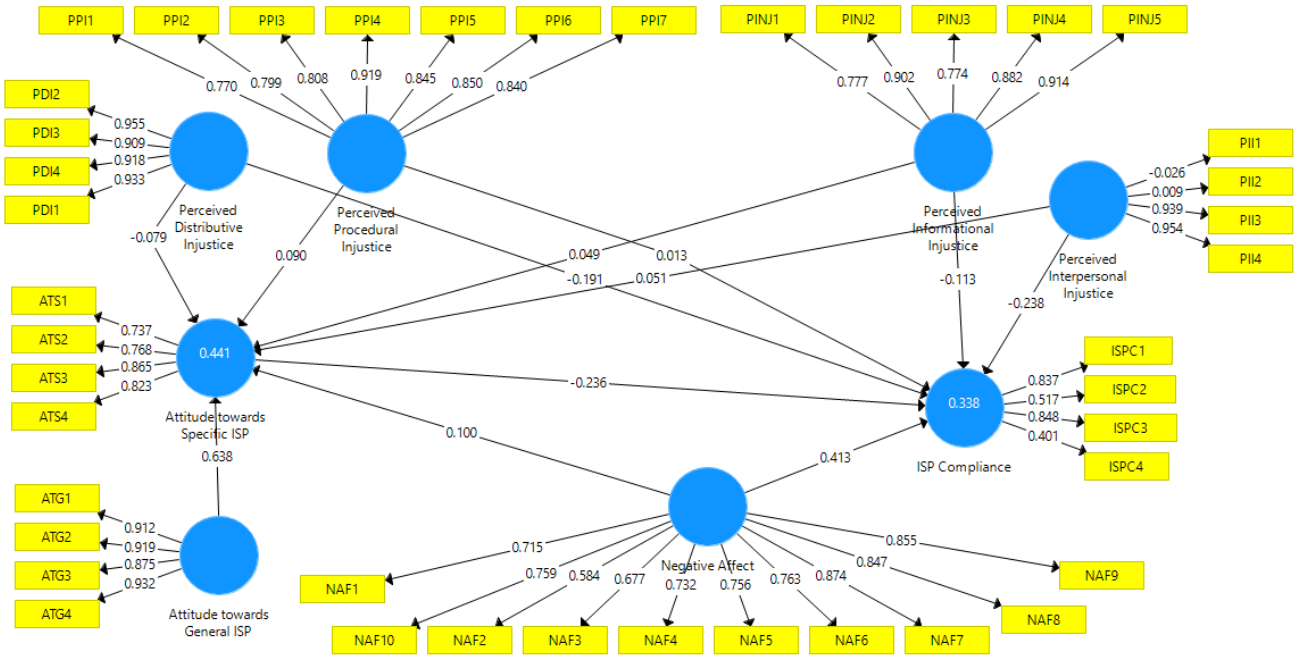



Normal P-P Plot of Regression Standardized Residual
Dependent Variable: ISPNC
Expected Cum Prob
Observed Cum Prob
0.0
0.2
0.4
0.6
0.8
1.0


Scatterplot
Dependent Variable: ISPNC
Regression Standardized Residual
Regression Standardized Predicted Value
3
2
1
0
-1
-2
-3
-2
-1
0
1
2
3
4

Appendix G:

Initial run of PLS Analysis showing Factor Loadings



Appendix H:

Model fit, Reliability, Validity, Coefficient and Outer Loading

Model_Fit

Fit Summary | rms Theta

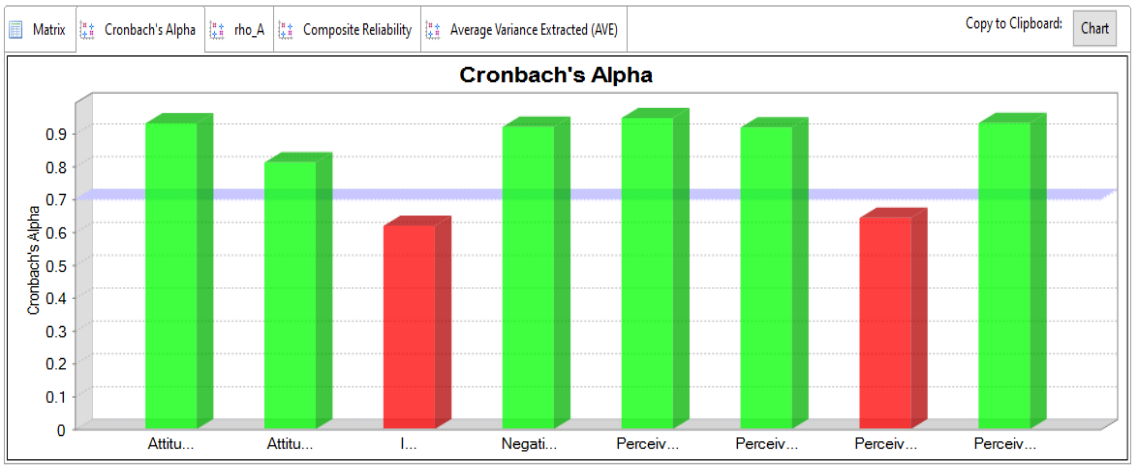
	Saturated Model	Estimated Mo...
SRMR	0.123	0.123
d_ULS	13.742	13.771
d_G	3.667	3.671
Chi-Square	1893.627	1894.608
NFI	0.600	0.600

Construct Reliability and Validity

Matrix | Cronbach's Alpha | rho_A | Composite Reliability | Average Variance Extracted (AVE)

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Attitude towards General ISP	0.931	0.942	0.951	0.828
Attitude towards Specific ISP	0.812	0.828	0.876	0.639
ISP Compliance	0.619	0.744	0.759	0.462
Negative Affect	0.920	0.956	0.931	0.579
Perceived Distributive Injustice	0.947	0.958	0.962	0.863
Perceived Informational Injustice	0.918	0.870	0.930	0.726
Perceived Interpersonal Injustice	0.643	0.871	0.615	0.448
Perceived Procedural Injustice	0.932	1.114	0.941	0.696

Construct Reliability and Validity



Discriminant Validity

Fornell-Larcker Criterion | Cross Loadings | Heterotrait-Monotrait Ratio (HTMT) | Heterotrait-Monotrait Ratio (HTMT) | Copy to (

	Attitude towar...	Attitude towar...	ISP Compliance	Negative Affect	Perceived Distr...	Perceived Infor...	Perceived Inter...	Perceived Proc...
Attitude towar...	0.910							
Attitude towar...	0.643	0.800						
ISP Compliance	-0.365	-0.293	0.680					
Negative Affect	-0.172	-0.004	0.378	0.761				
Perceived Distri...	-0.071	-0.051	-0.105	0.235	0.929			
Perceived Infor...	-0.059	0.043	-0.121	0.186	0.379	0.852		
Perceived Inter...	0.325	0.260	-0.336	-0.111	-0.063	0.033	0.669	
Perceived Proc...	0.035	0.130	-0.063	0.230	0.386	0.465	0.057	0.834

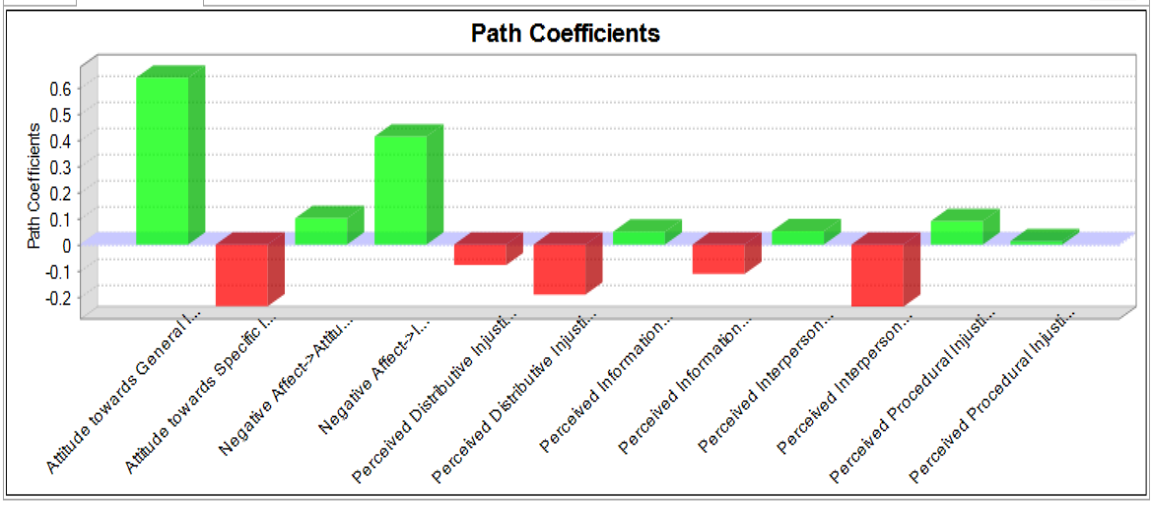
Path Coefficients

Matrix | Path Coefficients | Copy t

	Attitude towar...	Attitude towar...	ISP Compliance	Negative Affect	Perceived Distr...	Perceived Infor...	Perceived Inter...	Perceived Proc...
Attitude towar...		0.638						
Attitude towar...			-0.236					
ISP Compliance								
Negative Affect		0.100	0.413					
Perceived Distri...		-0.079	-0.191					
Perceived Infor...		0.049	-0.113					
Perceived Inter...		0.051	-0.238					
Perceived Proc...		0.090	0.013					

