Spring 5-2020

Three Essays on Managing Information Security Using the Fraud Triangle

Randi Jiang

THREE ESSAYS ON MANAGING INFORMATION SECURITY USING THE FRAUD TRIANGLE

by

Randi Jiang, B.B.A., M.B.A.

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

COLLEGE OF BUSINESS
LOUISIANA TECH UNIVERSITY

May 2020

LOUISIANA TECH UNIVERSITY

GRADUATE SCHOOL

March 27, 2020
Date of dissertation defense

We hereby recommend that the dissertation prepared by

Randi Jiang

entitled **Three Essays on Managing Information Security Using the Fraud Triangle**

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

Doctor of Business Administration, Computer Information Systems Concentration

T. Selwyn Ellis, Supervisor of Dissertation Research

T. Selwyn Ellis,
Head of Computer Information Systems

Members of the Doctoral Committee:
Dr. Jae Ung Lee
Dr. John Lauck

Approved:

Christopher Martin
Dean of Business

Approved:

Ramu Ramachandran
Dean of the Graduate School

GS Form 13a
(01/19)

ABSTRACT

Managing information security has increasingly become more important as information security breaches, computer fraud, and other devastating events are increasingly more frequent and disrupting business processes. Information is one of the most important enterprise assets. Therefore, information is valuable and should be properly protected. Accounting employees are tasked with specific responsibilities of information risk management. Therefore, ineffectively managing accountants may result in countless problems for the company, not the least of which are reputational problems, loss of stock value, material financial reporting errors, and financial losses. In Essay 1, I examine the elements of the fraud triangle and the impact to specific information security policy violations of copying sensitive financial information. In Essay 2, I find the unexpected effects of implementing higher demands on accountants. In Essay 3, I explore a deeper dimension of the accountant's internal justification when considering a violation in information security policies. This dissertation considers the challenges of managing the human aspect especially the role of accountants in information security. Security techniques and management tools have caught the attention from both academia and practitioners. This dissertation examines the fraud triangle as a theoretical framework for information security risk management among accountants. In the three essays', I attempt to integrate security policy theory, management system theory, the fraud triangle, and moral disengagement theory to provide a deeper understanding of information security

management. The findings carry implications for not only for future research on security violation behaviors, but also for continuation of broadening the theoretical foundation of the fraud triangle for further empirical research and application.

APPROVAL FOR SCHOLARLY DISSEMINATION

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

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

Author_____

Date _____

GS Form 14
(5/03)

DEDICATION

I dedicate this dissertation to my loving and supportive parents, James J. Jiang and Eileen Jiang. Thank you for involuntarily joining me for the “roller coaster” of my career path. Thank you for always believing in me.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGMENTS

I owe a great deal of gratitude to many individuals for their contribution to this dissertation as well as my success in the doctoral program at Louisiana Tech University. First, I would like to thank the entire computer information systems department and accounting department for their transference of knowledge and plethora of academic experiences to help prepare me for the academic career path. I would like to thank Dr. Selwyn Ellis, Dr. Jae-Ung Lee, and Dr. John Lauck, members of my dissertation committee for their many hours of head-scratching and advice towards my dissertation. I look forward to continuing to produce quality research with the tools Louisiana Tech University has given me.

I would also like to thank Jimmy Chien, my husband for his endless patience and support during this doctoral journey. Thank you for always making me laugh and reminding me to enjoy the little things in life.

CHAPTER 1

INTRODUCTION

Organizations' heavy reliance on information systems (IS) requires them to manage the risks associated with those systems. Although the United States' Sarbanes-Oxley Act (SOX) of 2002 serves to improve corporate responsibility and internal controls, the financial reporting processes are driven through IS. Specific sections of the SOX (i.e., Section 404, 409,802) give a broad overview of the necessary IS controls to reach rigorous and secure internal controls regarding an organization's IS. In order to properly enhance an organization's security management, many organizations have chosen to use a security framework (i.e., COSO, COBIT, ISO177799). In order to comply with the security framework guidelines organizations are required to create information security policies (ISPs). These ISPs specify the standards, limitations, and responsibilities employees have in order to assist with the deterrence, detection, and response to IS security-related incidents (Bulgurcu et al. 2010).

Despite information security management's efforts, there continues to be an abundance of intentional ISP violations. Employee intentional ISP violations may vary from data entry, failing to log off work computers, sharing passwords, delaying backups, to using unsecured USB's (Guo 2013; Johnston et al. 2016). The malicious and intentional computer abuse ranges from deliberate insider sabotage to committing computer fraud (Willison and Warkentin 2013).

The risks associated with ISP violations are a significant challenge for many organizations, since these risks may warrant unwanted consequences; including corporate liability, reputational damages, and monetary loss (Berezina et al. 2012; Campbell et al. 2003).

From the theoretical perspective, the perspectives of employees in a position of trust within an organization have become a focal point of research. Previous research has shown that employees are often the weakest link in information security (Bulgurcu et al. 2010; Martins and Elofe 2002). Organizations create ISPs to provide guidelines to employees to ensure information security; however, these ISPs alone are not enough to prevent ISP violations. Unfortunately, limited attention has been paid to explain this phenomenon in accounting literature. Therefore, this dissertation will lay the foundation to understanding the motivations and reasoning behind accounting employees and their intentional information security policy (ISP) violations.

Theoretical Background

In my research, I apply the fraud triangle from the accounting literature and apply this as a basis of this dissertation (Cressey 1953; Dorminey et al. 2012). The fraud triangle implies interrelationships between three fraud risk categories called opportunity, rationalization, and pressure. The fraud triangle is the dominant framework in auditing and forensic accounting and is entrenched in the formal ethical standards of professional associations around the globe (Murphy and Free 2015). Each element of the fraud triangle has given auditors a framework to follow when attempting to explain fraudulent behavior. Each element of the fraud triangle has been conceptualized to explain fraudulent behavior, which is known as illegal and malicious behavior. The opportunity

for fraud is seldom purposefully provided to the employee; however, in the case of perceived opportunity for an intentional, but not malicious ISP violation, it will be commonly presented (i.e. copying data to bring home to complete work). Therefore, the perception of opportunity may not play as critical a role in intentional ISP violation behavior. The rationalization for malicious fraudulent behavior is expected to be more important than the rationalization for intentional but non-malicious ISP violations. Usually, the ethics of the employees will prevent them from violating the organization's ISP, as suggested in the existing literature (Bulgurcu et al. 2010; Chia and Lim 2000; Goles et al. 2006). The pressure for fraudulent behavior mainly refers to the pressure from a non-shareable financial problem (Dorminey et al., 2012), but in the context of intentional but non-malicious ISP violating behavior, a non-shareable financial problem is not expected to be the primary source of pressure. Instead, ISP controls are expected to become the source of pressure for the violation behavior. Therefore, in this dissertation, I explore the pressure element of the fraud triangle as the most critical trait to explain the effect ISP controls have on accountant's ISP violating intention.

The term ISP pressure in this dissertation describes the stressful demands specifically imposed by security requirements. The pressure to commit a violation intention can be caused by internal or external security-related demands (D'Arcy et al. 2014; Fogarty et al. 2000). Stress experienced in information technology is a multidimensional concept (Ragu-Nathan et al. 2008). Stress is defined in terms of stimulating conditions that produce reactions such as declining physical and mental health (Lazarus and Folkman 1984). The conditions reflect employees' struggles to deal with workplace technologies and depletion of cognitive resources related to their use.

Drawing upon information security literature, I use the construct of security-related stress (SRS) to define ISP pressure. SRS considers the overload, complexity, and uncertain dimensions of stress (D'Arcy et al. 2014; Tarafdar et al. 2010). In the context of my study, ISP overload describes situations where ISP requirements increase the workload for employees. Research indicates that employees view these ISPs to hinder their work productivity (Posey et al. 2011b; Stanton and Stam 2006). This overload in work duties can enhance the perception of ISP pressure employees feel when choosing to violate ISPs. For example, when employees perceive the ISP requirements to be time-consuming or inconvenient, they look for ways to complete their assigned work even if that means stepping outside of the ISP boundaries.

ISP complexity describes situations when ISP requirements are regarded as too complicated. Employees are forced to expend extra time and effort to learn and understand the ISPs. For example, the ISPs may involve overly complicated technical jargon, and employees must devote more time to understand the language (Puhakainen and Siponen 2010). These extra burdens to comply can be frustrating for employees.

ISP uncertainty refers to organizations continuously changing their job-related security requirements. Organizations have faced a sudden increase in information security requirements in recent years (Clayton 2017; Haried et al. 2019). This uncertainty can be disconcerting for employees and cause pressure for employees which causes them to choose to violate ISPs intentionally. Thus, in my dissertation, I further expand on the notion of how employees will react when ISP pressure levels are high.

Management control over the processes, activities, and behaviors of employees is an integral part of any organization. Management controls include devices and systems

managers use to guarantee that the behaviors of their employees are consistent with an organization's objectives (Malmi and Brown 2008). Accounting controls will include types of governance controls that monitor budget forecasts and performance measures (Fiolleau et al. 2018). These management controls enhance effective organizational operations, yet there is a growing body of accounting research that suggests formal controls can negatively affect the behaviors of employees subjected to these controls (Christ et al. 2008). Therefore, in this study, I assume an organization's formal ISPs as a type of mandatory control system. When policies are implemented into an organization, organizations assume employees will comply with the new changes (Chae and Poole 2005; Malhotra and Galletta 2005). However, prior research has used reactance theory as a theoretical lens to explain why high levels of ISP controls backfire and increase unwanted employee behavior (Lowry and Moody 2015). Therefore, I explore further this notion of why management controls on employees may not achieve the expected outcomes.

An employee's perception of truth and fairness depends on how he views the standards of true or false and fair or unfair. Information systems within organizations can reinforce or dissolve the perception of fairness. There is substantial evidence that employees' perceptions of fairness will play an imperative role when making business-related decisions (Colquitt et al. 2003). Individual perceptions of organizational justice can influence co-workers, superiors, and compliance towards policies of the organization (Colquitt et al. 2001; Leventhal et al. 1980; Li et al. 2014; Willison et al. 2018). I argue in this study that organizations need to examine perceptions of fairness within an organization as a possible motivator to unwanted ISP violations.

Organizational justice is manifested in four specific ways: interactional, informational, distributive, and procedural (Colquitt et al. 2001; Greenberg 1987). Interactional justice is the perceived fairness of how employees receive the explanation of formal procedures (Bies and Shapiro 1987). In other words, interactional justice reflects employees' feelings of how fairly managers treat them. Informational justice refers to fairness in the communication process of formal company procedures (Colquitt et al. 2001). For example, an employee's perception of the sincerity of communication would determine the level of informational justice. Distributive justice refers to the perceived fairness of outcomes (Colquitt et al. 2003). Procedural justice is the perceived fairness of the process (e.g., policies and procedures, and their enactments) of determining outcomes or resource distributions (Colquitt et al. 2001). In this study, formal procedure refers to a company's rules, regulations, or policies (i.e., ISPs) that precisely guide an organization's information security management.

The perception of fairness of authorities and co-workers is an essential factor when examining employee behavior (Alge 2001; Willison et al. 2018; Zhang 2008). In the context of information security, I also examine how employees may rationalize corporate misconduct when they feel they are not being treated fairly (Colquitt et al. 2012; Li et al. 2014; Posey et al. 2011a; Willison et al. 2018).

Research Focus of the Three Essays

With the need for effective information security management, my dissertation examines practical scenarios organizations often encounter.

In Essay 1 the first goal is to examine whether the three elements of the fraud triangle exposed to an individual will be equally important (i.e. work pressure plays a

more significant role than the other two points of the triangle when examining the intent to copy company data to complete their work at home). The second goal of the study is to assess whether work completion justification will enhance the resolve of employees to copy company data to complete their work at home.

Essay 2 focuses on how organizational ISP controls influence accountant's ISP violating intention via the fraud triangle elements. I also aim to understand whether or not an employee's ISP self-efficacy will relieve part of the ISP stress accounting employees may encounter. As regulations and guidelines for ISP implementation continue to rapidly change, the essay examines the perception of work uncertainty to give further understanding of how the climate within an organization can motivate accounting employees to intentionally violate ISPs.

Essay 3 explores the ISP pressure further by attempting to understand the rationalization an accounting employee may do when considering an intentional ISP violation decision. As accounting employees justify their choices, they may consider other external factors. I examine the organizational justice to understand the influence of the perceptions of justice when accounting employees conduct this rationalizing.

Drawing on the fraud triangle theory (Cressey 1953) as the overarching theory, I postulate that an accounting employee's intentional ISP violation behavior will be influenced by a perception of opportunity, work pressure, specific security-related pressure, and rationalization of their misconduct. Building on the fraud triangle theory, I propose antecedents such as the organizational controls, ISP self-efficacy, and examination of the environment for levels of uncertainty may influence an accounting employee's violation behavior. I also investigate the role of justice within an organization

and hypothesize that it influences an accounting employee's rationalization as well as their intention to violate ISPs.

In Chapter 2, I propose Essay 1. Essay 1 examines the specific phenomena of intentional ISP violations through a specific scenario of copying company data to complete their assigned work. In order to avoid a possible threat of unwanted data leakage, specific ISPs may prohibit employees from copying and removing company data from the work environment. However, as employees with accounting, financial, or IT responsibilities continue to be given a bigger work load, it has become challenging for them to finish their assigned work during traditional working hours.

Essay 1 uses the fraud triangle theoretical lenses to examine this data copying behavior. The fraud triangle theory emphasizes the motives of individuals as the most critical points of the triangle and opportunity and rationalization at the other points. Since this type of ISP violation has no malicious financial gain to the individual, the stress experienced by employees will be from the general pressures of their work. Opportunity means there are possibilities for the employees to be able to copy company data to complete their work. The rationalization point in Essay 1 is constructed as an employee's level of personal technological idealism. This motivation will be the driving need for employees to complete their work. Work completion justification is hypothesized to enhance an employee's intentional ISP violation behavior.

In Chapter 3, I propose Essay 2. Essay 2 examines the roots of the three corners of the fraud triangle to further understand why accounting employees continue to display intentional ISP violation behaviors. The creation of the ISPs is to facilitate, prevent, and detect security incidents. Therefore, the first step to examine why intentional ISP

violations are still occurring, I look at how accounting employees perceive their organizations level of ISP control. Since accounting literature has thoroughly examined how accounting employees experience high levels of stress, I research some of the possible contributing factors to their ISP stress such as ISP self-efficacy and the organization's level of work uncertainty. In order to match the proper stress to ISP violation behavior, Essay 2 examines the specific ISP stress accountants may encounter (D'Arcy et al. 2014). These specific security strains are comprised of ISP uncertainty, ISP overload, and ISP complexity. Essay 2 stretches the boundaries of the fraud triangle to investigate causes and extends its application to ISP violations beyond the normal fraudulent behavior.

In Chapter 4, I propose Essay 3. Essay 3 further expands the understanding of the rationalization corner of the fraud triangle. The rationalization an individual does is a challenging matter to understand. Therefore, in Essay 3, the moral disengagement theory provides specific levels of rationalization an individual may encounter when accountants intentionally violate ISPs—specifically capturing how accountants may excuse their responsibility to ISPs (Bandura 1999). Since I attempt to explain an accountant's internal rationalization process for violating ISPs, it is essential to also examine external environmental factors that may cause an accountant to rationally ignore their information security responsibility. The organizational justice theory helps provide a holistic representation of how the perception of fairness within an organization will drive the intentional ISP violation behavior to be less or more (Colquitt et al. 2003).