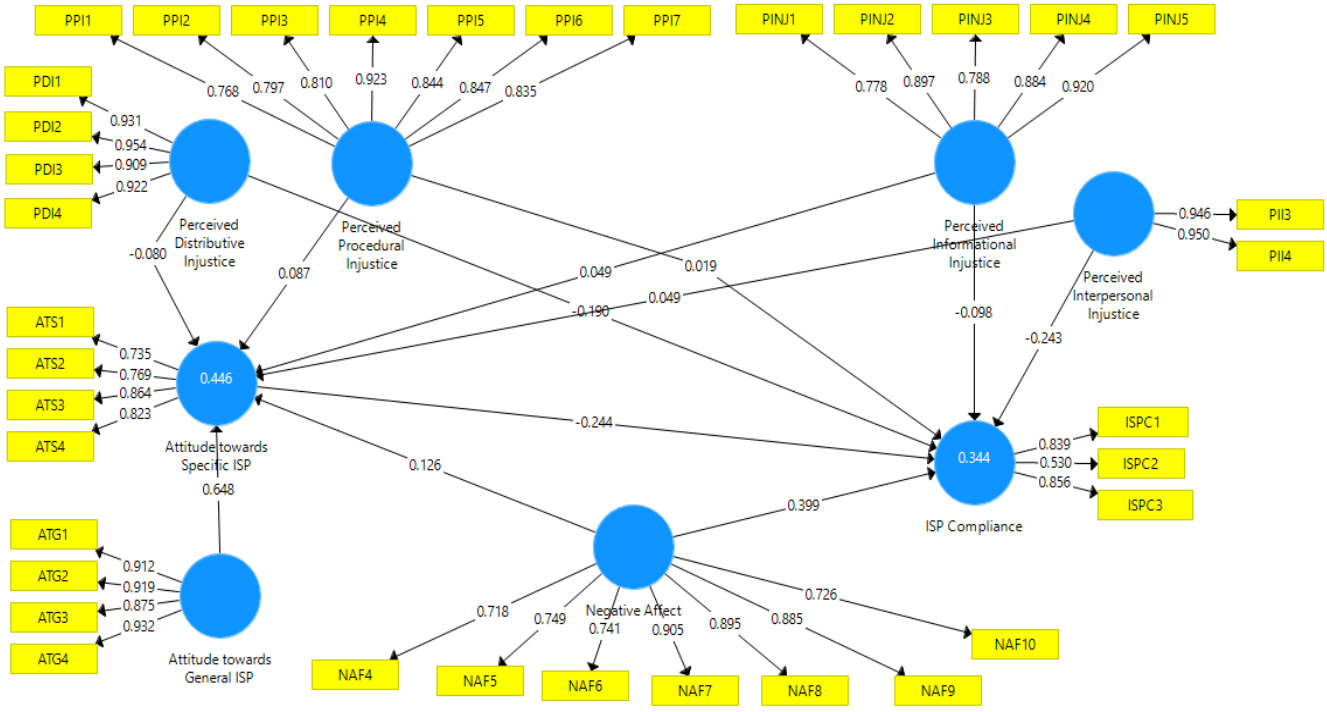
Path Coefficients

Matrix | Path Coefficients | Copy to Clipboard: Chart



Appendix I:

Rerun of PLS Analysis after PII1, PII2, ISPC4, NAF2, and NAF3 were deleted



Appendix J:

Model fit, Reliability, Validity, Coefficient and Outer Loading after PLS Rerun

Model_Fit

Fit Summary | rms Theta

	Saturated Model	Estimated Mo...
SRMR	0.074	0.074
d_ULS	3.604	3.624
d_G	1.992	1.995
Chi-Square	1180.941	1181.500
NFI	0.695	0.695

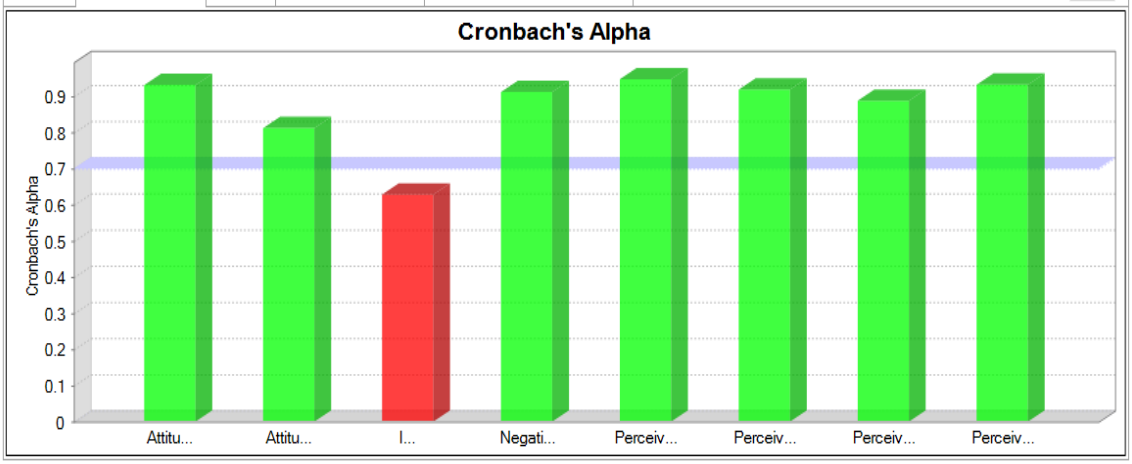
Construct Reliability and Validity

Matrix | Cronbach's Alpha | rho_A | Composite Reliability | Average Variance Extracted (AVE)

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Attitude towards General ISP	0.931	0.942	0.951	0.828
Attitude towards Specific ISP	0.812	0.828	0.876	0.639
ISP Compliance	0.628	0.707	0.794	0.572
Negative Affect	0.911	0.958	0.928	0.651
Perceived Distributive Injustice	0.947	0.952	0.962	0.863
Perceived Informational Injustice	0.918	0.918	0.932	0.732
Perceived Interpersonal Injustice	0.888	0.889	0.947	0.899
Perceived Procedural Injustice	0.932	1.141	0.941	0.694

Construct Reliability and Validity

Matrix | Cronbach's Alpha | rho_A | Composite Reliability | Average Variance Extracted (AVE) | Copy to Clipboard: Chart



R Square

Matrix | R Square | R Square Adjusted

	R Square	R Square Adjusted
Attitude towards Specific ISP	0.446	0.416
ISP Compliance	0.344	0.308

Discriminant Validity

Fornell-Larcker Criterion | Cross Loadings | Heterotrait-Monotrait Ratio (HTMT) | Heterotrait-Monotrait Ratio (HTMT) | Copy to Clipboard: Exce

	Attitude towar...	Attitude towar...	ISP Compliance	Negative Affect	Perceived Distr...	Perceived Infor...	Perceived Inter...	Perceived Proc...
Attitude towards General ISP	0.910							
Attitude towards Specific ISP	0.643	0.800						
ISP Compliance	-0.370	-0.300	0.756					
Negative Affect	-0.205	-0.004	0.381	0.807				
Perceived Distributive Injustice	-0.070	-0.050	-0.119	0.200	0.929			
Perceived Informational Injustice	-0.059	0.043	-0.128	0.150	0.379	0.856		
Perceived Interpersonal Injustice	0.319	0.254	-0.351	-0.120	-0.034	0.068	0.948	
Perceived Procedural Injustice	0.036	0.132	-0.069	0.206	0.387	0.465	0.078	0.833

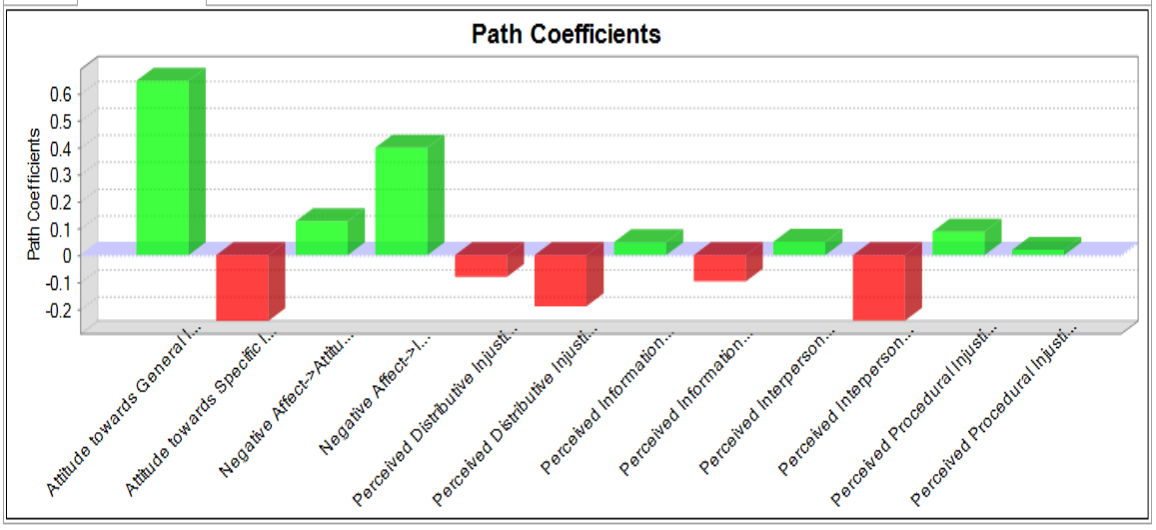
Path Coefficients

Matrix | Path Coefficients | Copy to Clipboard: Excel

	Attitude towar...	Attitude towar...	ISP Compliance	Negative Affect	Perceived Distr...	Perceived Infor...	Perceived Inter...	Perceived Proc...
Attitude towards General ISP		0.648						
Attitude towards Specific ISP			-0.244					
ISP Compliance								
Negative Affect		0.126	0.399					
Perceived Distributive Injustice		-0.080	-0.190					
Perceived Informational Injustice		0.049	-0.098					
Perceived Interpersonal Injustice		0.049	-0.243					
Perceived Procedural Injustice		0.087	0.019					

Path Coefficients

Matrix | Path Coefficients | Copy to Clipboard: Chart



Appendix K:

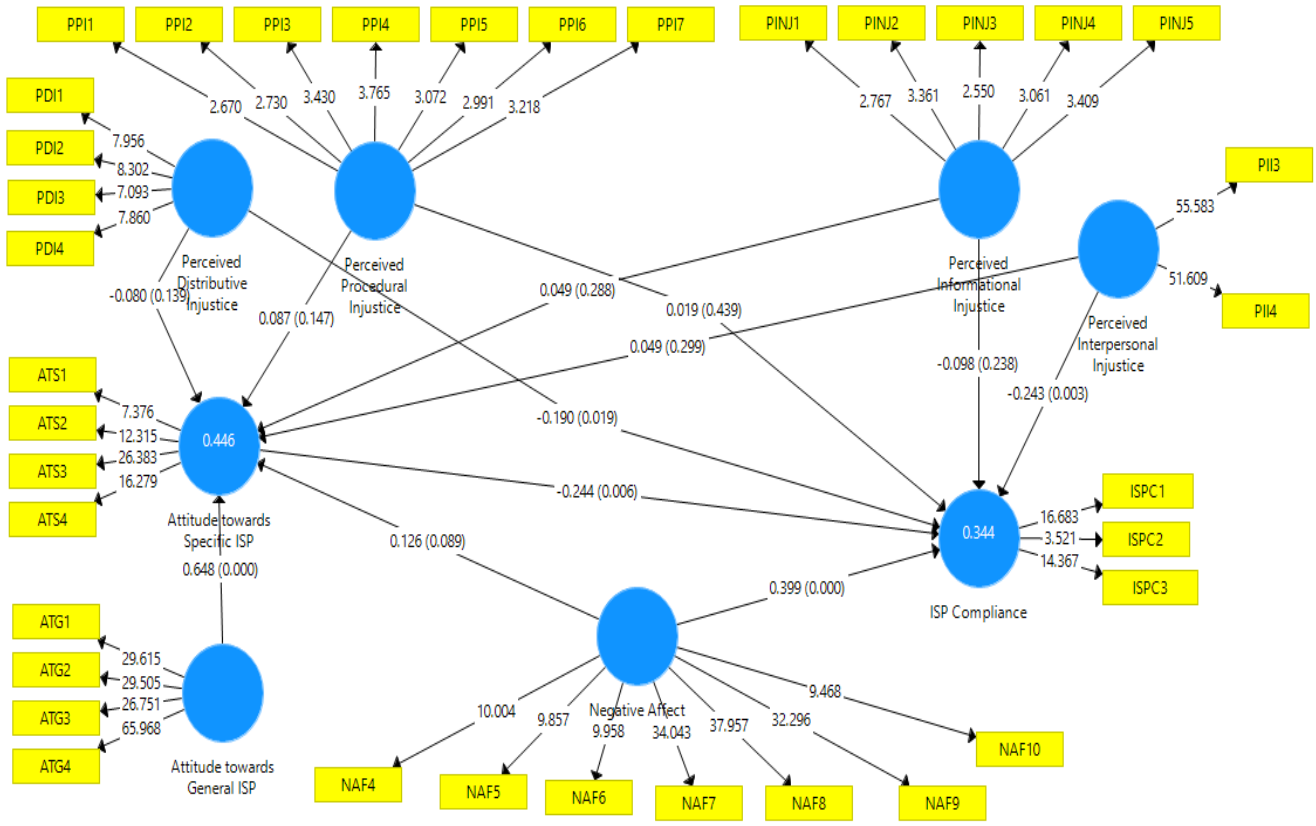
Indicator Items Cross Loadings

	ATG	ATS	ISPC	NAF	PDI	PINJ	PII	PPI
ATG1	**0.912**	0.518	-0.285	-0.215	-0.122	-0.038	0.233	-0.020
ATG2	**0.919**	0.512	-0.266	-0.173	-0.116	-0.121	0.226	-0.045
ATG3	**0.875**	0.612	-0.400	-0.211	0.016	0.008	0.344	0.125
ATG4	**0.932**	0.669	-0.374	-0.153	-0.050	-0.069	0.333	0.048
ATS1	0.434	**0.735**	-0.184	0.008	0.069	0.099	0.174	0.127
ATS2	0.481	**0.769**	-0.178	0.056	-0.075	0.055	0.222	0.059
ATS3	0.613	**0.864**	-0.305	-0.042	-0.071	-0.014	0.157	0.081
ATS4	0.509	**0.823**	-0.271	-0.021	-0.061	0.019	0.266	0.159
ISPC1	-0.273	-0.230	**0.839**	0.372	-0.132	-0.102	-0.281	0.019
ISPC2	-0.094	0.056	**0.530**	0.189	-0.076	-0.257	-0.167	-0.172
ISPC3	-0.404	-0.379	**0.856**	0.277	-0.062	-0.026	-0.324	-0.075
NAF1	-0.050	0.099	0.201	**0.726**	0.285	0.245	-0.055	0.251
NAF10	-0.070	-0.049	0.244	**0.718**	0.130	0.117	-0.008	0.176
NAF2	-0.173	-0.069	0.169	**0.749**	0.220	0.109	-0.081	0.162
NAF3	-0.084	0.052	0.226	**0.741**	0.282	0.212	-0.159	0.219
NAF4	-0.217	0.013	0.336	**0.905**	0.140	0.062	-0.080	0.176
NAF5	-0.231	-0.014	0.421	**0.895**	0.120	0.091	-0.096	0.085
NAF6	-0.233	-0.033	0.397	**0.885**	0.106	0.111	-0.171	0.187
NAF7	-0.036	-0.029	-0.125	**0.188**	0.954	0.383	-0.058	0.347
NAF8	-0.136	-0.087	-0.097	**0.197**	0.909	0.298	0.021	0.366
NAF9	-0.042	-0.009	-0.109	**0.192**	0.922	0.376	0.000	0.360
PDI1	0.875	0.612	-0.400	-0.211	0.016	0.008	0.344	0.125
PDI2	0.279	0.238	-0.325	-0.069	-0.030	0.104	0.946	0.054
PDI3	0.324	0.243	-0.341	-0.157	-0.035	0.028	0.950	0.093
PDI4	-0.128	-0.014	-0.080	0.244	0.435	0.778	-0.035	0.311
PII3	-0.032	0.070	-0.121	0.100	0.268	0.897	**0.022**	0.442
PII4	-0.039	0.031	0.027	0.088	0.259	0.788	**0.007**	0.382
PINJ1	-0.052	0.008	-0.080	0.114	0.382	**0.884**	0.062	0.395
PINJ2	-0.030	0.050	-0.126	0.113	0.317	**0.920**	0.143	0.442
PINJ3	0.001	0.064	0.021	0.219	0.317	**0.320**	0.128	0.768
PINJ4	-0.008	0.063	0.026	0.217	0.324	**0.359**	-0.059	0.797
PINJ5	0.023	0.108	-0.004	0.211	0.436	**0.483**	0.054	0.810
PPI1	0.065	0.180	-0.120	0.102	0.329	0.390	0.111	**0.923**
PPI2	-0.001	0.062	-0.100	0.211	0.371	0.389	-0.011	**0.844**
PPI3	-0.030	0.060	0.013	0.247	0.359	0.456	0.027	**0.847**
PPI4	0.054	0.094	-0.047	0.191	0.195	0.370	0.106	**0.835**
PPI5	-0.041	-0.055	-0.110	0.166	0.931	0.356	-0.085	**0.366**
PPI6	0.912	0.518	-0.285	-0.215	-0.122	-0.038	0.233	**-0.020**
PPI7	0.919	0.512	-0.266	-0.173	-0.116	-0.121	0.226	**-0.045**