All three essays utilize the survey method to test the research model. The initial survey instrument was developed by first identifying and creating appropriate measures

based on a comprehensive literature review. Data was then collected by administrating the final survey instrument online.

The present chapter introduces the concepts of the fraud triangle and provides a brief review of management controls and organizational justice. Each essay will present a conceptual research model consisting of potential mediators and moderators in addition to the direct effects of the fraud triangle for intentional ISP violations. This dissertation is organized as follows: each chapter will present a brief review of the relevant literature, highlight the unique contributions of my work, a research model, development of hypotheses to be tested, followed by a summary of the research method, and a description of the data analysis and presentation of the results. Finally, each study will discuss the findings, implications, and future research directions.

CHAPTER 2

ESSAY 1: USING THE FRAUD TRIANGLE TO EXPLORE MOTIVATIONS FOR EMPLOYEES' COPYING COMPANY DATA

Introduction

Copying company data, such as personal sensitive employee details, e-mail, corporate documents, third-party sensitive data, company directories, and business calendars, to Portable Storage Devices (PSD, including USB drives, PDAs and smartphones) has become increasingly common in organizations. Consequently, organizations have raised concerns being raised on the potential of data leakage (Gorge 2005). To avoid this threat of unwanted data leakage, organizations often develop specific information security policies (ISP) to prohibit employees from copying company data and bringing company data home to avoid related information security problems (Tetmeyer and Saiedian 2010). For example, ISPs may prohibit portable media devices such as unsecured USB drives to be brought into the organization. (Conner and Coviello 2004; Gorge 2005; Lee et al. 2009). However, as employees become increasingly overwhelmed by their workload, it has become more challenging for them to finish their work during traditional working hours. Due to the pressure to complete their work,

employees are forced to copy company data in order to continue work at home. Thus, there exists an irreconcilable conflict between ISP compliance and timely work completion. Even when specific ISP policies have been created to address this violation, there are still employees who choose to violate these policies (Guo et al. 2011; Siponen and Vance 2010). This study explores the motivation for this unique intentional violation behavior (i.e., copying company data to bring home).

Previous research has examined several different theoretical lenses to explain the employees' ISP intentional violating behavior in the information system security literature. One such theory known as deterrence theory has been applied to investigate the effects of organizational deterrent measures on employee computer misuse (D'Arcy et al. 2009; Herath and Rao 2009; Hu et al. 2011). Another significant theory utilizes a code of ethics to clarify responsibility to deter unethical behavior (Harrington 1996; Myyry et al. 2009). Yet another, unified model of ISP compliance considers fear, moral beliefs, social factors, and deterrents to predict intention to comply with information security policies (Moody et al. 2018). Although these different theories have provided essential insights on the general intentional violating behavior, researchers have called on the antecedents exploration by focusing on specific violating behavior because it can provide more fine-grained insights and more actionable implications for the practices (Johnston et al. 2019; Moody et al. 2018; Vance et al. 2019). For example, copying company data behavior in this study further distinguishes the purpose of examining general intentional ISP violating behavior. If the employees copy data for a financial benefit (i.e. insider trading, leaking sensitive information), then this violating behavior is not only intentional but is also malicious (Harrington 1996; Posey et al. 2011a; Willison and Warkentin 2013; Willison

et al. 2018). In stark contrast to copying data for financial gain, when employees violate the ISP and copy company data for the purpose of working at home, the violating behavior may be intentional, but is not malicious (D'Arcy et al. 2014). When comparing these two types of data copying behavior, I find there are different motivations for their violating behavior. In this study, I focus on the motivation exploration for intentional but not malicious behavior consistent with copying company data in order to complete their work.

Interestingly, D'Arcy et al. (2014) considers ISP demands as one unique pressure to result in the employee's ISP violating behavior; unfortunately, there is a lack of knowledge in examining the effect of other types of pressure such as work pressure on the violating intention, which I argue is the essential reason for the data copying behavior.

In this study, I take the fraud triangle (Dorminey et al. 2012) from the accounting literature and apply this as a foundation of my theoretical model, which implies but does not formalize interrelationships between three fraud risk categories called opportunity, rationalization and pressure. The fraud triangle is a dominant framework in auditing and forensic accounting and it has become entrenched in the formal ethical standards of professional associations around the globe (Murphy and Free 2015). The three perceived elements of the fraud triangle are opportunity, rationalization, and pressure. Opportunity is defined as engaging in fraudulent activity arise when employees perceive a control weakness is present and that the ability to commit a fraudulent act without detection is high while the likelihood of being caught is remote (Dorminey et al. 2012). Rationalization occurs when individuals who commit fraud desire to do so without

incurring negative self-perceptions, so they will typically seek to rationalize their fraudulent actions to themselves (Dorminey et al. 2012). Pressure to commit fraudulent behavior can be categorized as personal, employment, and external pressure (Albrecht and Albrecht 1982). Prior research studies have found that when all three dimensions are detected the higher the likelihood of fraudulent behavior will be present in an organization (Dorminey et al. 2012; Dorminey et al. 2010; Ramamoorti 2008).

In this study, I extend the boundaries of the fraud triangle to provide one theoretical perspective to understand the motivations for specific data copying behavior. This theory emphasizes the motives, pressures, and needs of individuals at the most critical corner of the triangle; opportunity and rationalization sit at the other two corners (Wilks and Zimbelman 2004). The opportunity arises for computer fraud when there is an absence of controls, ineffective controls, or the ability to override controls. In the context of my study, no opportunity will be defined as no channel or interface for the employees to copy company data. For example, the computer in an organization may be programmed so that data can only be stored and accessed but not copied. Therefore, opportunity will be the first antecedent of the data intentional data copying behavior. Rationalization is an attitude to commit computer misuse. Rationalization happens when individuals make a conscious decision to use technology to present fraudulent or misrepresented information for a personal gain (i.e., asset misappropriations). In this study, employees' morality will use idealism as a proxy, and it will play a role in rationalizing ISP compliance. The level of morality of the employees will prevent them from violating the organization's ISP, as suggested in the existing literature (Bulgurcu et al. 2010; Chia and Lim 2000; Goles et al. 2006). Finally, general work pressure, as the

third dimension, may give employees an incentive to commit fraud. General work pressure will also be the crucial source of the conflict with ISP compliance. Therefore, I argue it will be the third antecedent of the data copying behavior and the most critical factor on whether employees will copy company data to bring home. With these three factors, opportunity, rationalization and work pressure, I propose a violating triangle model to explore the first goal of this study. I explore whether all the three elements of the fraud triangle exposed to an individual will be equally important (i.e., work pressure plays a more significant role than the other two points of the triangle in this context) to predict the intention of copying company data to complete their work at home.

Research studies shows that people will justify their behavior before conducting any action (Haines and Leonard 2007a; Haines and Leonard 2007b; Paradice and Dejoie 1991). Prior research points out that the main reason for non-compliance with security policies is that ISPs conflict with work productivity (Kirlappos et al. 2013; Zimmermann and Renaud 2019).

Therefore, I argue that work completion justification will influence the condition for an individual's justification for copying company data and bringing their work home. Specifically, when stronger work completion justification is formed, work pressure will increase employees' intention to violate specific ISP policies. In contrast, when more compelling work completion justification is formed, the goodness of employees (idealism) on ISP violating intention will be reduced. Employees who finish their work in their designated work hours reduce the mental stress that considering intentional ISP causes. The opportunity of violating is not influenced by the work completion justification to enhance the violating intention. Therefore, the second goal of this study is

to explore whether work completion justification will enhance the possibilities of employees' copying company data intention.

The remainder of the paper is organized as follows. First, I present an outline of the previous research on information security to present the theoretical model, the fraud triangle to examine employees' behavior of copying company data and to bring back home and then I present the hypotheses. Subsequently, followed by the description of the model discussion, data analysis using Partial Least Square (PLS) is discussed. In conclusion, I will discuss the findings, contributions, implications, and limitations as well as future directions for research.

Literature Review/Prior Research

Information system users in an organization have been considered as the weakest link for organization information security (Spears and Barki 2010; Wang et al. 2015; Warkentin and Willison 2009), especially with a wide variety of computer systems being integrated into the business processes operation. As the complexity of information systems grow, organizations risk having their systems compromised by both intentional and unintentional acts of organization employees. To address these issues (Kelloway et al. 2002) suggested that counterproductive behaviors (i.e. undesirable corporate conduct) and organizational citizenship (i.e. complying with ISPs) behaviors are empirically distinct. General management studies traditionally focus on general policies that govern employee citizenship behavior in the workplace. Information security (IS) literature, on the other hand, focuses on a specific set of policies—ISPs—that govern how employees behave to deal with counterproductive security issues. More specifically, prior IS research examine three main types of ISP violation acts caused by insiders. The first

being unintentional acts of ISP violations, which have been described as employees who perform their duties according to company policies and are not intentionally subverting controls to engage in violation behaviors (Loch et al. 1992; Taylor 2006). The second being classified as non-malicious intentional ISP security violations (Guo et al. 2011). These non-malicious yet intentional ISP violations are conceptualized as not self-benefitting actions and are done without malicious intent (Siponen and Vance 2010). The third category of ISP violation is considered computer abuse which is defined as the unauthorized and deliberate misuse of the local organizational information system by individuals including violations against hardware, programs, data, and computer services (Dhillon 1999; Straub Jr 1990). I present Table 2-1 to highlight the main differences between the three main classifications of ISP violations caused by internal users.

Table 2-1

Comparison of Unintentional, Intentional (Non-Malicious), Intentional (Malicious) Information Security Violations

Concepts	Key Differences	Examples	References
Unintentional security violations	Unintentional, not malicious, no financial gain, no self-benefits	Accidental data entry, accidental destruction of data	(Loch et al. 1992; Taylor 2006)
Intentional, non-malicious security violations	Intentional making conscious decision to violate, self- benefitting without malicious intent, voluntary rule breaking	Copy sensitive data to USB drives, Password sharing, Failure to logoff computer, delaying security patch updates	(Guo et al. 2011; Siponen and Vance 2010)
		Copying data to bring home to complete work	(Guo 2013; Siponen and Vance 2010)
Intentional, malicious computer abuse	Intentional, illegal, unethical, malicious, financial and personal self-benefits	Revealing confidential information to outsiders that may harm organization, writing viruses, software piracy	(D'Arcy et al. 2009; Straub Jr 1990; Willison and Warkentin 2013)

Scholars view ISPs as guidelines– normative lists of actions that the employees should (or should not) perform (Hevner et al. 2004; Siponen and Iivari 2006; Warman 1992). However, the design of ISPs faces the problem that such policies and guidelines do not necessarily make it possible to address all situations reasonably. For example, (Puhakainen and Ahonen 2006) observed that organizational ISPs strictly forbid taking any information away from the company premises without formal permission from the IS managers but, the employees of the company still took their laptops, USB sticks, and CDs to their homes and to meetings outside of the company. According to a 2019 survey, global information technology leaders found that one in three companies suffer from these specific security-related issues with remote workers (Rowe 2019). Unfortunately, no empirical study has exclusively examined this critical phenomenon to provide more specific insights and more actionable implications on the practice (Johnston et al. 2019; Moody et al. 2018; Vance et al. 2019).

Previous research has explored different theoretical lenses to explain the employees' ISP violating or compliance intention or behavior. First**,** deterrence theory is one of the most widely applied theories in behavioral IS security studies (D'Arcy et al. 2009). Based on the rational choice view of human behavior, the theory predicts that illicit behavior can be controlled by the threat of sanctions that are certain, severe, and swift (D'arcy and Herath 2011). However, by emphasizing the difference between malicious and non-malicious security violation (NMSV) behaviors, (Guo et al. 2011) proposed one NMSV model based on the theory of reasoned action (TRA) and the theory of planned behavior (TPB). They pointed out that deterrence theory may help explain why users comply with computer use or security rules but not why they break these rules

or engage in NMSVs. Their empirical result also shows no significant effect of sanction on the NMSV behavior. Second, beyond the lens of deterrence theory, (Siponen and Vance 2010) adopted a neutralization theory to provide a compelling explanation for IS security policy violations and offer new insight into how employees rationalize this behavior. This theory emphasizes that employees will rationalize their violations of security policies by using several neutralization techniques such as the defense of necessity. Also, when employees perceive stressful ISP requirements, this will result in the justification for employee's violation intention and behavior (D'Arcy et al. 2014). Third, an ethical perspective, which refers to the ethical content of informal norms and behavior, was frequently used to deal with those situations where no formal rules or policies are in place (Chatterjee et al. 2015).

The underlying logic for ethical perspective in security-related behavior is that the impact of the morality and ethical beliefs held by the individuals will influence their attitude to the computer-related violating behavior and further reduce the violating intention (Gattiker and Kelley 1999; Sojer et al. 2014). To some extent, morality and ethical beliefs held by the individuals could be one tool of neutralization technique to rationalize their compliance but not violating behavior. Fourth**,** criminal opportunity theory was recently adopted as another critical lens to consider opportunity as the explanation for employee behavior of unauthorized access attempts on information systems applications in a financial institution (Wang et al. 2019). For example, (Padayachee 2016) identified opportunity-reducing technologies as an effective mechanism to mitigate insider threats.

The literature review revealed that although prior studies have provided some valuable insights on the conceptualization of security-related violating behaviors. However, there are some limitations and gaps that warrant further investigations. In this study, I specifically examine the antecedents that have not been examined for intentional ISP violations (i.e. intentional copying company data). In the context of copying data to continue work at home, employees may not consider their violation behavior as unethical which poses doubts on the ethical perspectives on this violating behavior. Although the stress of employees as a motivational factor for the rationalization for violating behavior has been examined, discussion in the literature on the sources of stress is still limited to the ISP itself, including burdensome, complex, and ambiguous information security requirements.

Organizations continue to place mandatory compliance towards ISPs (Renaud 2011). However, this sometimes creates impossible standards that interfere with their ability to work effectively. For the behavior of copying data from the organization in order to continue work at home, to considering work stress in more depth is necessary because the extent of work stress that employees are under may not only directly result in employees' stress, but also ISP stress in this context. The perception of opportunity should also be integrated to explain the specific data copying behavior explored in this study because the organization controls the possibility for the employees to copy data. Previous research has proposed one general composite behavior model to understand the NMSV in the workplace (Guo et al. 2011). In addition, IS behavioral research can improve the practical relevance without loss of rigor by measuring specific examples of ISP violations, that is, data copying in this study (Siponen and Vance 2014).

Therefore, to adequately explain the data copying as one specific non-malicious but intentional violating behavior, it is necessary to integrate different theoretical lenses in the existing literature to propose one integrated but contextualized research model. As discussed, this integrated model should include three components: moral or ethical beliefs held by employees, work pressure as rationalization, and opportunity to copy data for use at home which implies the theoretical lens of the fraud triangle.

Fraud Triangle Model

The fraud triangle literature has slowly multiplied over the last decade, and its concepts have gradually been applied to a wide array of disciplines (Cressey 1954; Huber et al. 2015; Lou and Wang 2009; Morales et al. 2014; Schuchter and Levi 2016). Antifraud efforts have attracted the attention of professionals, including but not limited to internal and external auditors, members of the board of directors, management, and regulators. The Association of Certified Fraud Examiners' (ACFE) 2018 Report to the Nation estimates the cost of fraud to be over $7 billion in total fraud losses in annual revenues (Examiners 2018). To understand why individuals, commit fraud, many professionals refer to the fraud triangle. The significance of the fraud triangle in understanding motivation and its importance is most evident in Statement on Auditing Standards (SAS) 99, Consideration of Fraud in a Financial Statement Audit. The fraud triangle has enhanced professionals' ability to prevent, deter, detect, investigate, and remediate fraud (Dorminey et al. 2010).