Variables in bold must be higher than the variables in the corresponding row or column

Appendix L:

Significant Results of Bootstrapping



Path Coefficients

Mean, STDEV, T-Values, P-Values | Confidence Intervals | Confidence Intervals Bias Corrected | Samples

	Original Sampl...	Sample Mean (...	Standard Devia...	T Statistics (|O/...	P Values
Attitude towards General ISP -> Attitude towards Specific ISP	0.648	0.636	0.096	6.713	0.000
Attitude towards Specific ISP -> ISP Compliance	-0.244	-0.250	0.098	2.501	0.006
Negative Affect -> Attitude towards Specific ISP	0.126	0.118	0.093	1.348	0.089
Negative Affect -> ISP Compliance	0.399	0.394	0.076	5.269	0.000
Perceived Distributive Injustice -> Attitude towards Specific ISP	-0.080	-0.081	0.074	1.085	0.139
Perceived Distributive Injustice -> ISP Compliance	-0.190	-0.198	0.092	2.070	0.019
Perceived Informational Injustice -> Attitude towards Specific ISP	0.049	0.058	0.087	0.560	0.288
Perceived Informational Injustice -> ISP Compliance	-0.098	-0.083	0.137	0.714	0.238
Perceived Interpersonal Injustice -> Attitude towards Specific ISP	0.049	0.060	0.094	0.526	0.299
Perceived Interpersonal Injustice -> ISP Compliance	-0.243	-0.238	0.089	2.735	0.003
Perceived Procedural Injustice -> Attitude towards Specific ISP	0.087	0.081	0.083	1.048	0.147
Perceived Procedural Injustice -> ISP Compliance	0.019	0.004	0.127	0.154	0.439

Total Effects

Mean, STDEV, T-Values, P-Values | Confidence Intervals | Confidence Intervals Bias Corrected | Samples | Copy to Clipboard:

	Original Sample (O)	Sample Mean (M)	Standard Deviation (S...	T Statistics (|O/...	P Values
Attitude towards General ISP -> Attitude towards Specific ISP	0.648	0.636	0.096	6.713	0.000
Attitude towards General ISP -> ISP Compliance	-0.158	-0.155	0.057	2.759	0.003
Attitude towards Specific ISP -> ISP Compliance	-0.244	-0.250	0.098	2.501	0.006
Negative Affect -> Attitude towards Specific ISP	0.126	0.118	0.093	1.348	0.089
Negative Affect -> ISP Compliance	0.368	0.367	0.081	4.525	0.000
Perceived Distributive Injustice -> Attitude towards Specific ISP	-0.080	-0.081	0.074	1.085	0.139
Perceived Distributive Injustice -> ISP Compliance	-0.170	-0.177	0.093	1.835	0.033
Perceived Informational Injustice -> Attitude towards Specific ISP	0.049	0.058	0.087	0.560	0.288
Perceived Informational Injustice -> ISP Compliance	-0.110	-0.100	0.131	0.838	0.201
Perceived Interpersonal Injustice -> Attitude towards Specific ISP	0.049	0.060	0.094	0.526	0.299
Perceived Interpersonal Injustice -> ISP Compliance	-0.255	-0.257	0.087	2.945	0.002
Perceived Procedural Injustice -> Attitude towards Specific ISP	0.087	0.081	0.083	1.048	0.147
Perceived Procedural Injustice -> ISP Compliance	-0.002	-0.017	0.128	0.015	0.494

References

AbuKhalifeh, A. N., & Som, A. P. M. (2012). Service quality management in hotel industry: A conceptual framework for food and beverage departments. *International Journal of Business & Management, 7*(14), 135-141.

Adams, J. S. (1963). Wage inequities, productivity and work quality. *Industrial Relations: A Journal of Economy and Society, 3*(1), 9-16.

Adams, J. S. (1965). Inequity in social exchange. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (vol. 2, pp. 267-299). Academic Press.

Adams, A., & Sasse, M. A. (1999). Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures. *Communications of the ACM, 42*(12), 40-46.

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.

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

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology & Health, 26*(9), 1113-1127.

Ajzen, I., & Fishbein, M. (2005). The influences of attitudes on behavior. In D. Albarracin, B. T. Johnson & M. P. Zanna (Eds.), *Handbook of attitudes and attitude change.* Lawrence Erlbaum Associates.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security, 29*(4), 432-445.

Alder, G. S., & Ambrose, M. L. (2005). Towards understanding fairness judgments associated with computer performance monitoring: An integration of the feedback, justice, and monitoring research. *Human Resource Management Review, 15*(1), 43-67.

Alotaibi, M., Furnell, S., & Clarke, N. (2016). A novel model for monitoring security policy compliance. *Journal of Internet Technology and Secured Transactions, 5*(3/4), 205-514.

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.

Ambrose, M. L., Seabright, M. A., & Schminke, M. (2002). Sabotage in the workplace: The role of organizational injustice. *Organizational Behavior and Human Decision Processes, 89*(1), 947-965.

Anderson, L. S., Chiricos, T. G., & Waldo, G P. (1977). Formal and informal sanctions: A comparison of deterrent effects. *Social Problems, 25*(1), 103-114.

Anderson, J. C., & Gerbing, D. W. (1991). Predicting the performance of measures in a confirmatory factor analysis with a pretest assessment of their substantive validities. *Journal of Applied Psychology, 76*(5), 732.

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*(7), 1073-1091.

Aronson, E., & Carlsmith, J.M. (1968). Experimentation in social psychology. In G. Lindzey & E. Aronson (Eds.), *The Handbook of Social Psychology* (pp. 1-79). Addison-Wesley.

Aryee, S., Budhwar, P. S., & Chen, Z. X. (2002). Trust as a mediator of the relationship between organizational justice and work outcomes: Test of a social exchange model. *Journal of Organizational Behavior, 23*(3), 267-285.

Ashton-James, C. E., & Ashkanasy, N. M. (2005). What lies beneath? A process analysis of affective events theory. *Research on Emotion in Organizations, 1*, 23-46.

Ayyagari, R., & Tyks, J. (2012). Disaster at a university: A case study in information security. *Journal of Information Technology Education, 11*, 85-96.

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

Bachman, R., Paternoster, R., & Ward, S. (1992). The rationality of sexual offending: Testing a deterrence/rational choice conception of sexual assault. *Law & Society Review, 26*(2), 343-372.

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.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science, 16*(1), 74-94.

Bahr, G. S., & Ford, R. A. (2011). How and why pop-ups don't work: Pop-up prompted eye movements, user affect and decision making. *Computers in Human Behavior, 27*(2), 776-783.

Banerjee, D., Cronan, T. P., & Jones, T. W. (1998). Modeling IT ethics: A study in situational ethics. *MIS Quarterly, 22*(1), 31-60.

Bansal, P., & Corley, K. (2012). Publishing in AMJ-Part7: What's different about qualitative research? *Academy of Management Journal, 55*(3), 509-513.

Barclay, J. H., & Harland, L. K. (1995). Peer performance appraisals: The impact of rater competence, rater location, and rating correctability on fairness perceptions. *Group and Organization Management, 20*, 39-60.

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.

Barnett, T., Bass, K., & Brown, G. (1994). Ethical ideology and ethical judgment regarding ethical issues in business. *Journal of Business Ethics, 13*(6), 469-480.

Baruch, Y., & Holtom, B. C. (2008). Survey response rate levels and trends in organizational research. *Human Relations, 61*(8), 1139-1160.

Baskerville, R., Park, E. H., & Kim, J. (2014). An emote opportunity model of computer abuse. *Information Technology & People, 27*(2), 155-181.

Bauer, J., & van Eeten, M. (2009). Cybersecurity: Stakeholder incentives, externalities and policy options. *Telecommunications Policy, 33*(10-11), 706-719.

Becker, G. S. (1974). Crime and punishment: An economic approach. In: Essays in the economics of crime and punishment. *NBER*, 1-54.

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

Berry, C. M., Ones, D. S., & Sackett, P. R. (2007). Interpersonal deviance, organizational deviance, and their common correlates: A review and meta-analysis. *Journal of Applied Psychology, 92*(2), 410-424.

Bies, R. J., & Moag, J. F. (1986). Interactional justice: Communication criteria of fairness. In R. Lewicki, M. Bazerman & B. Sheppard (Eds.), *Research on negotiation in organization*s (Vol. 1, pp. 43-55). Greenwich, CT: JAI Press.

Boudreau, M., Gefen, D., & Straub, D. (2001). Validation in IS research: A state-of-the-art assessment. *MIS Quarterly, 25*(1), 1-23.

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

Boss, S. R., & Kirsch, L. J. (2007, December). *The last line of defense: Motivating employees to follow corporate security guidelines* [Paper presentation]. 28th International Conference on Information Systems, Montreal.

Brotheridge, C. M. (2003). The role of fairness in mediating the effects of voice and justification on stress and other outcomes in a climate of organizational change. *International Journal of Stress Management, 10*(3), 253-268.

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.

Cappetta, R., & Magni, M. (2015). Locus of control and individual learning: The moderating role of interactional justice. *International Journal of Training and Development,* 19(2), 110-124.

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

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. *Journal of Information Privacy & Security, 1*(3), 18-40.

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.

Cenfetelli, R. T. (2004). *Getting in touch with our feelings towards technology. In Best Paper Proceedings of the Academy of Management Conference* (pp. F1-F6). New Orleans, LA.

Chen, C., Chen, M. Y., & Liu, Y. (2013). Negative affectivity and workplace deviance: the moderating role of ethical climate. *The International Journal of Human Resource Management, 24*(15), 2894-2910.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, O. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security, 39*, 447-459.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems, 29*(3), 157-188.

Chen, X., Wu, D., Chen, L., & Teng, J. K. L. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management, 55*(8), 1049-1060.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research, 295*(2), 295-336.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research, 14*(2), 189-217.

Chu, A. M. Y., & Chau, P. Y. K. (2014). Development and validation of instruments of information security deviant behavior. *Decision Support Systems, 66*, 93-101.

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.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Erlbaum.

Cohen, J. (1992). A power primer. *Psychological Bulletin, 112*(1), 155-159.

Cole, E. (2015). Insider threats and the need for fast and directed response. SpectorSoft, https://www.sans.org/reading-room/whitepapers/analyst/insider-threats-fast-directed-response-35892

Colquitt, J. A. (2001). On the dimensionality of organizational justice: A construct validation of a measure. *Journal of Applied Psychology, 86*(3), 386-400.

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

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology, 92*(4), 909-927.

Comesaña, M., Soares, A. P., Perea, M., Piñeiro, A. P., Fraga, I., & Pinheiro, A. (2013). ERP correlates of masked affective priming with emoticons. *Computers in Human Behavior, 29*(3), 588-595.

Compeau, D., Marcolin, B., Kelley, H., & Higgins, C. (2012). Generalizability of information systems research using student subjects – a reflection of our practices and recommendations for future research. *Information Systems Research, 23*(4), 1093-1109.

Copes, H. (2003). Societal attachments, offending frequency, and techniques of neutralization. *Deviant Behavior, 24*(2), 101-127.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017) Organizational information security policies: A review and research framework. *European Journal of Information Systems, 26*(6), 605-641.

Crede, M., Chernyshenko, O. S., Stark, S., Dalal, R. S., & Bashshur,M. (2007). Job satisfaction as mediator: An assessment of job satisfaction's position within the nomological network. *Journal of Occupational and Organizational Psychology, 80*(3), 515-538.

Creswell, J. W. (2002). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research*. Merrill Prentice Hall.

Creswell, J. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches.* Sage Publications.

Cromwell, P., & Thurman, Q. (2003). The devil made me do it: Use of neutralizations by shoplifters. *Deviant Behavior, 24*(6), 535-550.

Cropanzano, R., Stein, J. H., & Nadisic, T. (2011). *Social justice and the experience of emotion*. Routledge.

Cropanzano, R., Bowen, D. E., & Gilliland, S. (2007). The management of organizational justice. *Academy of Management Perspectives, 21*(4), 34-48.

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

CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper. (2013, June 17). *2013 US State of Cybercrime Survey*. https://resources.sei.cmu.edu/asset_files/Presentation/2013_017_101_58739.pdf.

Dalal, R. S., Lam, H., Weiss, H. M., Welch, E. R., & Hulin, C. L. (2009). A within-person approach to work behavior and performance: Concurrent and lagged citizenship-counter productivity associations, and dynamic relationships with affect and overall job performance. *Academy of Management Journal, 52*(5), 1051-1066.

Diamantopoulos, A., & Winklhofer, H. M. (2001). Index construction with formative indicators: An alternative to scale development. *Journal of marketing research, 38*(2), 269-277.

Dell. (2015). Insider threat spotlight report. https://software.dell.com/whitepaper/insider-threat-spotlight-report890546/

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80.

Djamasbi, S. (2007). Does positive affect influence the effective usage of a Decision Support System? *Decision Support Systems, 43*(4), 1707-1717.

Djamasbi, S., & Strong, D. M. (2008). The effect of positive mood on intention to use computerized decision aids. *Information & Management, 45*(1), 43-51.

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.

Doherty, N., & Fulford, H. (2005). Do information security policies reduce the incident of security breaches: An exploratory analysis. *Information Resources Management Journal, 18*(4), 21-39.

Dolnicar, S. (2003). Simplifying three-way questionnaires - do the advantages of binary answer categories compensate for the Loss of information. *Proceedings of the (ANZMAC) Marketing Academy Conference,* Australia and New Zealand, 1-8.

Douglas, S. C., & Martinko, M. J. (2001). Exploring the role of individual differences in the prediction of workplace aggression. *Journal of Applied Psychology, 86(4),* 547-559.

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.

Dutton, D. G. (1986). Wife assaulter's explanations for assault: The neutralization of self-punishment. *Canadian Journal of Behavioural Science/Revue Canadienne Des Sciences Du Comportement*, *18*(4), 381-390.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, *22*(5), 474-489.

D'Arcy, J., & 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., Hovay 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.

D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal, 29*, 43-69.

Eagleman, D. (2011). There is someone in my head, but it is not me. In *Incognito: The secret lives of the brain* (1st ed., pp. 1–20). Vintage Books.

Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes.* Harcourt Brace Jovanovich.

Eddy, E. R., D'Abate, C. P., & Thurston, Jr. P. W. (2010). Explaining engagement in personal activities on company time. *Personnel Review, 39*(5), 639-654.

Ellis, T., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology, 6*, 323-337.

Ellis, T. J., & Levy, Y. (2012). Data sources for scholarly research: Towards a guide for novice researchers. *Proceedings of Informing Science & IT Education Conference.* http://proceedings.informingscience.org/InSITE2012/InSITE12p405-416Ellis0114.pdf

Elovainio, M., Kivimaki, M., Steen, N., & Vahtera, J. (2004). Job decision latitude, organizational justice and health: multilevel covariance structure analysis. *Social Science and Medicine, 58*(9), 1659-1669.

Elster, J. (1986). *Rational choice*. New York University Press.

Emerson, E., Felce, D., & Stancliffe, R. J. (2013). Issues concerning self-report data and population-based data sets involving people with intellectual disabilities. *Journal of intellectual and developmental disabilities, 51*(5), 333-348.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics, 5*(1), 1-4.

Fassina, N. E., Jones, D. A., & Uggerslev, K. L. (2008). Meta-analytic tests of relationships between organizational justice and citizenship behavior: Testing agent-system and shared variance models. *Journal of Organizational Behavior, 29*(6), 805-828.

Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods, 41*, 1149-1160.

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

Finch, J. (1987). The vingnette technique in survey research. *Sociology, 21*(1), 105-114.

Finucane, M. L., Alhakami, A., Slovic, P., & Johnson, S.M. (2000). The affect heuristic in judgments of risks and benefits. *Journal of Behavioral Decision Making, 13*(1), 1-17.

Folger, R., & Cropanzano, R. (1998). *Organizational justice and human resource management*. Sage Publications.

Forbes Insights (2017, July 1). *Enterprises re-engineer security in the age of digital transformation*. http://media.cms.bmc.com/documents/Forbes_Insights_SecOps_Survey.pdf?elqTrackId=4dc60730d916444ab83e697a97760ae8&elq=fabd8c3bd9714e25a1b915f46abf6708&elqaid=2152&elqat=1&elqCampaignId=1899.

Forgas, J. P. (2008). Affect and cognition. *Perspectives on Psychological Science, 3*(2), 94-101.

Fornell, C. & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*, 39-50.

Francis, L., & Barling, J. (2005). Organizational injustice and psychological strain. *Canadian Journal of Behavioural Science, 37*(4), 250-261

Furnell, S., & Thomson, K. (2009). From culture to disobedience: Recognizing the varying user acceptance of IT security. *Computers & Security, 2009*(2), 5-10.

Gefen, D., Straub, D., & Boudreau, M. (2000). Structural equation modeling techniques and regression: Guidelines for research practice. *Communications of AIS, 7*(7), 1-78.