First, the management or other employees have an incentive or are under pressure, which provides a reason to commit fraud. Second, circumstances exist—for example, the absence of controls and/or ineffective controls creating a perception of

opportunity. Perceived opportunity is the perception (1) that a control weakness is present, and importantly, (2) that the likelihood of being caught is remote. Therefore, perceived opportunity requires the ability to commit the act, and to do so without detection (Hollinger and Clark 1983). Third, those involved can rationalize committing a fraudulent act. Some individuals possess an attitude, character, or set of ethical values that allow them to knowingly and intentionally commit a dishonest act. However, even "honest" individuals can commit fraud in an environment that imposes sufficient pressure on them. Rationalization is an attempt to reduce the cognitive dissonance within the individual (Ramamoorti 2008; Ramamoorti et al. 2009). The higher the incentive or pressure, the more likely an individual will be able to rationalize the acceptability of committing fraud. (AICPA, 2002). Likewise, the greater the perceived opportunity or the more intense the pressure, the less rationalization it takes to motivate someone to commit fraud (Albrecht et al. 1984).

A representation of the "fraud triangle" theory is illustrated in Figure 2-1. This model highlights the separation of the individual who perpetrates the crime from the criminal act. As organizations continue to become technologically advanced, employees continually rely on computers for their daily tasks. Thus, some research has shown that individuals may engage use computers to engage in occupational fraud (Guragai et al. 2015). Since systems legitimize individual wrongdoing by allowing people to focus on their duties within the system, the disassociation will enable employees to not overlook the moral impact of their actions (Adams 1998).

The three points of the fraud triangle capture the necessary antecedents to provide a finer grained insight on the intentional but not malicious ISP violation such as copying data from the organization to bring home in order to complete their work.

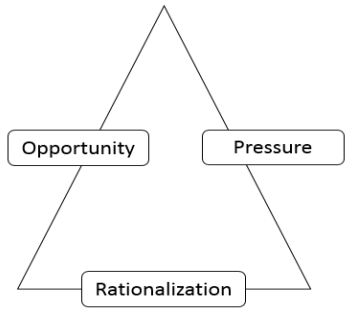


Figure 2-1: Three Points of the Fraud Triangle

Opportunity

When the term opportunity was initially introduced as a term into the entrepreneurship literature, it was defined as an "alertness to changed conditions or to overlooked possibilities" (Kirzner 1979). In this study, opportunities arise for violating ISP's when there is an absence of controls, ineffective controls, or the ability to override controls. These opportunities can be noticed even by persons who are not actively seeking them. For instance, previous research has investigated individuals practicing "safe computing practices" such as changing passwords and updating security software (Boss et al. 2015; Workman et al. 2008). Opportunities are courses of action that seek to derive benefits from these changes (Baron 2006). Individuals may recognize these opportunities as an effort to form beliefs regarding whether or not enacting a course of action could lead to benefits such as the convenience of continuing work from home in order to meet work deadlines (Shepherd et al. 2007).

Idealism/Rationalization

In the investigative context of this study, rationalization is built from one of Forsyth's distinct ethical belief, idealism (Forsyth 1980). Forsyth theorizes that individual moral beliefs and attitudes are part of an integrated conceptual system of personal ethics. Forsyth's (1980) model suggests that moral judgment will vary according to their position on idealism and relativism. This study focuses only on idealism as individuals making ethical judgments in business-related issues had a higher sense of idealistic ideology (Barnett et al. 1994).

Individuals high in idealism seek to always avoid harm by assuming proper action, good consequences can be obtained (Davis et al. 2001). In the context of intentional ISP violations, an employee's level of idealism will encourage them to follow ISPs since ISPs are considered to be the organization's security code of conduct (Forsyth 1980). Technological idealism is an individual's belief that technology should not be used to harm anyone (Chatterjee et al. 2015). Technological idealism is based on the notion that any technology-related action should maximize the (good) consequences.

Typically, using IT unethically increases the likelihood of causing harm to others. For example, intentionally violating ISP behaviors such as voluntarily disregarding company ISP to copy sensitive work data to bring home to meet work deadlines could lead to data breaches (handling sensitive data insecurely). Applied to ISP, idealism in information technology can be conceptualized as an ISP which describes an ideal or a moral code of conduct for the organization's employees to follow. Thus, if actions conflict with ISPs, it is deemed to be wrong or punishable. Hence, it can be assumed that

individuals who have a high level of technological idealism would tend to have a negative attitude toward intentional ISP violations.

Work Pressure

The pressure part of the fraud triangle is construed as work-related stress (Cavanaugh et al. 2000). The US audit standard describes it as "employees have an incentive or are under pressure, which provides a reason to commit fraud" (PCAOB, 2015, AU 316.07). (Albrecht et al. 2008) give examples of pressures such as needing to report results better than actual performance, experiencing frustration with work, and finding a need to circumvent internal controls for the organization's systems. Employees who face unreasonable work deadlines or are given a large number of responsibilities with unmanageable expectations are considered under work-related stress.

New global business models and the digital age have shifted expectations of employees. There is a sizeable body of research demonstrating a relationship between performance goals and employee performance (Deci 1972; Guzzo 1979; Latham et al. 1978; Locke et al. 1981). When the performance goals or objectives become too challenging, this can become a source of work pressure. Although there are many sources of pressure on employees, I specifically focus on the relationship of work pressure towards job performance. Work pressure has been defined as the extent to which the "job performance required in a job is excessive or overload due to performance required on a job" (Iverson and Maguire 2000). Work pressure has been found as a critical determinant of worker stress and health, especially in offices with computer work (Carayon 1995; Carayon et al. 2003). In this study, work pressure is defined as the perception of high job demands that never seem to diminish, which include tight deadlines that people have a

hard time keeping up with. Work pressure is found in many work environments nowadays (Andries et al. 1996; Carayon and Zijlstra 1999). Understanding the role of perceptions of work pressure is essential especially in understanding why intentional but non-malicious ISP violations occur.

Work Completion Justification

Employees may view security as an obstacle to finishing their day-to-day work tasks (Dourish et al. 2004). For example, employees dislike booting their computer in order to deal with security configurations. The persistence of virus checkers, intrusion detectors, and other similar systems all interrupt current work flow to insist on timely security updates can be problematic to employees (Dourish et al. 2004; Guo et al. 2011). Complying with ISPs are normally not a part of employee's job performance evaluation (Besnard and Arief 2004).

Thus, in this study, I assume this as an indication that job performance is more important to employees than complying with ISPs (i.e. finishing their allocated work on time). As employees are more concerned with their job performance, ISPs will more likely be ignored. Employees may also intentionally choose to bypass security measure if doing so can help them complete their work and improve job evaluations (Guo et al. 2011; Post and Kagan 2007). Therefore, in my study work completion justification is defined to the extent to which employees will justify their actions to help them complete their job (i.e. copying sensitive company data to bring home to complete their work). Table 2-2 to summarize the constructs used in this study.

Table 2-2

Constructs Used in the Study

Construct Name	**Definition (source)**
Independent Variables	
Opportunity	The extent to which circumstances exist when there is an absence of controls, ineffective controls, or ability to override control (PCAOB 2015 AU 316.07).
Rationalization/Idealism	Individuals believes that any technology-related action should maximize the good without harming another (Forsyth 1980; Chatterjee et. al 2015).
General Work-Related Pressure	The extent to which a job involves employees perceiving general work related stress (Cavanaugh et al. 2000).
Work Completion Justification	Reconstructing harmful ISP violations (i.e. copying sensitive company data to a USB to bring home) as getting the job done more efficiently and meeting deadlines whether it is for personal accomplishments or because they feel like they are doing a service for their organization (Guo et al. 2011; Siponen and Vance 2010)
Dependent Variable	
Intentional ISP non-malicious Violation	To the extent to which an employee will engage in voluntary intentional ISP volitional behavior without malicious intents and no financial gains (i.e. copying data on insecure USB drive to bring home in order to complete their work) (Guo et al. 2011)

Hypotheses Development

There is a growing body of academic security literature with an emphasis on behavioral security issues (Siponen and Vance 2010; Spears and Barki 2010; Warkentin and Willison 2009; Willison and Warkentin 2013). By merging the issues being examined in the IS security policy literature to the specific phenomenon of employees voluntarily violating ISP policies in order to complete their work duties, I link numerous factors including the opportunity provided to employees to copy data to bring home,

work pressure, a sense of idealism towards technology, and the sense of work completion to reveal a deeper understanding of non-malicious but intentional violations of ISPs.

The first component of the fraud triangle is the perception of opportunity. The US audit standard defines opportunity as when "circumstances exist, for example, the absence of controls, ineffective controls, or the ability of management to override controls – that provide an opportunity for fraud to be perpetrated" (PCAOB, 2015, AU 316.07). Opportunities for the commission of these violations of internal controls are likely to manifest themselves when employees sense that they might be able to safely use their credentials to circumvent internal Information Technology (IT) security controls. Opportunities to violate ISP's result from circumstances that provide chances to commit these violations of trust. Employees are often charged with specific workloads and finishing their job involves a high degree of employee judgment and subjectivity to time management. Because one can perceive opportunities within an organization to copy data to bring home to work without repercussions, the following hypothesis has been drawn out:

H1: *Opportunity is positively associated with the likelihood to commit intentional but non-malicious ISP violations.*

The second component of the fraud triangle is rationalization. Rationalization is defined as an attitude or character that leads one or more individuals to commit an intentional but non-malicious ISP violation rationally (Goles et al. 2006). Rationalization happens when individuals who commit violations against the organization desire to do so without incurring negative self-perceptions, so they will typically seek to rationalize their actions to themselves (Dorminey et al. 2012). In the context of this study, employees may

engage in actions (i.e., violating security policies) which may be seen as legitimate means to their desired ends (i.e., job performance). In 1989, Sharp, an early psychologist interested in moral judgment, examined individual variations in approaches to moral judgment. The focus of this study is on the second major dimension of moral judgment focuses on idealism in one's moral attitudes (Forsyth 1980). Because one can rationalize or attempt to self-justify their actions to commit intentional but non-malicious ISP violations, the following hypothesis has been drawn out:

H2: *Rationalization is negatively associated with the likelihood to commit intentional but non-malicious ISP violations.*

The third component of the fraud triangle is perceived pressure. The subject of unwanted pressure has extensively been examined in organizational and psychology literature (Hay and Gray 1974; Rodell and Judge 2009). I offer a different avenue for understanding employee's intent to commit intentional but non-malicious ISP violations – namely, work-related pressure. Work-related pressure is felt when the pressure is being applied by employees to minimize their work effort. This type of work pressure introduces security risks as the relentless pressure to perform work may result in employees taking risks to respond to this pressure (Allam et al. 2014). Employees may perceive little to no control over the perceived pressure for the security requirements imposed upon them by the organization (D'Arcy et al. 2014). For instance, the time-consuming security requirements may hinder an employee's job and further increase the pressure for employees to circumvent information system controls. Many industries require periodic security training sessions that expose employees to new security requirements (PricewaterhouseCoopers 2018). These new requirements may cause more

risks as employees need to continually adjust to new requirements with little time to develop a normalized work routine. Work-related pressure can be threatening for employees and raise perceptions of pressure. Therefore, the following hypothesis has been drawn out:

H3: *Perceived general work-related pressure is positively associated with the likelihood to commit intentional but non-malicious ISP violations.*

Although there are many sources of pressure on employees that serve as motivations for intentional but non-malicious ISP violations, I focus on the relationship of work completeness as justification for the intentional but non-malicious ISP violation. Previous research has demonstrated that employees are feeling more stressed at work (Taylor et al. 1997). A recent study from Staples Business Advantage (White 2016) found that over 75% of employees work more than 40 hours a week. However, instead of spending it to get ahead on work, employees are using their extra hours to stay afloat to meet organization deadlines. For employees that use IS in an organization setting, making decisions to complete their work remotely may involve copying sensitive organizational data to a mobile data storage device to bring home to finish their assigned tasks.

Performance goals or objectives can be a source of work pressure. Managers may impose objectives for employees without regard to the complexities of the job or without making adjustments for the skill and responsibilities of the employee. Employees may feel overwhelmed as they pursue to so satisfy all these performance objectives (Marsden and French 1998). Although the purpose of performance objectives is to set specific and challenging goals for employees when goals become excessive, employees begin to use this need to complete their work as justification to meet their performance goals by

whatever means (e.g. intentionally violating ISP's) (Locke et al. 1981). When work performance is the goal that users try to accomplish, security often becomes a trivial task.

Receiving high work performance evaluations can be seen as a positive outcome that employees attempt to achieve (Dobre 2013; Longenecker et al. 1987). Therefore, the significant influence of work performance confirms that work completion will be an essential decision factor when employees deal with specific security issues. For example, if an action can help employees carry out their assigned tasks, improve productivity, and complete their work, employees will likely engage in the action even if the action violates organizational ISPs. Thus, violating ISPs would not become a problem for employees if these violations help complete their work. Therefore, the following hypotheses have been drawn out:

H4a: *Work completeness justification will positively moderate the effectiveness of perceived opportunity to intentionally commit a non-malicious ISP violation.*

H4b*: Work completeness justification will negatively moderate the effectiveness of perceived level of idealism to intentionally commit a non-malicious ISP violation.*

H4c*: Work completeness justification will positively moderate the effectiveness of perceived level of idealism to intentionally commit a non-malicious ISP violation.*

The resulting research model is illustrated in Figure 2-2.

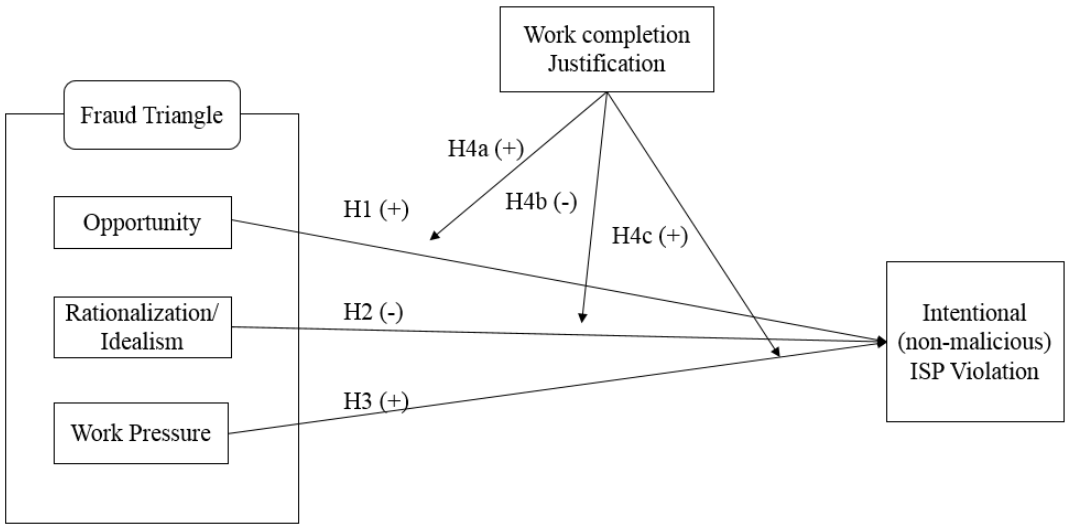


Figure 2-2: Research Model

Methodology

Measures

I utilized an online survey instrument for data collection. The measurement items in my questionnaire were adapted from existing validated and well-tested scales in the extant literature. In addition to using previously validated questions, all measures were pretested by two business professors with expertise in survey research and ten professionals with ISP experience. The objective of the pretest was to ensure that the measures were meaningful and that they unambiguously captured the domain of each construct. Based on detailed interviews with each participant, appropriate changes were made to the measures.

All measures were pilot tested in a survey with a small portion of targeted samples, which only resulted in minor wording changes. I conducted a reliability analysis and exploratory factor analysis for each set of measures. The validity and reliability of

the adapted measures fulfilled the necessary requirements, which indicated all measures were clear to the targeted samples, relevant and captured the intended concepts. The results placed sufficient confidence in the measures to proceed with the survey administration of the target sample frame. In the questionnaire, all items were measured with 5-point Likert scales, ranging from “strongly disagree” to “strongly agree.”

Sample

I used a market research firm to invite participants to take my survey. External panelists have been used increasingly in IS research (Ayyagari et al. 2011; Bulgurcu et al. 2010) and have certain advantages over traditional methods that were key to my study. First, panels guarantee respondent anonymity and thereby encourage honest responses to questions that may be subject socially desirable responses. Second, external panels contain respondents from a wide range of industries and positions. The marketing research firm was instructed to collect responses from employed computer-using professionals. The research firm paid participants a small amount for their participation. Respondents were paid $10 each for participating in the study. In the questionnaire, the targeted samples were first asked to indicate their computer experience in the company. If a targeted sample had not used a computer in the company, that person was excluded from further consideration. The questionnaire then asked the respondents to measure the subjects’ perceptions of opportunity, idealism and work-related pressure in terms of following information security policies, and the intentional ISP violation.

A total of 574-panel members accepted the invitation to participate in the survey by viewing the consent agreement and clicking past the first page. After excluding incomplete responses, I used a data set of 209 responses in all analyses. Table 2-3 shows

sample demographics for these respondents. All employees sampled must use a computer to complete their daily work tasks. Sample demographics reveal that 62 percent were female and tended to be well-educated (71 percent with at least a bachelor's degree).

Table 2-3

Sample Distribution by Classification

Gender	Count	Education	Count
Female	129	High-school	29
Male	80	2 year degree	31
		4 year degree	93
		Professional Degree	53
		Doctorate	3
Total	**209**	Total	**209**

Control Variables

To account for rival explanations of the intentional ISP violation, I implemented several control variables in this study. I recognize that the behavioral intention to commit intentional but non-malicious ISP violations might also be influenced by respondents' characteristics, such as age, gender, education, accounting responsibilities, and perception of monitoring within an organization. The examination of the control variables and their influence on the intention to voluntarily commit intentional non-malicious ISP violations revealed that none of these significantly influenced how employees may formulate their intentions to do so.

Data Analysis and Results

The research model was tested using PLS. PLS is a component-based structural equation modeling technique, which facilitates simultaneous tests of measurement models and structural models and is particularly suitable for testing nonlinear effect such as moderation (Chin 1998; Chin et al. 2003). PLS is well suited for the predictive nature of this study, and properly assessed the relative influence of the fraud triangle to the likelihood of an intentional ISP violation. Further, the use of PLS is appropriate mainly because of the early theoretical development nature of the study (Gefen et al. 2011). PLS was employed to both validate the measurement instrument and test the research model.

PLS supports simultaneous analyses of multiple indicator variables and enables empirical testing of extensive interactions among the moderator and latent predictors. This model was evaluated using PLS to illustrate how multiple interaction effects work together. I assessed measurement validity in three ways. First, convergent validity was assessed by how each item was related to its corresponding construct by examining the factor loadings. Convergent validity is considered satisfactory if the factor loading of a measure is 0.7 or higher. All factor loadings were above the cutoff point of 0.70 with a t-value higher than 1.96. The measures loaded on their appropriate factors and there was no evidence of significant cross-loading. Average variance extracted (AVE) was also examined to evaluate convergent validity. AVE is greater than 0.5, establishing convergent validity. As a result, each construct had an AVE greater than 0.5, suggesting that the measures exhibited adequate convergent validity.

Second, the reliability of the measures was examined through two criteria, Cronbach's alpha (CA) and composite reliability (CR). The CA and CR of construct was

greater than 0.7, a common threshold for signifying satisfactory construct reliability. According to the results, the minimum CA and CR values exceed the recommended threshold of 0.7, indicating acceptable reliability of the measures. These tables are presented in the Appendices.

Third, discriminant validity is verified by the difference between the AVE of a construct and its correlation with other constructs. For adequate discriminant validity, the square roots of AVE of any construct should be greater than the correlations between the construct and other construct, which means that the diagonal elements should be greater than corresponding off-diagonal ones. (Fornell and Larcker 1981). As a result, the criterion for sufficient discriminant validity was also met in this study. I tested for common method variance (CMV) through Harman's single-factor test by conducting an exploratory factor analysis to determine whether all measures loaded on a single factor (Podsakoff et al. 2003). The measures in the data set loaded on separate factors, so common method bias did not appear to be a serious problem.

The proposed hypotheses were tested through the examination of the structural model as presented in Figure 2-3. For increased robustness and statistical validity, a bootstrap resampling procedure was used with 1,000 resamples. The standardized PLS path coefficients for testing the structural model are shown in Figure 2-3. The model accounts for a significant portion of the variance in intentional ISP violation ($R^2 = 40$ percent). Overall, PLS analyses generally confirm that the fraud triangle (i.e., opportunity, rationalization and work pressure) significantly influences intentional ISP violation. More specifically, opportunity (path coefficient = 0.13, $p < 0.05$) and work pressure (path coefficient = 0.19, $p < 0.05$) had significant, positive effects on intentional

ISP violation, in support of H1 and H3. However, idealism had an insignificant effect on intentional ISP violation (path coefficient = -0.06, $p > 0.05$). Therefore, H2 was not supported.

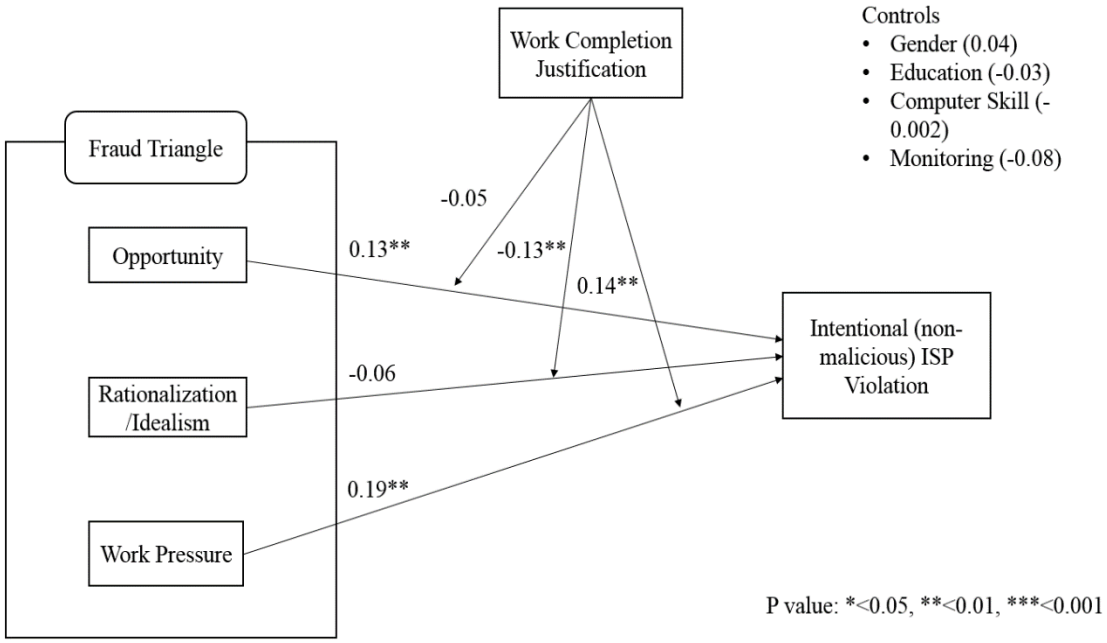


Figure 2-3: Predictive Model Results

I followed the steps proposed by Aiken and West (Aiken and West 1991) to examine the moderation hypotheses. The interaction terms were mean-centered prior to creating the interaction variables in order to reduce the potential for collinearity (Chin et al. 2003). Work completion justification positively moderated the positive effect of work pressure on intentional ISP (path coefficient = 0.14, $p < 0.05$). However, it did not moderate the positive effect of opportunity on intentional ISP violation (path coefficient = -0.05, n.s.). Therefore, H4c was supported while H4a was not.

Interestingly, work completion justification negatively moderated the effect of idealism on intentional ISP. Therefore, H4b was supported.

Discussion and Theoretical Implications

This study is motivated by a desire to understand different possible motivations for non-malicious but intentional ISP violations. I examine how the elements of the fraud triangle will affect an individual's intention to copy company data to bring home with the influence of an individual's desire to complete their assigned workload. After carefully considering the investigative goal of the study, I determined that opportunity and work pressure have a significant positive relationship with intentional ISP violation intentions. However, an individual's level of idealism did not show a significant effect on company data copying intention. At the edges, idealism has a strong significant relationship with attitude (Chatterjee et al. 2015). Thus, idealism is related to attitude only when the idealism perceptions are either very strong or very weak. For these reasons, it explains why idealism did not have a strong relationship with an employee's intention to commit ISP violations.

The results revealed that work justification positively influences the impact of work pressure on ISP violation intention but negatively moderates the effect of the idealism. Work justification had no significant moderating effect on the effectiveness of the perception for ISP violating opportunity. These findings provide new insight into the understanding of the employees' data copying behavior and implications for future studies.

First, the fraud triangle theory appears to be a useful framework for identifying why certain ISP's and regulations will be violated by incorporating work pressure, as an essential antecedent to violating with ISP for copying data and bringing it home to work. (D'Arcy et al. 2014) identified that ISP demands are a form of particular stress that causes

employees to react negatively and commit ISP violations. I provide a more fine-grained view of the specific type of ISP violating behavior (i.e., copying company data to bring home) with the work pressure. I extend the understanding of the role of potential pressures on ISP violating behaviors.

Furthermore, previous research has revealed that copying data can be a severe concern for organizations when malicious employees take sensitive information and create information leaks that can lead to costly financial losses (Abu-Musa 2006; Renaud 2011). On the other hand, while employees continue to experience the opportunity to violate ISP policies, this study shows that their most significant driving motivation is the overwhelming work pressure they face to complete their job. In short, these results suggest that work pressure (or different types of pressure) may play a critical reason for the non-malicious but intentional ISP violations.

Second, information security research has focused on enhancing an employee's ethical stance towards ISP violation intention. (Leiwo and Heikkuri 1998; Ruighaver et al. 2010) stated the use of ethics in information security has two purposes: to identify the criteria between "good" and bad and thus to promote good desires. Prior studies have suggested establishing guidelines for an individual's accountability towards moral intensity (Chia and Lim 2000; Robin et al. 1996), enforcing a code of ethics (Harrington 1996), and implementing ethical decision-making aids (Bulgurcu et al. 2010; Goles et al. 2006). The fraud triangle, which is the focal theory of this study, suggests that an individual's rationalization/idealism stance would reduce the possibility of committing violation behaviors (Schuchter and Levi 2016; Sorunke 2016). In my study, I capture an employee's good desires with their level of idealism. I also focus on the non-ethical issue

of copying data to complete their work, as opposed to personal gain, which belongs in the domain of non-malicious but intentional violations. Without a better understanding of the non-malicious intentions of employees, strengthening the user attitudes towards ISP compliance seems unlikely.

Lastly, increasing the knowledge of the work completion justification for an employee is also relevant because of the consistently significant link between work performance and work stress (Abramis 1994; Fisher 2001; Jamal 1984; Motowidlo et al. 1986). The issue of work completion justification enforces an individual's concept of self-identity (Lee et al. 2006). In the context of an organization, an individual's self-identity is generally their sense of purpose or responsibilities. Finishing their assigned work becomes a stable self-concept and can encourage individuals to engage in behaviors that will be consistent with this bottom line. In order to complete their assigned workload and continue their "purpose" at the organization, employees will use identity enhancing events that only improves their psychological well-being even if it means violating ISPs to achieve these goals. On the contrary, employees tend to avoid behaviors that are inconsistent with their organizational self-identity. Being unable to complete their work may be seen as identity-threatening events that may lead to decreased psychological well-being. In other words, when employees feel that ISPs do not help carry out business tasks and improve productivity, employees will likely engage in behaviors even if these behaviors violate organizational ISPs (Guo 2013; Guo et al. 2011). Utilized in an organizational context, an employee could argue that he/she must violate ISPs in order to get his/her work done (Siponen and Iivari 2006).

Therefore, a significant influence of work completion justification can be interpreted as a positive outcome that employees try to achieve. The significant influence of work completion is an important decision factor when employees are concerned with security policies that may hinder their workload. Rather than merely accepting the need to have additional security policies to prevent catastrophic organizational ISP violations, I explore the idea that ISPs may need to be reconsidered to reduce this conflict.

Implications for Practice

With the growth of computer technology, employees may feel that the higher demands of their work, such as, pressing deadlines, create an environment that encourages employees to copy data to take out of the office in order to complete their work assigned to them. The results suggest that a shift in IS security management may be necessary and also suggest a need to reevaluate the importance of certain ISPs within an organization. IS management should address the important issue of what they can do to help employees with their job in order to create a security-friendly culture.

Employees are practical, and they care about completing their workload more than IS security. When implementing a security policy, IS management should first understand what this policy means for employees and how it will affect their daily work tasks. IS management can also explore avenues that will restrict bringing work home in order to eliminate this specific ISP violation further. For example, high-tech companies may start directly using the local area network in the workplace and leave no interface for copying company data to portable media. IS management needs to align the security objectives with employee objectives.

This study has indicated an association between the evaluation of employee work performance as a significant influence on an employee's compliance with ISPs. Previous studies have suggested that organizations should utilize periodic security education, training, and awareness programs in order to reduce the uncertainty towards ISPs. However, in intentional yet non-malicious ISP violations, organizations, may fare by better putting resources towards a critical examination of what is considered necessary ISP compliance and how certain ISP violations can affect the business performance of the organization. IS managers should examine how employees' workload collide with the rapid speed ISPs are being implemented rather than focusing on implementing more security measures.

Limitations and Additional Future Research

As with many other behavioral security research projects, this project is limited by the use of intention instead of actual behavior as the dependent variable. How intention translates to actual conduct is not completely clear, but the limited focus on intention is consistent with the majority of information security studies (Paternoster 2010).

A second limitation of this study is the consequence of using a scenario-based research design. As (Siponen and Vance 2010; Willison et al. 2018) explained, the participants in a study involving scenarios of policy violations may have already been involved in similar experiences and may feel compelled to conceal their true intentions because they perceived this behavior as socially undesirable. Previous research (Siponen and Vance 2010; Willison et al. 2018) suggested that the expected number of previous violators in their sample pool was likely to be insufficient to skew the results of the study.

Because of the sample size used in the present study, it is reasonable for this study to infer the same expectation.