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*(1), 91-109.

Gonzalez, J. J., & Sawicka, A. (2002). A framework for human factors in information security. *In: Proceedings of the 2002 WSEAS International Conference on Information Security (ICIS'02)*, Rio de Janeiro

Greenberg, J. (2006). Losing sleep over organizational injustice: Attenuating insomniac reactions to underpayment inequity with supervisory training in interactional justice. *Journal of Applied Psychology, 91*(1), 58-69.

Greenberg, J. (1990). Employee theft as a reaction to underpayment inequity: The hidden cost of pay cuts. *Journal of Applied Psychology, 75*(5), 561-568.

Guhr, N., Lebek, B., & Breitner, M. H. (2018). The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. *Information Systems Journal, 29*(2), 340-362.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis* (7th Ed.). Prentice Hall.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing theory and Practice, 19*(2), 139-152.

Hair, J. F., Hult, J. T. M., Ringle, C. M., & Sarstedt, M. (2014). *A primer on partial least squares structural equation modeling (PLS-SEM)* (1st ed.). Sage Publications.

Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)* (2nd ed.). Sage Publications.

Hair, J., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1).

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.

Hassanzadey, M., Jahangiri, N. & Brewster, B. (2014). *Emerging trends in ICTs security. A conceptual framework for information security awareness, assessment, and training.* Morgan Kaufmann.

Hedstrom, K., Kolkowska, E., Karlsson, F. & Allen, J. (2011). Value conflicts for information security management. *Journal of Strategic Information Systems*, *20*, 1-12.

Hechter, M., & Kanazawa, S. (1997). Sociological rational choice theory. *Annual Review of Sociology*, *23*(1), 191-214.

Henry, S. (2009). *Social deviance*. (1st ed.). Polity Press.

Henry, S., & Eaton, R. (1989). *Degrees of deviance: Student accounts of their deviant behavior.* Gower Publishing Company.

Henry, J. (2019, April 7). *These 5 types of insider threats could lead to costly data breaches*. https://securityintelligence.com/these-5-types-of-insider-threats-could-lead-to-costly-data-breaches/

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115-135.

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.

Hershcovis, M. S., Turner, N., Barling, J., Arnold, K. A., Dupré, K. E., Inness, M., LeBlanc, M. M., & Sivanathan, N. (2007). Predicting workplace aggression: A meta-analysis. *Journal of Applied Psychology*, *92*(1), 228-238.

Hinkin, T. R. (1998). A brief tutorial on the development of measures for use in survey questionnaires. *Organizational Research Methods*, *1*(1), 104-121.

Hoffman, K.D. & Kelley, S.W. (2000). Perceived justice needs and recovery evaluation: A contingency approach. *European Journal of Marketing*, *34*(3/4), 418-432.

Homans, G. C. (1974). *Social behavior: Its elementary forms* (Revised ed.). Harcourt Brace Jovanovich.

Höne, K., & Eloff, J. H. P. (2002). Information security policy - what do international information security standards say? *Computers & Security, 21*(5), 402-409.

Hooper, D., Coughlan, J., & Mullen, M. R. (2008). Structural equation modelling: Guidelines for determining model fit. *Electronic Journal of Business Research Methods, 6*(1), 53-60.

Houston, J., & Tran, A. (2001). A survey of tax evasion using the randomized response technique. *Advances in Taxation*, 69-94.

Hu, L., & Bentler, P. M. (1998). Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification. *Psychological Methods, 3*(4),424-453

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

Hu, Z., & Qin, J. (2018). Generalizability of causal inference in observational studies under retrospective convenience sampling. *Statistics in Medicine, 37*, 2874-2883.

Hubbel, A. P., & Chory-Assad, R. M. (2005). Motivating factors: Perceptions of justice and their relationship with managerial and organizational trust. *Communication Studies, 56*(1), 47-70.

Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: A review of four recent studies. *Strategic Management Journal, 20*(2), 195-204.

Humphrey, R. H. (2006). Promising research opportunities in emotions and coping with conflict. *Journal of Management and Organization, 12*(2), 179-186.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69-79.

IIies, 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.

Ilies, R., Scott, B. A., & Judge, T. A. (2006). The interactive effects of personal traits and experienced states on intraindividual patterns of citizenship behavior. *Academy of Management Journal, 49*(3), 561-575.

ISACA. (2019, April 8). *State of cybersecurity implications for 2016. An ISACA and RSA conference survey*. http://www.isaca.org/cyber/pages/state-of-cybersecurity-implications-for-2016.aspx?utm_referrer=

Jasso, G. (2006). Factorial survey methods for studying beliefs and judgments. *Sociological Methods and Research, 34*(3), 334-423.

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

Jones, D. A. (2009). Getting even with one's supervisor and one's organization: Relationships among types of injustice, desires for revenge, and counterproductive work behaviours. *Journal of Organizational Behaviour, 30*(4), 525-542.

Judge, T. A., (1992). The dispositional perspective in human resources research. *Research in Personnel and Human Resources Management, 10,* 31-72.

Judge, T. A., & Kammeyer-Mueller, J. D. (2012). Job attitudes. *Annual Review of Psychology, 63*, 341-367.

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), 126-38.

Judge, T. A., Woolf, E. F., & Hurst, C. (2009). Is emotional labor more difficult for some than for others? A multilevel, experience-sampling study. *Personnel Psychology, 62*(1), 57-88.

Karahann, E., Straub, D. W. & Chervany, N. L. (1999). Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS Quarterly, 23*(2), 183-213.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal, 25*(6), 607-635.

Khattak, M. N., Zolin, R., & Mohammad, N. (2020). The combined effect of perceived organizational injustice and perceived politics on deviant behaviors. *International Journal of Conflict Management.* https://doi.org/10.1108/IJCMA-12-2019-0220

Kieser, M., & Wassmer, G. (1996). On the Use of the Upper Confidence Limit for the Variance from a Pilot Sample for Sample Size Determination. *Biometrical Journal, 38*(8), 941-949.

King, W., & Jun, H. (2005). External validity in IS survey research. *Communications of the Association for Information Systems, 16*, 880-894.

King, R. B., McInerney, D. M., Ganotice Jr., F. A., & Villarosa, J. B. (2015). Positive affect catalyzes academic engagement: Cross-sectional, longitudinal, and experimental evidence. *Learning and Individual Differences, 39*, 64-72.

Kline, R. B. (2012). Assumptions in structural equation modeling. In R. H. Hoyle (Ed.), *Handbook of structural equation modeling.* Guilford Press

Kline, R. B. (2011). *Principles and practice of structural equation modeling*. Guilford Press.

Klockars, C. B. (1974). *The professional fence.* Free Press.

Knapp, H., & Kirk, S. A. (2003). Using pencil and paper, Internet, and touch-tone phones for self-administered surveys: Does methodology matter. *Journal of Computers in Human Behavior, 19*(1), 117-134.

Kock, N. (2015). One-tailed or two-tailed P values in PLS-SEM? *International Journal of e-Collaboration (IJeC), 11*(2), 1-7.

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics, 38*(2), 143-154.

Lavelle, J. J., Rupp, D. E., & Brockner, J. (2007). Taking a multifoci approach to the study of justice, social exchange, and citizenship behavior: The target similarity model. *Journal of Management, 33*(6), 841-866.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review, 37*(12), 1049-1092.

Lee, A. S., & Baskerville, R. L. (2003). Generalizing generalizability in information systems research. *Information Systems Research, 14*(3), 221-243.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security, 10*(2/3), 57-63.

Lee, H. K., Keil, M. K., Smith, H. J., & Sarkar, S. (2017). The roles of mood and conscientiousness in reporting of self-committed errors on IT projects. *Information Systems Journal, 27*(5), 589-617.

Leedy, P. D., & Ormrod, J. E. (2005). *Practical research: Planning and design* (8th ed.). Pearson Prentice Hall.

Lerner, J. S., & Keltner, D. (2000). Beyond valence: Toward a model of emotion-specific influences on judgment 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*. Plenum.

Levy, Y. (2006). *Assessing the value of e-learning systems*. Information Science Publishing.

Levy, Y., & Danet, T. (2010). Implementation success model in Government agencies: A case of a centralized identification system at NASA. *International Journal of Information Systems in the Service Sector, 2*(2), 19-32.

Levy, Y., & Green, B. (2009). An Empirical Study of Computer Self-Efficacy and the Technology Acceptance Model in the Military: A Case of a U.S. Navy Combat Information System. *Journal of Organizational and End User Computing (JOEUC), 3*(21), 1-23.

Lewis-Beck, M., Bryman, A. E., & Liao, T. F. (2003). *The Sage encyclopedia of social science research methods.* Sage Publications.

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems, 51*(3), 434-445.

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

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.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13-24.

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.

Lind, E. A., & Tyler, T. R. (1988). *The social psychology of procedural justice*. Plenum Press.

Loiacono, E., & Djamasbi, S. (2010). Moods and their relevance to systems usage models within organizations: An extended framework. *Transactions on Human-Computer Interaction, 2*(2), 55-72.

Lowry, P. B., Twyman, N. W., Pickard, M., Jenkins, J. L., & Bui, Q. N. (2014). Proposing the affect-trust infusion model (ATIM) to explain and predict the influence of high- and low-affect infusion on web-vendor trust. *Information Management, 51*(5), 579-594.

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. *Information Systems Journal, 25*, 433-463.

Lowry, P. B., Posey, C., Bennett, R. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal, 25*(3), 193-230.

Lyubomirsky, S., King, L., & Deiner, E. (2005). The benefits of frequent positive affect: Does happiness lead to success? *Psychological Bulletin, 131*(6), 803-855.

Ma, Q., & Wang, K. (2009). The effect of positive emotion and perceived risk on usage intention to online decision aids. *CyberPsychology & Behavior, 12*(5), 529-532.

Mahalanobis, P. C. (1936). On the generalized distance in statistics. *National Institute of Science of India, 2*, 49-55.

Mangione, T. (1995). *Mail surveys: Improving the quality*. Sage Publications, Inc.

Mayr, S., Erdfelder, E., Buchner, A., & Faul, F. (2007). A short tutorial of GPower. *Tutorials in Quantitative Methods for Psychology, 3*(2), 51-59.

Matta, F. K., Scott, B. A., Colquitt, J. A., Koopman, J., & Passantino, L. G. (2017). Is consistently unfair better than sporadically fair? An investigation of justice variability and stress. *Academy of Management Journal, 60*(2), 743-770.

Maruna, S., & Copes, H. (2005). What have we learned from five decades of neutralization theory research? *Crime and Justice, 32*, 221-320.

Masterson, S. S., Lewis-Mcclear, K., Goldman, B. M., & Taylor, S. M. (2000). Integrating justice and social exchange: The differing effects of fair procedures and treatment on work relationships. *Academy of Management Journal, 43*(4), 738-748.

McCarthy, B. (2002). New economics of sociological criminology. *Annual Review of Sociology, 28*(1), 417-42.

Mertler, C. A., & Reinhart, R. V. (2017). *Advanced and multivariate statistical methods: Practical application and interpretation* (6th ed.). Routledge.

Mertler, C., & Vannatta, R. A. (2013). *Advanced and multivariate statistical methods.* Pyrczak Publishing.

Milne, G. R., & Bahl, S. (2010). Are there differences between consumers' and marketers' privacy expectations? A segment-and technology-level analysis. *Journal of Public Policy & Marketing, 29*(1), 138-149.

Mitchell, L. D. (2011). Job satisfaction and affective events theory: What have we learned in the last 50 years? *Business Renaissance Quarterly, 6*(2), 43-53.

Mitchell, M. S., & Ambrose, M. L. (2007). Abusive supervision and workplace deviance and the moderating effects of negative reciprocity beliefs. *Journal of Applied Psychology, 92*(4), 1159-1168.

Minor, W. W. (1981). Techniques of neutralization: A reconceptualization and empirical examination. *Journal of Research in Crime and Delinquency, 18*(2), 295-318.

Moon, J., & Kim, Y. (2001). Extending the TAM for a World-Wide-Web context. *Information & Management, 38*(4), 217-230.

Moorman, R. H. (1991). Relationship between organizational justice and organizational citizenship behaviors: Do fairness perceptions influence employee citizenship? *Journal of Applied Psychology, 76*(6), 845-855.

Nagin, D. S., & Pogarsky, G. (2001). Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence and evidence. *Criminology, 39*(4), 865-891.

Newton, J. D., Newton, F. J., Ewing, M. T., Burney, S., & Hay, M. (2013). Conceptual overlap between moral norms and anticipated regret in the prediction of intention: Implications for theory of planned behaviour research. *Psychology & Health, 28*(5), 495-513.

Neys, W. D. (2006). Dual processing in reasoning: Two systems but one reasoned. *Psychological Science, 17*(5), 428-434.

Ng, B. Y., & Xu, Y. (2007). Studying users' computer security behavior using the health belief model. *PACIS 2007 Proceedings, 45*, 423-437.

Niedhammer, I., Tek, M. L., Starke, D., & Siegrist, J. (2004). Effort-reward imbalance model and self-reported health: Cross sectional and prospective findings from the GAZEL cohort. *Social Science & Medicine, 58*(8), 1531-1541.

Norman, D.A. (2002). Emotion and design: Attractive things work better. *Interactions: New Visions of Human-Computer Interaction IX, 4*, 36-42.

Oblinger, D. G., & Hawkins, B. L. (2006). The myth about IT security. *Educause Review, 41*(3), 14-15.

Olson, K. (2010). An examination of questionnaire evaluation by expert reviewers. *Field Methods, 22*(4), 295-318.

Organ, D. W., & Konovsky, M. A. (1989). Cognitive versus affective determinants of organizational citizenship behavior. *Journal of Applied Psychology, 74*(1), 157-164.

Organ, D. W., & Near, J. P. (1985). Cognition vs. affect in measures of job satisfaction. *International Journal of Psychology, 20*(2), 241-253.

Panaccio, A., Vandenberghe, C., & Ayed, A. K. B. (2014). The role of negative affectivity in the relationships between pay satisfaction, affective and continuance commitment and voluntary turnover: A moderated mediation model. *Human Relations, 67*(7), 821-848.

Paternoster, R., & Pogarsky, G. (2009). Rational choice, agency and thoughtfully reflective decision making: The short and long-term consequences of making good choices. *Journal of Quantitative Criminology, 25*(2), 103-127.

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.

Pessoa, L. (2008). On the relationship between emotion and cognition. *Nature Reviews Neuroscience, 9*(2), 148-158.

Pham, M. T., Cohen, J. B., Pracejus, J. W., & Hughes, G. D. (2001). Affect monitoring and the primacy of feelings in judgment. *Journal of Consumer Research, 28*(2), 167-188.

Pinsonneault, A., & Kraemer, K. (1993). Survey research methodology in management information systems: an assessment. *Journal of Management Information Systems, 10*(2), 75-105.

Piquero, A., & Hickman, M. (1999). An empirical test of Tittle's control balance theory. *Criminology, 37*(2), 319-342.

Piquero, N. L., Tibbetts, S. G., & Blankenship, M. B. (2005). Examining the role of differential association and techniques of neutralization in explaining corporate crime. *Deviant Behavior, 26*(2), 159-188.

Pfleeger, C. P., & Pfleeger, S.L. (2003). *Security in computing* (3rd ed.). Prentice Hall, division of Pearson Education Inc.

Posey, C., Bennett, R. J., Roberts, T. L., & Lowry, P. B. (2011). When computer monitoring backfires: Privacy invasions and organizational injustice as precursors to computer abuse. *Journal of Information System Security, 7*(1), 24-47.

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information Management, 51*(5), 551-567.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179-214.

Post, G., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security, 26*(3), 229-237.

PwC. (2019, April 7). *The global state of information security survey*. http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml

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

Rapaport, P., & Orbell, S. (2000). Augmenting the theory of planned behaviour: Motivation to provide practical assistance and emotional support to parents. *Psychology & Health, 15*(3), 309-324.

Renaud, K. (2011). Simply blaming non-compliance is too convenient: What really causes information breaches? *IEEE Security and Privacy,* 1-11.

Rea, L. M., & Parker, R. A. (2014). *Designing and conducting survey research: A comprehensive guide*. John Wiley & Sons.

Richard, R., de Vries, N. K., & van der Pligt, J. (1998). Anticipated regret and precautionary sexual behavior. *Journal of Applied Social Psychology, 28*(15), 1411-1428.

Robinson, S. L., & Bennett, R. J. (1995). A typology of deviant workplace behaviors: A multidimensional scaling study. *Academy of Management Journal, 38*(2), 555-572.

Rodell, J. B., & Judge, T. A. (2009). Can "good" stressors spark "bad" behaviors? The mediating role of emotions in links of challenge and hindrance stressors with citizenship and counterproductive behaviors. *Journal of Applied Psychology, 94*(6), 1438-1451.

Rogers, J. W., & Buffalo, M. D. (1974). Neutralization techniques: Toward a simplified measurement scale. *Pacific Sociological Review, 17*(3), 313-331.

Rosenbaum, A., Rabenhorst, M. M., Reddy, M. K., Fleming, M. T., & Howells, N. L. (2006). A comparison of methods for collecting self-report data on sensitive topics. *Journal of Violence and Victims, 21*(4), 461-71.

Rothbard, N. P., & Wilk, S. L. (2011). Waking up on the right or wrong side of the bed: Start-of-workday mood, work events, employee affect, and performance. *Academy of Management Journal, 54*(5), 959-980.

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

Safa, N. S., Sookhak, M. S., Solms, R. V., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & security*, *56*, 70-82.