Third, the model focuses on a specific type of non-malicious but intentional ISP violation intention as the ultimate dependent variable, thereby limiting the scope of the study. Future research should investigate different types of non-malicious ISP violations (i.e. password sharing, avoiding timely security patches). Additional research can consider incorporating both individual factors and institutional factors (i.e., tone at the top, organizational climate) to explain the motivation to violate ISPs intentionally. Further research may be able to explain the layers of rationalization employees encounter when shaping their intention to violate ISPs.

Conclusion

In this study, I utilized the fraud triangle theory to determine whether employees develop a strong sense of work pressure that drives their intention to deliberately violate ISP policies to complete their work on a timely basis. The results of this study are important for three reasons. First, I expand the theoretical boundaries of the fraud triangle into the IS domain. Second, I provide an essential contribution to the current IS discussion to find a different motivation for the specific intentional but non-malicious ISP violating behavior (i.e., copying company data to complete work). Lastly, this study examines the significant influence of work completion as an essential decision factor when employees are considering ISP violations. The results of this study also suggest how future research can build on the current findings to develop effective strategies to aid in creating and implementing ISPs.

CHAPTER 3

ESSAY 2: UNEXPECTED EFFECT OF INFORMATION SECURITY POLICIES ON ACCOUNTING EMPLOYEES' INFORMATION SECURITY VIOLATION BEHAVIOR

Introduction

In today's business, information security management is a critical issue. There are often strict organizational controls known as information security policies (ISP) to avoid these potential information security problems. However, not only have stringent security controls failed to achieve the expected effect, but they have resulted in even more intentional ISP violations (Alge 2001; George 1996; Hsu et al. 2015; Lowry and Moody 2015; Posey et al. 2011a; Sewell and Barker 2006). Studies have shown that a class of employee security-related behaviors known as intentional ISP violations (D'Arcy et al. 2014), such as password sharing, sharing insider information, and unauthorized USB-usage, continue to plague organizations. For example, a recent Pricewaterhouse Coopers survey shows that current employees account for the highest amount of security incidents at 30% (PricewaterhouseCoopers 2018). Accounting employees are essential organizational insiders, who have an inherently higher risk of exposing organizations to information security threats. This risk is, in large part, due to their management and oversight of critical financial data used to predict the organization operating condition

and financial health of the company. Ineffectively managing accountants may result in countless problems for the company, not the least of which are reputational problems, loss of stock value, material financial reporting errors, and financial losses (Amiram et al. 2018; Fritz et al. 2014; Skaife et al. 2013). Given the accounting employee's importance to an organization, there has still yet to be a specific study to examine an accountant's ISP violation behavior. Therefore, this study aims to examine the effects of the organizational controls on the ISP-violating behavior of accountants.

In current information security literature, different organizational controls on information security compliance of general employees have been thoroughly examined, but have produced mixed results (Lowry and Moody 2015). Controls have been identified as either formal controls or informal controls (Eisenhardt 1985). Formal controls are properly documented and presented by specifications, evaluations, and rewards/punishments (Eisenhardt 1985; Hsu et al. 2015; Kirsch 1996). Informal controls are unwritten and often enforced by employees (Eisenhardt 1985; Hsu et al. 2015). Between the two types of controls, formal and informal, formal controls are considered more effective (Heales et al. 2007; Hsu et al. 2015). Most information security studies examine the line of formal control perspective have adopted deterrence theories and observed how the presence of sanctions drive employees to comply with expectations (D'arcy and Herath 2011; D'Arcy et al. 2009; Herath and Rao 2009; Hu et al. 2011; Willison et al. 2018). In order to be consistent with prior research, I consider ISP controls as formal controls. In this study, ISPs are considered to be a set of formalized procedures and guidelines which instruct employees their responsibilities to protect and use the information and technology resources of their organizations (Bulgurcu et al. 2010;

D'Arcy et al. 2009) properly. For example, control theory incorporates the concept of mandatoriness to argue that when individuals perceive ISPs as mandatory; they will more likely take security precautions (Boss et al. 2009). A common area of focus among these studies are on the effects of formal sanctions, which are explicit penalties for certain forms of misconduct (Siponen et al. 2012), and how they encourage desired behaviors and discourage undesired behaviors.

Interestingly, based on reactance theory, Lowry and Moody (2015) found that even with high levels of ISP controls, it could result in unintended consequences and increase undesirable employee behaviors in organizations. The reason appears to be that most employees have a tacit limit for the degree of tolerance they will feel towards management policies that are controlling and a similar threshold for how much individual freedom they will give up before negative consequences for the organization will occur (Lowry and Moody 2015). Other research has also provided evidence that ISP controls could result in a negative effect on the general employee's security compliance (Ariss 2002; Dhillon 2001; Posey et al. 2011a; Stanton et al. 2005). Therefore, as the levels of ISP control continue to increase, it is plausible that there may be an unintended negative consequence on intentional ISP violating behavior. The objective of this study is to examine how might ISP controls affect the accountant's intentional ISP violation behavior.

The fraud triangle has long been considered as a noteworthy theoretical lens to explain the effect of management controls as anti-fraud behaviors (Cressey 1953; Dorminey et al. 2010; Murphy and Free 2015; Murphy and Free 2016). The dimensions of the fraud triangle could be used as a meta-model to improve the anti-fraud efforts to

prevent, deter, detect, investigate, and remediate fraud (Dorminey et al. 2012). For example, Murphy and Free (2016) suggested organizational climate as one type of organizational control that could effectively reduce fraud behavior via three dimensions of the fraud triangle. On the other hand, while the fraud triangle theory has been mainly used to explain the malicious fraud behavior or criminal behavior, others such as (Murphy and Free 2016) have pointed out that the fraud triangle has been called into question for its narrow interpretation (Morales et al. 2014) and lack of comprehensiveness (Murphy and Free 2015).

Cressey 1953 conceptualized the fraud as a violation of trust such that the fraud triangle could be generally used to understand offenders when committing negative trust-violating judgments. As such, I argue that the fraud triangle could be able to explain the non-malicious yet still intentional violating behavior of accountants. Specifically, I consider the effect of ISP controls on intentional ISP violation behavior along with the three elements (opportunity, rationalization/attitude, and pressure) of the fraud triangle in the context of accountants and their daily work responsibilities.

Opportunity refers to the perceived possibility of successfully committing the wrongdoing without being reported to the organization (Dorminey et al. 2012). Therefore, the opportunity arises when there is an absence of controls, ineffective controls, or the ability to override controls. In the accounting ISP violation context, the opportunity is generally conceptualized as the cost for accountants to gain unauthorized access to the organizational information system or other employees' computers. Given collaboration among accountants has been an indispensable part of an accountant's daily work, high levels of ISP violating opportunity exist for accountants. For example,

accountants often work in a collaborative environment (El-Sayed and Westrup 2011). However, this may result in inexperienced, unmotivated, uncooperative, poor adaptation to technological advances in the industry, knowledge sharing risks, and regulation risks (Bhimani and Willcocks 2014; Coras and Tantau 2013; Low et al. 2008). In the context of ISP violation behavior, team members may intentionally share passwords or failure to secure workstations in order to ensure their accounting team continues to perform work duties as quickly as possible.

Second, rationalization or a change in attitude to commit computer fraud happens when individuals make a conscious decision to use technology to present fraudulent or misrepresented information for a personal gain (e.g. asset misappropriations) (Bell and Carcello 2000). In this study, employees' morality, using idealism as a proxy, will play its role in rationalizing their ISP compliance. Idealism is one of the two distinct ethical beliefs formed from Forsyth's ethical model. The original model theorizes that individual moral beliefs and attitudes are integrated with their personal level of ethics (Forsyth 1980). Forsyth's (1980) model suggests that moral judgment will vary according to an individual's level of idealism and relativism. In this study, I focus only on idealism because individuals making ethical judgments in business-related issues have had a higher sense of idealistic ideology (Barnett et al. 1994). In the context of ISP violation intentions, I argue when accounting employees hold themselves to a higher standard of ethics, this will prevent them from violating the organization's ISP regardless of the circumstances.

Finally, pressure as the third dimension of the fraud triangle could facilitate employees with an incentive to commit fraud, which provides the most influential

motivation for fraud. Accounting professionals are known to have high-pressure jobs and are subjected to stress from many sources including elements such as work-life balance, dealing with demanding clients, inflexible deadlines, and meeting requirements expected of them in an organization such as staying up to date with the technological skills and accounting standards (Collins and Killough 1992; Viator 2001). In the context of accounting employees' ISP violating intention, ISP controls can create stress in accounting employees (known with high-pressure). Therefore, this form of employee stress termed ISP pressure may theoretically be a contributor to ISP violations. Higher ISP controls, thus, may increase the intentional ISP violating behaviors by increasing ISP pressure.

In short, I examine the effects of ISP controls on the triad of factors brought by the fraud triangle on intentional ISP violations caused by accounting employees. Therefore, the first goal of this study is to determine how organizational ISP controls will influence accounting employees' ISP violating behavior via the fraud triangle elements.

I further explore the influence of organizational ISP controls on accounting employee's ISP pressure. The accounting profession is often known as a high-pressure profession. Therefore, accountants may adopt demands more quickly than other employees. However, whether the implementation of additional ISP controls will result in accountants' ISP pressure may depend on the extent they think they can effectively respond to the ISP requirements. ISP self-efficacy thus captures the capacity of how accountants can complete their job using technology while simultaneously complying with ISP requirements. This self-efficacy could be an essential personal characteristic to consider as a side effect of ISP controls on ISP pressure.

Due to the rise in cybersecurity incidents, there have been increasingly more changes and additions to accounting regulations. These changes have brought about more uncertainty to the accountant's work environment (Hamdan 2017; Steinbart et al. 2018). ISPs are designed and deployed based on specific business processes. Therefore, the implementation of new accounting rules means that new ISPs should be devised by adding or modifying existing ISPs. Therefore, I argue the accountants' work uncertainty from accounting-rule changes will be another essential condition to enhance the effect of ISP controls on ISP pressure. Whether organizations are adding new ISPs or modifying an existing ISP, both require mental and behavioral adjustments, which both result in more ISP pressure. Therefore, the second goal of this study is to examine whether the effect organizational ISP controls on ISP pressure will be weakened by an accountant's ISP self-efficacy but will be enhanced by the level of work uncertainty perceived by an accountant.

Based upon the fraud triangle theory, in the context of accounting employees' ISP violating behavior, I develop and test a model that evaluates the effects of how higher levels of information security controls within an organization can have an unintended impact on accounting employee's ISP pressure levels to commit intentional ISP violations. Furthermore, I consider how ISP self-efficacy as a personal characteristic and how perceived work uncertainty may be a significant environmental characteristic for determining the unintended impact of ISP controls on ISP stress. Based on the analysis of a data set of 163 responses from accountants, it does appear that although ISP controls will significantly reduce accounting employees' opportunity to violate ISPs. They also increase violating intention by increasing the ISP pressure of accounting employees. The

effect of ISP controls on ISP pressure is reduced by the ISP self-efficacy but is enhanced by the perceived work uncertainty.

These findings contribute to the literature by (1) proposing and confirming ISP stress as the key factor to explain the side effect of organizational ISP controls on the violating intention of accounting employees, which extends the suggestion of the "pressure" aspect of the fraud triangle theory; (2) to the best of my knowledge, be the first to consider newly emerging intentional ISP violation behaviors of accountants in the extant accounting literature; (3) identifying high work uncertainty and low ISP self-efficacy as possible explanations for the high ISP stress of accountants when facing high levels of controls.

Theoretical Background

Management control over the processes, activities, and behaviors of employees has been an integral part of any organization (Zimmerman 2006) and also a significant concern in the accounting literature stream (Fiolleau et al. 2018). Management control includes any systems managers use to ensure the behavior and decisions of their employees are aligned with an organization's objective and goals (Malmi and Brown 2008). For example, accounting controls like budgets and performance measures, administrative controls including organizational structure and governance, and social controls such as values and culture must be assimilated in the management control system (Fiolleau et al. 2018). Although management controls have pledged effective organizational operations, there has been evidence that suggest otherwise. Research has suggested that these formal management controls can negatively affect the attitudes and behaviors of employees subjected to these controls (Christ et al. 2008; Das and Teng

2001; Dineen et al. 2006). Negative consequences of control include decreased effort and cooperation, reduced organizational citizenship behavior, and in extreme cases, employee fraud or theft (Christ 2013; Das and Teng 1999; Das and Teng 2001; Dunlop and Lee 2004).

The accounting literature recognizes ISP as a type of mandatory control system (Boss et al. 2009; Dopuch et al. 1974). Previous research has shown that when policies are implemented into an organization, this is a signal to employees. Employees are then expected to comply with the new changes (Chae and Poole 2005; Malhotra and Galletta 2005). Using the control theory to view the concept of mandatoriness, it is evident when employees perceive ISPs as mandatory; they are more likely to take security precautions (Boss et al. 2009). In this study, the term organizational formal ISP controls refer to the existing organizational formal general ISP policies.

Previous research has also used the reactance theory as a theoretical lens to explain why high levels of ISP controls could backfire and increase undesirable employee behavior (Lowry and Moody 2015; Posey et al. 2011a). The reason being most employees have a tacit limit for the degree of tolerance they will feel towards management policies that are controlling and a similar threshold for how much individual freedom they will give up before negative consequences for the organization will occur. In short, studies have indicated that management controls on employees may not achieve the expected outcomes, especially the ISP controls. However, there is still a need for a deeper understanding and explanation of the unexpected effect of ISP controls on ISP violating behavior.

The fraud triangle has been a well-known conceptual framework for understanding the drivers of fraud. It has organized part of the management control literature that focuses on reducing dysfunctional behavior. While the fraud triangle has been historically used for explaining fraud behavior as wrongful criminal intentional deception for personal gain involving a violation of trust, researchers have argued that the fraud triangle could be extended to explain general dysfunctional behaviors of employees (Cressey 1953; Fiolleau et al. 2018; Ramamoorti 2008; Ramamoorti and Olsen 2007). Dysfunctional employee behaviors occur when individuals knowingly make a choice that puts their interests before that of the organization (Cohen et al. 2007), which is not illegal (e.g., not fraudulent), yet are contrary to the organizational shareholders' interests. In this study, dysfunctional behaviors are considered as the intentional but not malicious ISP violating behaviors of accountants, which is often intentionally committed for convenience or an expression of one's dissatisfaction but without financial gain, such as copying sensitive data to USB drives to continue an accountant's work remotely, password sharing, failure to logoff computer.

It is generally argued that if all of the three fraud triangle elements — (1) pressure, (2) opportunity, and (3) attitude or rationalization — are present within the organization, then dysfunctional behavior risk is higher (Cressey 1953; Fiolleau et al. 2018). In other words, if the organizational management control systems effectively control the three elements, the dysfunctional behaviors of employees are expected to be vastly reduced. In the early version of the fraud triangle, these three elements are all found to be essential (Cressey 1953; Cressey 1954). However, as the fraud triangle evolved, the relative importance among the three elements is found to be determined by

the specific dysfunctional behaviors. The level of importance of the three corners of the triangle has shown to be different when conceptualized in a different context (Dorminey et al. 2012; Johnson et al. 2013; Trompeter et al. 2013). For example, previous accounting literature has categorized four different types of dysfunctional behaviors as misreporting of accounting information, earnings management, illegal actions, and self-interested investment decisions (Fiolleau et al. 2018). Therefore, these different types of behaviors suggest different management controls should be uniquely developed to effectively control the opportunity, rationalization, and pressure under different circumstances.