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

Salami, S. O. (2010). Job stress and counterproductive work place behavior: Negative affectivity as a moderator. *The Social Sciences, 5*(6), 486-492.

Salkind, N. J. (2012). *Exploring research* (8th ed.). Pearson Education Inc.

Samnani, A., Salamon, S. D., & Singh, P. (2014). Negative affect and counterproductive workplace behavior: The moderating role of moral disengagement and gender. *Journal of Business Ethics, 119*(2), 235-244.

Sarwar, A., & Mohammad, L. (2020). Impact of employee perceptions of mistreatment on organizational performance in the hotel industry. *International Journal of Contemporary Hospitality Management, 32*(1), 230-248

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

Schultz, E. (2005). The human factor in security. *Computers & Security, 24*, 425-426.

Sekaran, U. (2002). *Research methods for business. A skill building approach* (4th ed.). John Wiley & Sons Inc.

Sekaran, U., & Bougie, R. (2013). *Research methods for business: A skill-building approach* (6th ed.). John Wiley & Sons Inc.

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.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177-191.

Sindhav, B., Holland, J., Rodie, A.R., Adidam, P.T. & Pol, L.G. (2006). The impact of perceived fairness on satisfaction: Are airport security measures fair? Does it matter? *Journal of Marketing Theory and Practice, 14*(4), 323-335.

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., Mahmood, A., & Pahnila, S. (2009). Are employees putting your company at risk by not following information security policies? *Communications of the ACM, 52*(12), 145-147.

Siponen, M., Mahmood, A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.

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

Siponen, M. T., Vance, A., & Willison, R. (2012). New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs. *Information & Management, 49*(7-8), 334-341.

Siponen, M., Pahnila, S., & Mahmood, A. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64-71.

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2004). Risks as analysis and risks as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk Analysis, 24*(2), 311-322.

Skarlicki, D. P., & Folger, R. (1997). Retaliation in the workplace: The role of distributive, procedural, and interactional justice. *Journal of Applied Psychology, 82*(3), 434-443.

Skinner, R., Nelson, R. R., Chin, W. W., & Land, L. (2015). The Delphi method research strategy in studies of information systems. *Communications of the Association for Information Systems, 37*, 31-63.

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

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2016). SECURQUAL: An Instrument for evaluating the effectiveness of enterprise information security programs. *Journal of Information Systems, 30*(1), 71-92.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-169.

Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS Positivist research. *Communications of the Association for Information Systems, 13*(24), 380-427.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

Sulu, S., Ceylan, A., & Kaynak, R. (2010). Work alienation as a mediator of the relationship between organizational injustice and organizational commitment: Implications for healthcare professionals. *International Journal of Business and Management, 5*(8), 27-38.

Syed, F., Naseer, S., & Bouckenooghe, D. (2020). Unfairness in stressful job environments: The contingent effects of perceived organizational injustice on the relationships between job stress and employee behaviors. *Journal of General Psychology*, https://doi.org/10.1080/ 00221309.2020.1747968

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

Taguchi, G., Chowdury, S., & Wu, Y. (2001), *The Mahalanobis Taguchi system*. McGraw Hill.

Teh, P., Ahmed, P. K., & D'Arcy, J. (2015). What drives information security policy violations among banking employees? Insights from neutralization and social exchange theory. *Journal of Global Information Management, 23*(1), 44-64.

Teo, T. S. H., Srivastava, S. C., & Jiang, L. (2008) Trust and electronic government success: An empirical study. *Journal of Management Information Systems, 25*(3), 99-132.

Tepper, B. J. (2001). Health consequences of organizational injustice: Tests of main and interactive effects. *Organizational Behavior and Human Decision Processes, 86*(2), 197-215.

Thatcher, J. B., & Perrewé, P. L. (2002). An empirical examination of individual traits as antecedents to computer anxiety and computer self-efficacy. *MIS Quarterly, 26*(4), 381-396.

Thong, J. Y. L., & Yap, C. S. (1998). Testing an ethical decision-making theory: The case of softlifting. *Journal of Management Information Systems, 15*(1), 213-227.

Thurman, Q. C. (1984). Deviance and the neutralization of moral commitment: An empirical analysis. *Deviant Behavior, 5*(1-4), 291-304.

Trochim, W. M. K., & Donnelly, J. P. (2008). *The research methods knowledge base* (3rd ed.). Atomic Dog.

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., & Bies, R. (1990). Beyond formal procedures: The interpersonal context of procedural justice. In J. S. Carroll (Ed.), *Applied social psychology and organizational settings* (pp. 77-98). Erlbaum.

Ullman, J. B., & Bentler, P. M. (2003). *Handbook of Psychology Structural equation modeling* (2nd ed.). John Wiley.

van der Heijden, H. (2003). Factors influencing the usage of Web sites: The case of a generic portal in the Netherlands. *Information & Management, 40*(6), 541-549.

Vance, A., & Siponen, M. T. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational End User Computing, 24*(1), 21-41.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information Management, 49*(3/4), 190-198.

Venkatesh, V. (1999). Creation of favorable user perceptions: Exploring the role of intrinsic motivation. *MIS Quarterly, 23*(2), 239-260.

Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information Systems Research, 11*(4), 342-365.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478.

Venkatesh, V., & Speier, C. (1999). Computer technology training in the workplace: A longitudinal investigation of the effect of mood. *Organizational Behavior and Human Decision Processes, 79*(1), 1-28.

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

Wagner, A., Krasnova, H., Abramova, O., Buxmann, P., & Benbasat, I. (2018). From privacy calculus to social calculus: Understanding self-disclosure on social networking sites. *ICIS 2018 Proceedings*.

Wakefield, R. (2013). The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems, 22*(2), 157-174.

Walter, F., & Bruch, (2009). An affective events model of charismatic leadership behavior: A review, theoretical integration, and research agenda. *Journal of Management, 35*(6), 1428-1452.

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., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems, 18*(2), 101-105.

Watson, D., & Clark, L. (1984). Negative affectivity: The disposition to experience aversive emotional states. *Psychological Bulletin, 96*(3), 465-490.

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.

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*. JAI Press.

Weston, R., & Gore Jr., P. A. (2006). A brief guide to structural equation modeling. *The Counseling Psychologist, 34*(5), 719-751.

Whitman, M. E., & Mattord, H. J. (2009). *Principles of information security* (3rd ed.). Thompson Course Technology.

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

Willison, R., Lowry, P. B., & Paternoster, R. (2018). A tale of two deterrents: Considering the role of absolute and restrictive deterrence in inspiring new directions in behavioral and organizational security. *Journal of the Association for Information Systems, 19(*12), 1187-1216.

Wolff, K., Nordin, K., Brun, W., Berglund, G., & Kvale, G. (2011). Affective and cognitive attitudes, uncertainty avoidance and intention to obtain genetic testing: An extension of the theory of planned behavior. *Psychology and Health, 26*(9), 1143-1155.

Wong, K. K.-K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin, 24*(1), 1-32.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.

Wright, T. A., Cropanzano, R., & Bonett, D. G. (2007). The moderating role of employee positive well-being on the relation between job satisfaction and job performance. *Journal of Occupational Health Psychology, 12*(2), 93-104.

Xue, Y., Liang, H., & Wu, L. (2010). Punishment, justice, and compliance in mandatory IT settings. *Information Systems Research, 22*(2), 400-414.

Yang, J., & Diefendorff, J. M. (2009). The relations of daily counterproductive workplace behavior with emotions, situational antecedents, and personality moderators: A diary study in Hong Kong. *Personnel Psychology, 62*(2), 259-295.

Yean, T. F., & Yusof, A. A. (2016). Organization injustice: A conceptual discussion. *Procedia – Social and Behavioral Sciences, 219*, 798-803.

Yin, D., Bond, S. D., & Zhang, H. (2014). Anxious or angry? Effects of discrete emotions on the perceived helpfulness of online reviews. *MIS Quarterly, 38*(2), 539-560.

Yoon, C., Hwang, J., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *The Journal of Information and Systems in Education, 23*(4), 407-415.

Yu, J., Hu, P. J., & Cheng, T. (2015). Role of affect in self-disclosure on social network websites: A test of two competing models. *Journal of Management Information Systems, 32*(2), 239-277.

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.

Zang, P., & Li, N. (2005). The importance of affective quality. *Communications of the ACM, 48*(9), 105-108.

Zhang, P., & Li, N. (2007). Positive and negative affect in IT evaluation: A longitudinal study. In *Proceedings of the Sixth Annual Workshop on HCI Research in MIS* (pp. 67-71). Montreal, Canada.

Zikmund, W. G. (2013). *Business research methods.* Dryden Press.

Zivkovic, J. (2012). Strengths and weaknesses of business research methodologies: Two disparate case studies. *Business Studies Journal*, *4*(2), 91-99.

Zohar, D. (1995). The justice perspective of job stress. *Journal of Organizational Behavior*, *16*(5), 487-495.