Each element of the fraud triangle has been mainly conceptualized to explain fraudulent behavior, which is commonly known as illegal and malicious behavior. The pressure for fraud behavior mainly refers to the pressure from a non-shareable financial problem (Ashton 1990; Cressey 1953; Dorminey et al. 2012). However, in the context of intentional but non-malicious ISP violating behavior, a non-shareable financial problem is not expected to be the primary source of pressure. Instead, ISP controls are expected to become the source of pressure for the violation behavior. The perceived opportunity for fraud is seldom purposefully provided to the employee. However, in the case of perceived opportunity for an intentional but not malicious ISP violation, it will be commonly presented. For example, accounting employees often work in a collaborative environment (Wessels 2005). This may result in new, unmotivated, uncooperative, poor adaptation to technological advances in the industry, knowledge sharing risks, and regulation risks (Bhimani and Willcocks 2014; Coras and Tantau 2013; Low et al. 2008). In the context of ISP violation behavior, team members may intentionally share

passwords, encourage remote access to information systems or failure to secure workstations in order to ensure their accounting team continues to perform work duties as quickly as possible (Safa et al. 2018). Therefore, the perception of opportunity may not play as critical a role in intentional ISP violation behavior. The rationalization for malicious fraudulent behavior is also expected to be more critical than the rationalization for intentional but non-malicious ISP violations. For example, the ethics of the employees will prevent them from violating the organization's ISP, as suggested in the existing literature (Bulgurcu et al. 2010; Chia and Lim 2000; Goles et al. 2006). Therefore, it is expected that the pressure element of the fraud triangle will be the most critical trait to explain the effect of ISP controls on accountants' ISP violating intention. Concise definitions of all constructs in this study have been listed in Table 3-1.

Table 3-1

Constructs in the Research Model

General Concept	**Construct**	**Operational definition**	**Reference**
Management Controls	*ISP Controls*	The organization's ISP tools that seek to elicit behavior that achieves strategic objectives of an organization, such as budgets, performance measures, standard operating procedures, and protection of digital assets	(Free et al. 2007)
Pressure	*ISP Stress*	Employee's attempts and struggles to deal with constantly evolving workplace information security policies and the cognitive and social requirements to complete their work duties	(D'Arcy et al. 2014; Ragu-Nathan et al. 2008; Tarafdar et al. 2010)
	ISP Uncertainty	Situations where the organization continually updates and changes its job-related security requirements	
	ISP Overload	Situations where security requirements increase the workload for employees which may create time pressures for them to complete job duties	
	ISP Complexity	Situations where security requirements are viewed as overly complex either forcing employees to expend time and effort in learning to understand security requirements or are unable to grasp the security policy fully	
Opportunity	*ISP violation Opportunity*	The extent to which circumstances exist when there is an absence of controls, ineffective controls, or ability to override controls	PCAOB 2015 AU 316.07
Rationalization	*ISP violation Idealism*	Individual's belief that any technology-related action should maximize the good without harming another	(Chatterjee et al. 2015; Forsyth 1980)
Work uncertainty	*Work uncertainty*	Individual's inability to assign probabilities with confidence with regard to how environmental/work factors are going to affect the success or failure of the accounting employee	(Colquitt et al. 2012; Duncan 1972)
Computer Self-efficacy	*ISP self-efficacy*	Individual's judgement in their capability to organize and execute information security policies	(Rhee et al. 2009)
Fraud behavior (Violation of Trust)	*Intentional ISP violation intention*	Any act by an employee that is against the established information security policy of the organization	(Bulgurcu et al. 2010; Willison and Warkentin 2013)

Hypotheses Development

Associations Between ISP Controls and Elements of the Fraud Triangle

ISPs specify the standards, boundaries, and responsibilities for accountants of information and technology resources in order to facilitate the prevention, detection, and response to security incidents (Bulgurcu et al. 2010; Lowry and Moody 2015). For example, the creation of Sarbanes-Oxley began imposing internal control obligations for accountants (Rockness and Rockness 2005; Wallace et al. 2011; Walters 2007). Explicitly, Section 302, in addition to certifying the accuracy of disclosures, officers must affirm that they are responsible for internal controls; and designed such controls to ensure that material information has been presented to report this conclusion about its effectiveness. Given perception of opportunity in this study refers to the perceived cost for accountants able to acquire unauthorized access to the organizational information system or other employees' computers by violating some ISP, the perceived opportunity arises when accountants have the perception (1) that an ISP control weakness is present, (2) that the likelihood of being caught is remote. Therefore, higher ISP control is expected to reduce the perceived ISP violating opportunity. Hence, I hypothesize that:

H1a*: An accountant's perceived organizational ISP controls will be negatively associated with the perceived opportunity to commit ISP violations.*

Accountants' attitude to the ISP violating behaviors or how the accountants will rationalize the ISP violating behavior will naturally depend on their morality; therefore, I use idealism as a proxy. Idealism refers to the positive ethical values held by the employee to prevent them from harming others intentionally(Forsyth 1980). Thus, individuals high in idealism seek to avoid harm by always assuming the proper action

(ISP controls). In other words, some employees may possess an attitude or set of ethical values that allow them to knowingly and intentionally commit a dishonest act against the organization (Murphy and Free 2016). While attitudes are changeable, as clearly demonstrated by social psychology research (Elliot and Devine 1994), ethical values presumed to be one's beliefs about right versus wrong, are not as easily swayed (Bayou et al. 2011; Ghoshal 2005; Wenzel 2005). Instead, ethical values are formed gradually as individual's gain experience and form knowledge of their surroundings (Bazerman and Tenbrunsel 2012; Nevins et al. 2007). Therefore, they are less likely to be associated with ISP controls in the organization. Therefore, I hypothesize:

H1b*: An accountant's perceived organizational ISP controls will be not significantly associated with their level of idealism.*

Early accounting literature has found that the quantity and quality of task demands (i.e., work-related stressors) and control in organizations are the main antecedents to cause the accounting employees' stress (Libby 1983). Therefore, I bring focus on the stress sourced from the information security tasks and ISP controls for the accountants. Borrowing the conceptualization of employees' security-related stress (SRS) in the IS literature, I conceptualize the ISP pressure of accountants as pressure from overloaded, complexity, and uncertainty of information security requirements/policies. Implementation of stringent security controls may trigger undesirable information security behavior because individuals may feel pressured to perform at the same operational level before the implementation of ISPs, which can cause employees to view these controls as constraining, inconvenient, and difficult to understand (Posey et al. 2011a). For example, employees perceive increased security measures as job stressors

(Moore et al. 2008) and privacy invasions, which lead to increased rather than decreased computer abuse incidents (Posey et al. 2011b). Therefore, I argue that increases in internal ISP controls within organizations can be evaluated in terms of organizational triggers. When organizations enforce an increased amount of ISP controls, the more ISP pressure is expected to be perceived by the accountants. Hence I hypothesize:

> ***H1c:*** *An accountant's perceived organizational ISP controls will be positively associated with their perceived ISP stress.*

Associations Between Elements of the Fraud Triangle and Intentional ISP Violations

As discussed, although the fraud triangle has been extended to explain the general dysfunctional behavior, beyond the typical fraudulent behavior, different dysfunctional behaviors may make these three elements of the fraud triangle show different importance in explanatory power. For intentional ISP violating behavior, I emphasize the non-malicious and distinguish it from malicious ISP violating behaviors, such as computer fraud, revealing confidential information to outsiders that may harm an organization, writing viruses, and software piracy (D'Arcy et al. 2009; Siponen and Vance 2010).

When comparing malicious dysfunctional behaviors (e.g., fraud) to dysfunctional behaviors that are not illegal (i.e., not fraudulent), accountants may not act in shareholders' interest but cannot be committed by an outsider (Fiolleau et al. 2018). In other words, the perceived opportunity for intentional ISP violations should be more natural to identify rather than the opportunity for malicious ISP violations. For example, accountants could easily violate the ISP to share passwords with other employees at little to no cost. However, there are higher barriers for accountants to cross to copy sensitive

personal company data and share this data with competitive companies (Fiolleau et al. 2018). Hence, I argue opportunities for intentional, but non-malicious ISP violations will be easier to identify. In this condition, idealism and ISP pressure will emerge as two direct factors that result in intentional ISP violations. High idealism means that accountants believe that any technology-related action should maximize the good without harming another (Forsyth 1980). Then even when an opportunity exists, an accountant with high idealism will not intentionally violate the ISP because this behavior conflicts with their values.

On the other hand, accounting employees' stress will produce higher levels of dysfunctional organizational behavior (Fogarty et al. 2000; Gaertner and Ruhe 1981; Libby 1983). Therefore, high levels of ISP pressure will create motivations for an accountant to utilize the opportunity to violate ISP for personal convenience. For the opportunity itself, I argue the existence of an opportunity for an intentional ISP violation will not be an essential condition that results in ISP violations. Therefore, based on the discussion above, I hypothesize that:

H2a: *An accountant's perceived opportunity for ISP violations is not significantly associated with intentional ISP violations.*

H2b: *An accountant's idealism will be negatively associated with intentional ISP violations.*

H2c: *An accountant's perceived ISP stress will be positively associated with intentional ISP violations.*

Moderating Effect of ISP Self-Efficacy and Perceived Work Uncertainty

New global business models and the digital age have shifted expectations of the work of accountants. Accounting employees have felt comfortable claiming job success attributed to the level of specific technical skills acquired by the accountants (Rebele 1985). However, as society continues into the digital age, more academic studies have shown that the accountants need to develop higher technological adaptability by acquiring new IT skills and determining how new technologies should be best incorporated into their accounting practices (Cory and Pruske 2012; Pan and Seow 2016; Stanciu and Tinca 2016).

Self-efficacy is the belief that one has the capability to perform a particular behavior (Bandura 1977). Self-efficacy perceptions have been found to influence decisions about what behaviors to accept. Self-efficacy refers to the amount of effort and persistence when individuals attempt to perform a specific behavior. The response to the particular behavior may cause levels of stress and anxiety to the individual (Bandura 1977; Hackett and Betz 1981). Therefore, in the context of this research, information security policy self-efficacy is defined as the belief that one can organize and execute information security policies with success. It incorporates judgments of the ability to apply technical skills to broader tasks (Compeau and Higgins 1995) (e.g., deciphering technical jargon, applying needed encryption, analyzing what programs are needed). Individuals with high ISP self-efficacy might perceive themselves as being able to accomplish all regulated tasks required without assistance than those of lower judgments of self-efficacy. Therefore, facing the same ISP controls, accountants with high ISP self-efficacy will have less ISP stress perception because they will believe they may be able to

handle these ISP controls effectively (Gist and Mitchell 1992; Herath and Rao 2009; Ifinedo 2012). As such I hypothesize:

H3a: *An accountant's ISP self- efficacy will negatively moderate the relationship between ISP controls and perceived ISP stress.*

The level of ISP controls within an organization will influence an accountant's ISP pressure, which will be the critical factor in their intent to violate ISPs. I argue there will be two critical conditions (personal and environmental characteristics) for a relationship between ISP controls and ISP pressure. The discussion above reflects the personal characteristic.

The environmental characteristic of ISP compliance will be considered as the work content and responsibility of a specific accountant's position. Any changes in the assigned work will mean changes with the corresponding ISP. For example, accountants often face new accounting-rule changes, which will not only mean there will be new accounting tasks to finish but also new ISP requirements to follow. Therefore, I consider any work changes of an accountant as work uncertainty. Uncertainty has been identified as an essential related variable because it makes managerial planning and effective internal control more difficult (Duncan 1972; Lawrence and Lorsch 1967; Weick 1969). For example, different facets of the organizations which face unpredictable change may find that static budgets are ineffective control devices because the initial standards rapidly become out of date. In the case of employees who anticipate more work uncertainty (internal ISP changes), I expect that controls on existing ISP will cause more ISP pressure because new ISPs may be added or an existing ISP may be modified. For example, the evolving data breach notification laws and other security-based regulations

(i.e., Sarbanes-Oxley Act [SOX]) and Health Insurance Portability and Accountability Act [HIPPA]) have imposed new encryption rules and authentication procedures for accessing corporate systems (Chen et al. 2012; Kwon and Johnson 2013).

A consequence of these dynamic organizational security environment is that employees are continually adjusting to new requirements with little chance to develop a base of experience or assimilate security into their work routines. This uncertainty can be unsettling for employees and cause higher stress. Recent research provides evidence that changes within employees' work environments (e.g., relationship strains and job changes) relate to IT espionage and sabotage incidents (Shropshire 2009). Therefore, I hypothesize:

H3b: *An accountants' perceived work uncertainty will positively moderate the relationship between ISP controls and perceived ISP stress.*

The resulting research model is illustrated in Figure 3-1.

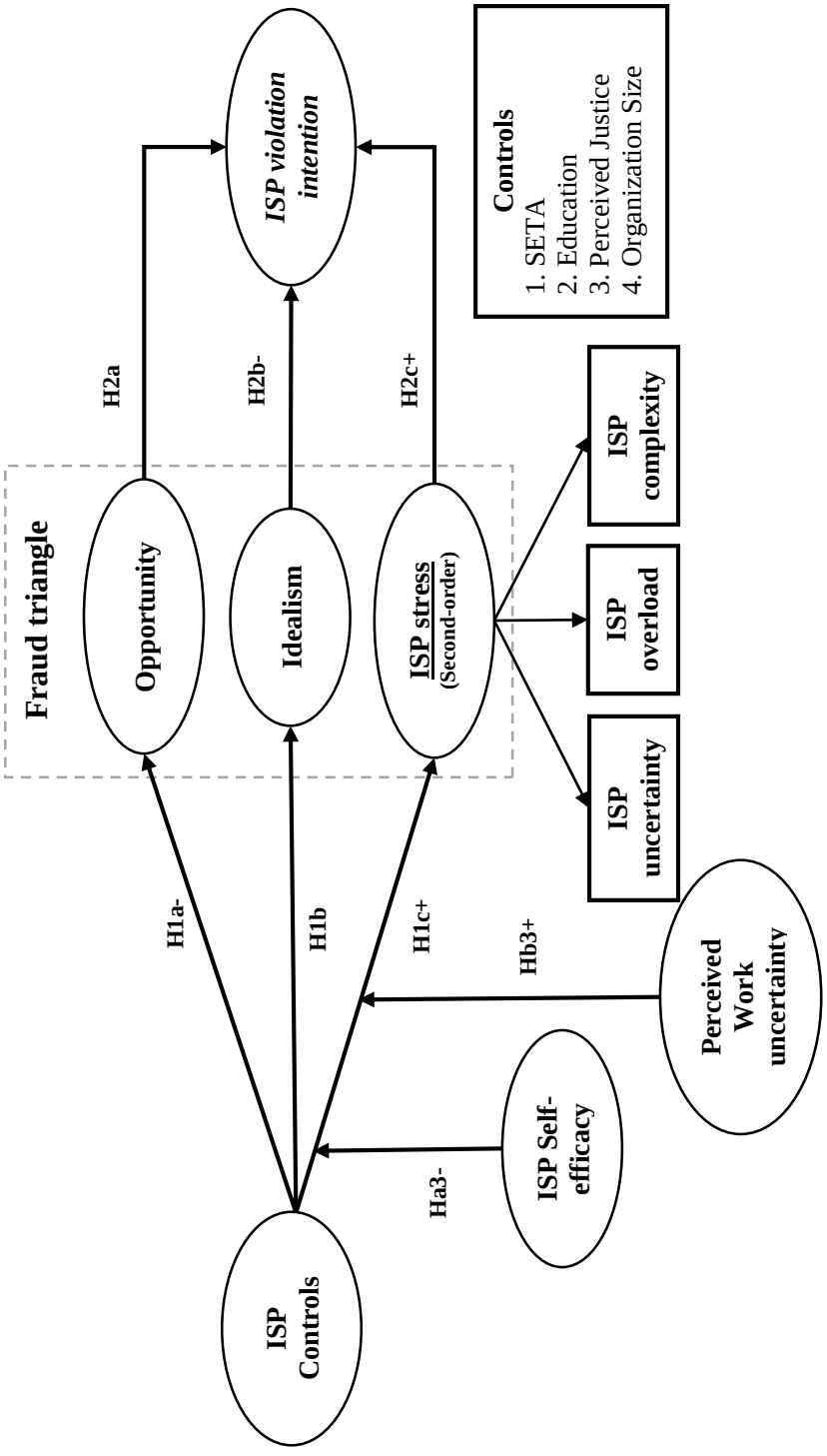


Figure 3-1: Research Model

Methodology

I developed a two-time point survey. The first time point focuses on the responses on ISP controls, three elements of the fraud triangle and two moderators (ISP self-efficacy and perceived work uncertainty) while the second time point contained the instrumental climate measure. I intentionally separate the responses on ISP violations as the dependent variable and responses on other constructs in this study in order to eliminate the possibility of common method bias (Podsakoff et al. 2012). The data used in this study was collected from a sample of full-time accounting professionals in the U.S.

The measurement items in the questionnaire were adapted from existing validated and well-tested scales in the extant literature. In addition to using previously validated questions, all measures were pretested by two business professors with expertise in survey research and ten professionals with ISP experience. The objective of the pretest was to ensure that the measures were meaningful and they unambiguously captured the domain of each construct. Based on detailed interviews with each professional, appropriate changes were made to the measures. All measures were pilot tested in a survey with a small portion of the targeted sample, which only resulted in minor wording changes. I conducted a reliability analysis and exploratory factor analysis for each set of measures. The validity and reliability of the adapted measures fulfilled the necessary requirements, which indicated all measures were clear to the targeted samples, relevant, and captured the intended concepts. The results placed sufficient confidence in the measures to proceed with the survey administration of the target sample frame. All scales used in the study are presented in Appendices. In the questionnaire, all items were

measured with 5-point Likert scales, ranging from “strongly disagree” to “strongly agree.” These measures had been proved to have good validity and reliability.

In this study, the dependent variable is the respondent’s self-reported intention to conduct intentional but non-malicious ISP violations. I adopted the work of Willison and Warkentin (2013) of not changing passwords regularly, delayed security backup, and bringing materials back home, as three specific examples of intentional but not malicious ISP violations for respondents to accurately evaluate their intention. In particular, the survey emphasized “not malicious” in each statement. Also, to avoid the social desirability bias, there was no use of the “first-person perspective” but “third-person perspective” for each statement to measure the ISP violating intention. The response options ranged on a fully anchored scale from one to five, in which five served as ‘strongly agree’ with the statement that the respondent would engage in actions similar to those of the hypothetical employee in the scenario under circumstances that represented various levels of the antecedent variables.

For the organization, ISP controls, I used two items focusing on the “perceived organizational ISP formal controls” to capture it, which are adapted from the work of (Hsu et al. 2015). The ISP pressure in this study is considered as a second-order construct, estimated using the factor scores of its three first-order dimensions as reflective indicators, respectively ISP uncertainty, ISP complexity, and ISP overload (D'Arcy et al. 2014). ISP overload describes situations where ISP increases the workload for employees and, as a result, creates added time pressure for them to complete job duties. ISP complexity describes situations where ISP are viewed as complex and thereby forces employees to expend time and effort in learning and understanding security measures.

ISP uncertainty refers to contexts where the organization continually updates and changes its job-related ISP.

For the ISP violation opportunity, I used the extent to which an accountant could generally access the company's computer resources without the authorization, using three items adapted from (Pratt and Cullen 2000). Rationalization, as the final element of the fraud triangle, has been measured by the individual's level of idealism (Forsyth 1980), which is also adopted and adapted as three items in this study. To evaluate the ISP self-efficacy, it was required of the respondents to report their capacity to complete their job using technology and follow the ISP requirements, respectively in the condition of "no one to tell them," "only software manuals," and "no prior software usage experience," which are adapted from the work of (Compeau and Higgins 1995). Finally, to measure another moderator, perceived work uncertainty, I adopted the four items of (Colquitt et al. 2012) to evaluate the changes in their work situation and content.

To control the potential alternative explanation on the hypothesized relationship, I considered the heterogeneity from the individual level and organizational level and also measure them in this study. First, I consider the ISP training and education of the accountants as two important individual characteristics to be controlled. Additionally, I also consider two critical organizational characteristics, respectively, organizational justice and organizational size (number of employees within the organization of the respondent). The examination of the control variables and their influence on ISP violating intentions revealed that none of these significantly influenced how employees may formulate their intentions to commit an intentional ISP violation. In the questionnaire, all

items were measured with 5-point Likert scales, ranging from “strongly disagree” to “strongly agree.”

I used a market research firm to invite full-time professional accountants to take the survey. External panelists have been used increasingly in accounting IS research (Ayyagari et al. 2011; Bulgurcu et al. 2010) and have certain advantages over traditional methods that were key to this study. First, panels guarantee respondent anonymity and thereby encourage honest responses to questions that may be subject to socially desirable responses. Second, external panels contain respondents from a wide range of industries and positions. The marketing research firm was instructed to collect responses from employed computer-using accountant professionals. Respondents were paid $10 each for participating in the study. In the questionnaire, the targeted samples were first asked to indicate their computer experience in the company. If the participant did not use a computer extensively as part of their daily work duties, that person was excluded from further consideration. The questionnaire then asked the respondents to measure the subjects’ perceptions of each research constructs.

A total of 574-panel members accepted the invitation to participate in the survey by viewing the consent agreement and clicking past the first page. After excluding incomplete responses, a total data set of 163 responses were included in all analyses. Table 3-2 shows additional demographics for these respondents. Sample demographics reveal that 57 percent were female and tended to be well-educated (72 percent with at least a bachelor’s degree).

Table 3-2

Sample Demographics

Respondents' Gender	**Percentage**	**Respondents' education**	**Percentage**	**Work age**	**Percentage**
Male	42.9%	High school	15.3%	<1 Year	0.6%
Female	57.1%	Technical Degree	12.3%	1-5 Years	28.2%
ISO certification	**Percentage**	College Degree	47.9%	5-10 Years	30.7%
Yes	41.7%	Graduate Degree	23.3%	10-15 Years	12.9%
No	58.3%	Doctoral Degree	1.2%	>15 Years	27.6%

Data Analysis and Results

Following the recommendations of Lowry and Gaskin (2014), there are reasons for this study to employ the use of Partial Least Squares (PLS) for building and testing the research model. First, PLS-based structural equation modeling (SEM) is easier for me to process the second-order construct of ISP related stress. Second, PLS-SEM is a "silver bullet" in this research situation when models are relatively complex and representative sets of data are rather small (Lowry and Gaskin 2014; Ringle et al. 2012). By using PLS estimation, the variance observed in the dependent variable can be maximized, which conform to the study's intention to identify the explanatory power of the fraud triangle on the intentional violation behavior and further compare the relative importance of the three-factors of the fraud triangle. Therefore, in my study, SmartPLS (version 2.0) was the primary statistical tool to analyze the measurement and structural models.

The measurement model was tested by assessing both the convergent and discriminant validity. Because the study viewed ISP stress as superordinate, second-order constructs composed of multiple reflective, first-order dimensions, the validity of the

reflective measures (three dimensions of ISP pressure) were also assessed. Validity was assessed three ways. First, I assessed convergent validity, which is how each item was related to its corresponding construct by examining the factor loadings. Convergent validity is considered satisfactory if the factor loading of a measure is 0.7 or higher. All factor loadings were above the cutoff point of 0.70 with a t-value higher than 1.96. The measures loaded on their appropriate factors and there was no evidence of significant cross-loading. Average variance extracted (AVE) was also examined to evaluate convergent validity. AVE is greater than 0.5, establishing convergent validity. The results in Table 2 show that each construct had an AVE greater than 0.5, which suggests that the measures exhibited adequate convergent validity. Second, the reliability of the measures was examined through two criteria, Cronbach's alpha (CA) and composite reliability (CR). The CA and CR of construct was greater than 0.7, a common threshold for signifying satisfactory construct reliability. According to the results, the minimum CA and CR values exceed the recommended threshold of 0.7, indicating acceptable reliability of the measures. Third, discriminant validity is verified by the difference between the AVE of a construct and its correlation with other constructs. For adequate discriminant validity, the square roots of AVE of any construct should be greater than the correlations between the construct and other constructs, which means that the diagonal elements should be greater than corresponding off-diagonal ones (Fornell and Larcker 1981). As per the results in Table 3-3, the criterion for discriminant validity was also met in this study.

Table 3-3

Descriptive Statistics, Correlations (Among Directly Observed Constructs) and Reliability

Construct	***Mean(SD)***	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***9***	***IVI***
ISP Control	*2.48(0.93)*	***0.924***								
ISP Oppo	*4.14(0.73)*	*-0.23***	***0.936***							
Ideal	*4.36(0.73)*	*-0.23***	*0.13*	***0.858***						
ISPU	*3.06(1.05)*	*-0.06*	*0.20***	*0.10*	***0.875***					
ISPO	*2.26(1.02)*	*0.40***	*-0.14*	*-0.19**	*0.46***	***0.892***				
ISPC	*2.13(0.99)*	*0.48***	*-0.16*	*-0.28**	*0.35***	*0.70***	***0.890***			
WrkU	*2.62(1.13)*	*0.36***	*-0.13*	*-0.21**	*0.19**	*0.49***	*0.51***	***0.891***		
SE	*3.14(1.05)*	*-0.04*	*-0.01*	*-0.11*	*-0.05*	*-0.09*	*-0.20**	*0.01*	***0.853***	
IVI	*2.94(1.05)*	*0.22***	*-0.09*	*-0.07*	*0.1*	*0.32***	*0.35***	*0.31***	*-0.12*	***0.896***

Note: ** $p < 0.05$; ** $p < 0.01$;* Diagonal elements (in bold) are the square root of the AVE; The off-diagonal elements are the correlations among the constructs; Oppo=opportunity; Ideal= Idealism; ISPU=Information security policy uncertainty; ISPO= information security policy overload; ISPC= information security policy complexity; WrkU= work uncertainty; SE= ISP self-efficacy; IVI= Intentional ISP violation intention.

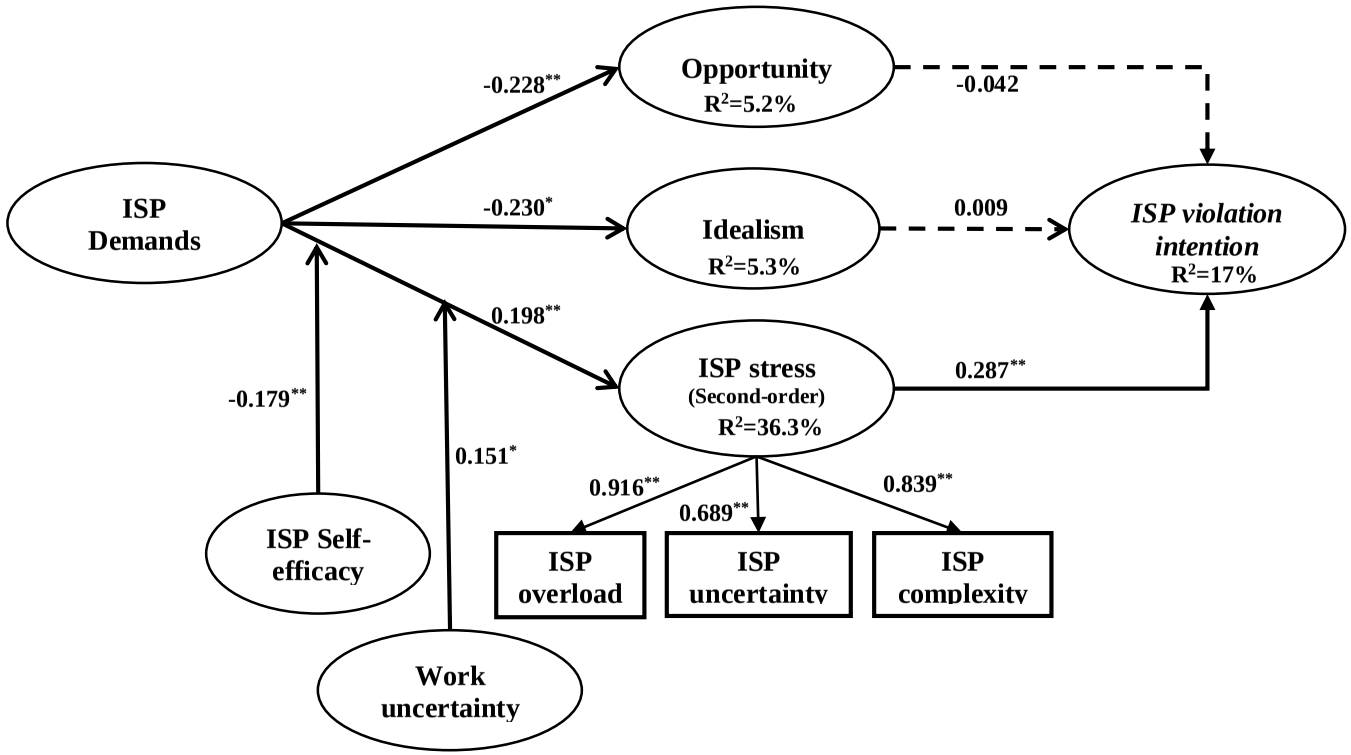
Common method variance (CMV) may have confounding effects on the observed relationships between the predictors and criterion variables (Podsakoff et al. 2003). Although the data was collected in two different phases with a two-week time difference for independent and dependent variables, data were all rated by employees, and thereby the potential CMV might not be removed completely. To further assess the potential effects of common method bias, Harman's single-factor test was conducted, and results showed all of the items of constructs in the research model cannot be loaded in a single factor in an EFA. In particular, no high correlation was found between the same marker variables in time 1 and time 2. The marker variables have low and insignificant correlations with all the studied constructs, while the partial correlations between the key

constructs were high and significant. Both of Harman's single factor test and marker variables test make the study confident that common method bias won't threaten the data results.

Results of Structural Model

The structural model for the hypotheses test is also examined through Smart PLS 2.0. I followed the steps proposed by (Aiken and Stephen 1985; Aiken et al. 1991) to examine the moderation hypotheses. The interaction terms were mean-centered before creating the interaction variables in order to reduce the potential for collinearity (Chin et al. 2003). Bootstrapping (1000 resamples) was used to determine the significance of the path coefficients. The second-order ISP stressors were estimated using the factor scores of their first-order dimensions as reflective indicators as seen in D'arcy et al (2014). The results for the structural model are presented in Figure 3-2. The model explains 17% of the variance of intentional ISP violation intention.

As shown in Figure 3-2, the organizational ISP controls will significantly reduce the perceived ISP opportunity in the organization ($\beta = -0.228$, $p < 0.01$; H1a is supported). On the other hand, the ISP controls will result in the higher ISP stress on the accountants ($\beta = 0.198$, $p < 0.01$; H1c is supported). Surprisingly, my results revealed the ISP controls will also reduce the idealism ($\beta = -0.230$, $p < 0.05$), therefore H1b is not supported). This result may be explained by the subjective measurement on the idealism. The high ISP controls perceived within an organization could have negatively impacted an accountant's perception of job autonomy (e.g. working remotely, high collaborative environment). This effect can gradually lower an accountant's resolve of idealism and distort their cognition.



Notes: Paths in dash are not significant (p > 0.05). Non-significant control variables are not shown. * p < 0.05; ** p < 0.01.

Figure 3-2. Structural Model Results

Among the three factors of the fraud triangle, only ISP related pressure is significantly related to the intentional ISP violation intention ($\beta = 0.287$, $p < 0.01$. H2c is supported). Both perceived ISP violating opportunity and idealism are not significantly related to the intentional ISP violation intention. H2a and H2b aren't supported in this study. These results show that the ISP pressure will be the only important element in fraud triangle to result in the ISP violation intention.

Finally, focusing two moderators on the effectiveness of the ISP controls on ISP stress, the results show that the standard path coefficients of work uncertainty ($\beta = 0.151$, $p < 0.05$) have positive and significant effect on ISP related pressure, which support the hypotheses H3b. In addition, the moderating effect of ISP self-efficacy on the relationship between ISP demands and ISP related stress is also significant ($\beta = -0.180$, $p < 0.01$).

Discussion

I theorize ISP controls as one type of formal management control and contextualize three elements of fraud triangle into accountant's intentional ISP violating behavior, respectively perceived ISP violating opportunity, accountants' idealism, and perceived ISP pressure. By linking accounting management controls and the fraud triangle together, I further explain the dysfunctional behavior. I examined how the ISP controls will influence the intentional ISP violating behavior via three elements of the fraud triangle. Using 163 responses from accounting professionals, it revealed that ISP controls did significantly influence the fraud triangle. ISP controls did indeed function properly by reducing opportunities for ISP violations. However, the shortcoming of high

levels of ISP controls created a lower sense of idealism and most importantly enhanced an accountant's perceived ISP pressure.

Among the three elements of the fraud triangle only ISP pressure was significantly associated with the accountants' intentional ISP violating behavior. Furthermore, ISP pressure was the only effective element to transfer the effect of organizational ISP controls to the ISP violation intention. I also examine the conditional effect of ISP self-efficacy as a personal characteristic and work uncertainty as an environmental characteristic on the relationship between ISP control and ISP pressure. Results show that high ISP self-efficacy will effectively reduce the ISP stress from ISP controls, but high work uncertainty will increase this pressure perception. These findings provide important contributions to the accounting literature and accounting employee management practice as follows.

Implications for the Accounting Literature and Future Research

First, this study to the best of my knowledge is the first to examine the newly emerging intentional ISP violation behaviors of accountants in the extant accounting literature.

Second, it contributes to accounting management controls literature by using the fraud triangle to explain the side effect of ISP controls on intentional ISP violating behavior. Previous accounting management control research has observed that formal controls can negatively affect the attitudes and behavior of employees subjected to the control (Christ 2013). Given that organizations cannot operate effectively without formal control mechanisms, it is important to the literature to expand the understanding of specific characteristics of controls that may elicit a negative response from employees so

organizations can limit these unintended consequences (Christ 2013; Enzle and Anderson 1993). In this study, I further identified and confirmed ISP pressure as the key factor to explain the side effect of organizational ISP controls on the intentional violating intention of accounting employees.

Third, this study contributes to the fraud triangle framework by examining its antecedents and extends its application in ISP violating behavior, beyond the fraud behavior known as wrongful criminal intentional deception for personal gain involving a violation of trust (Ramamoorti 2008). Dorminey et al. (2012) and Fiolleau et al. (2018) have called for the application of fraud triangle into general dysfunctional behavior, especially non-malicious behavior, and implied the different importance of three elements of the fraud triangle on explaining different, specific dysfunctional behavior. I confirmed this notion and empirically revealed that ISP pressure should be a dominant factor in explaining the specific dysfunctional behavior--intentional ISP violating intention, compared to another two elements (ISP violating opportunity and idealism).

Finally, I also contribute to the accounting stress literature by borrowing one new type of pressure, which is SRS, from IS literature. Although multiple sources of stress have been considered in existing accounting literature, such as the acronym M.I.C.E (M: money; I: ideology; C: coercion; E: ego) (Kranacher and Riley 2019), ISP pressure is rarely considered in the accounting studies. This study confirmed the role of ISP pressure in explaining the intentional ISP violating behavior. In addition, the supported link (ISP controls—ISP pressure—Intentional ISP violations) in this study is also consistent to the accounting stress model (Libby 1983). The task demands and management controls did result in accounting employees to perceive higher levels of stress causing increments or

decrements in cognitive performance (i.e. higher levels of ISP pressure resulting in intentional ISP violating behavior) Around this new type, stress, I further identify high work uncertainty and low ISP self-efficacy as possible explanations for the high ISP pressure of accountants when facing high levels of controls.

Implications for Practice

The findings also have important implications for practice as well. First, accounting managers should notice the side effect of organizational ISP controls. Although it's taken for granted that high controls will offer little to no opportunity for the dysfunctional behaviors, the findings showed that ISP violating opportunity is always high in the organization and more importantly it shows no direct effect on the ISP violating intention.

In contrast, the higher ISP controls will motivate the accountants' intentional ISP violating behavior by increasing their ISP pressure. Therefore, managers should make a careful balance to achieve the "perfect mix" of controls. Second, accounting managers should also take a hard look at their ISPs to understand the limitations the ISPs have created for their accountants. Accounting professionals have been characterized as a high-pressure position. Therefore, any new source of stress should be carefully considered. Finally, accounting managers should also notice the difference between illegal/malicious behavior and intentional but non-malicious behavior of accountants. Increased ISP controls in the context of illegal/malicious behavior may be beneficial since they reduce opportunity.

Limitations

There are also some limitations to the research methodology in this study. First, the results may still contain the social desirability bias, especially by using the self-reporting way to measure idealism and intentional ISP violating intention. Several steps were taken to overcome this issue including "third-person perspective" in the measuring statement and two-time point research design. Second, the findings in this study are based on a relatively small sample (163 accounting professionals). Therefore, careful consideration should be taken before generalizing the findings of this study. Third, future studies may benefit by expanding on the types of rationalization an accounting employee may undergo when faced with the decision to act upon dysfunctional employee behaviors. In this study, idealism may not have given researchers and practitioners alike a full picture of what ethics may do for accounting employees. Finally, although ISP violations were conceptualized as general violations, future researchers could further examine specific intentional ISP violating behavior, such as sharing passwords with colleagues, to obtain more contextualized but insightful findings.

Conclusion

In focusing on explaining how ISP controls influence intentional ISP violating behavior as a newly emerging behavior of accountants, I utilized the fraud triangle in this research setting to connect the ISP organizational control to the three legs of the fraud triangle for dysfunctional behavior to occur: opportunity (ISP violating opportunity in this study), pressure (ISP stress), and attitude/rationalization (idealism). The results show that ISP controls did reduce the ISP violating opportunity but meanwhile increased the ISP stress. However, the opportunity for ISP violations did not directly change the

violating behavior, but instead ISP stress will contribute to higher ISP violating intention. These findings show the side effect of ISP controls on ISP pressure. By incorporating personal (ISP-self efficacy) and environmental characteristics (work-uncertainty), my study reveals these factors will, in fact, impact an accounting employee's level of ISP pressure. ISP-self efficacy can be improved through extensive training and may help accounting employees relieve some of the ISP pressure. Organizations can monitor the levels of work uncertainty throughout an organization to reduce accounting employee's ISP pressure, which inevitably leads to an ISP violation.

ISP controls are an essential component of an organization's information security management. All organizations endeavor to safeguard and monitor sensitive and financial company data. Information security management is a multifaceted task. Governing accounting employees effectively helps organizations achieve this complex task. This study opens up one new avenue for future researchers to extend the application of the fraud triangle in general dysfunctional behavior and considers ISP pressure as one new type of source of pressure placed upon accountants.

CHAPTER 4

ESSAY 3: EXAMINING ACCOUNTING EMPLOYEES INFORMATION SECURITY POLICY STRESS: INSIGHTS FROM THE JUSTICE AND RESPONSIBILITY RATIONALIZATION

Introduction

A recent wall street journal article suggested that 29% of CEOs discussed having their organization fall victim to information technology (IT) security fraud (Cutter 2018). As information technology brings unprecedented advances in communication for all users, including accounting employees, it also offers greater reach for criminal activities (Hu et al. 2011; Moody et al. 2018; Straub Jr and Nance 1990; Willison and Warkentin 2013). There are a variety of sources of threats to accounting information systems. Some common examples include but are not limited to: unauthorized access that allows for employees to alter, delete, corrupt, destroy, or steal data, failure to maintain backup files, and theft or misuse of computers resulting in damages to the reputation of the organization. To address this IT security threat, organizations have devoted significant resources towards behavioral security measures, such as information security policy (ISP) development and education and training, in addition to continually updating their security technologies (Willison and Warkentin 2013; Willison et al. 2018). However, these IT security response measures fuel already stressed and over-worked employees by

demanding they comply with additional security regulations (D'Arcy and Teh 2019). Therefore, unsurprisingly, despite an organization's best efforts to prevent employee-related IT threats using multiple ISPs, there are a class of employee security-related violation behaviors known as voluntary ISP violations (D'Arcy et al. 2014) (e.g., password sharing, sharing insider information, unauthorized usage) that continue to plague organizations. ISP stress (security-related stress due to ISP requirement) is the critical element on employees' ISP violations (D'Arcy et al. 2014; D'Arcy and Teh 2019); however, there has been a lack of theoretical explanation offered to explain how ISP stress affects ISP violations of accounting employees. In this study, I attempt to provide insight into research that fills this gap.

From a theoretical perspective, the fraud triangle theory is unique to the accounting intentional fraud realm, which can be extended to examine accounting employees' intentional ISP violation behavior. The three factors that make up the fraud triangle are (1) opportunity, (2) pressure, and (3) rationalization. The opportunity arises for intentional fraud when there is an absence of controls, ineffective controls, or the ability to override controls. Work stress or environmental stress may exert pressure or provide an incentive for employees to commit fraud. Rationalization is an attitude or state of mind that allows an individual to make a conscious decision to use to use any means to present fraudulent or misrepresented information for a personal gain (e.g., asset misappropriations, fraud) (Carcello and Hermanson 2008; Murphy and Dacin 2011). Studies in the accounting literature have found that the three dimensions of the fraud triangle are all critical in explaining the likelihood of fraudulent behavior in accounting literature.

Nevertheless, despite this widespread circulation of the fraud triangle theory, it has also been the subject of considerable debate and criticism in recent years on the equal weights of the three elements in different contexts (Free 2015; Murphy and Free 2015). The fraud triangle suggests that the perpetrator has a non-sharable problem that is grounded in pressure, and when aligned with opportunity and rationalization, an otherwise "good" citizen succumbs to committing fraud known as the accidental fraudster (Ramamoorti et al. 2009). On the other hand, a predator is better organized and will have devised more complex concealment schemes. The predator naturally is better prepared to deal with auditors and other oversight mechanisms (Kranacher and Riley 2019; Kranacher and Stern 2004). The predator modifies the functional fraud triangle antecedents: pressure and rationalization are not necessary, and the sole element is the opportunity (Dorminey et al. 2010; Lokanan 2015). Therefore, the relative importance of the three elements of the fraud triangle depends on the context of the violation. In this study, I do not assume the accounting employees are "predators" but "accidental fraudsters" when committing ISP violation. The key elements for accidental fraudsters are pressure and rationalization. Therefore, in this study, I argue that pressure and rationalization will be the two key elements to explain the accountants' ISP violation intention, especially when considering the rationalization as a potential mechanism to explain the effect of pressure on the intentional ISP violation of accounting employees.

Information security literature has suggested the importance of employees' cognitive appraisal of stress and their coping strategies, such as rationalization, on their ISP violation behaviors (D'Arcy et al. 2014). The theoretical foundation for the rationalization construct comes from the moral disengagement theory, which argues that

the crucial precondition for managers to act opportunistically is due to the ability to disengage moral responsibility from their action by self-justifying the action to make it compatible with moral standards (Bandura 1990; Bandura 1999). Accounting researchers have noticed the imperative role of the rationalization element of fraud triangle in the context of accounting behavior research (Chong and Wang 2019; Murphy 2012; Murphy and Dacin 2011; Murphy and Free 2015). For example, concerning rationalizing fraud, Murphy and Dacin (2011) identified the following seven categories of rationalizations as (1) moral justification, by reconstruing an act as being morally worthy, (2) advantageous comparison, by comparing the act to something worse, (3) euphemistic labeling, or using convoluted language to make the act look better than it is, (4) minimize, ignore, or misconstrue the consequences of the act, (5) denial of or blaming the victim, (6) displacing responsibility by blaming someone else, and (7) diffusing responsibility, by blaming everyone else. In my study, I focus on the role of displacing responsibility and diffusing responsibility share the common theme of shifting responsibility to others; previous research conceptualized them together as “responsibility rationalization” (Chong and Wang 2019). Using the responsibility rationalization, I use this justification for unethical behavior (i.e., intentional ISP violations).

In this study, the displacement of responsibility specifically refers to attributing personal responsibility to an authority figure. Individuals use this cognitive mechanism to avoid responsibility by attributing his/her responsibility to an authority figure, such as a manager or superior. The individual can shift the 'feeling' of being 'responsible' or 'accountable' from an autonomous state to an agentic state. This psychological shift results in the individual feeling no responsibility for his or her action because any

unfavorable consequence can transfer back to the authority figure (e.g., My boss told me to do it) (Detert et al. 2008). In the context of this study, accounting employees engaging in the displacement of responsibility may argue they are merely following instructions from their superiors and therefore are not accountable for their decisions regarding ISP violations.

In contrast, diffusion of responsibility refers to attributing personal responsibility to others. This mechanism allows an individual to avoid the responsibility of accepting the unfavorable consequences of behaviors by dispersing blame among his or her peers. Consequently, individuals engaging in such diffusion will have little concern for the consequences of their decision even if it will be harmful to the organization (Mynatt and Sherman 1975). Diffusion of responsibility exists when people believe the harm associated with an undesirable act is attributed to many people. Therefore, it keeps any one person from feeling personally responsible (Bonner et al. 2016). For example, one easy way to diffuse responsibility is to argue that 'everyone does it!' (McKimmie et al. 2003). In the context of my study, 'everyone' refers to other accountants in the organization. Accounting employees engaging in the diffusion of responsibility may feel their obligation is diluted or weakened when their responsibility or blame is perceived to be shared with all other accountants and employees in the organization. Rather than feeling personally responsible, these accounting employees may argue they are not at fault because other accountants can also cause the consequence of intentional ISP violations in the organization.

In order to understand the effect of ISP pressure on accountants and their ISP violation behaviors, I investigate whether or not the ISP pressure will impact accounting

employees' intentional ISP violation behavior through responsibility rationalization. I predict that, when faced with ISP pressure, the ability to rationalize will provide accountants with a legitimate excuse for their wrongdoing or unethical behaviors such as an intentional ISP violation (Bies and Shapiro 1987; Snyder 1985; Wood and Mitchell 1981). To further examine the elements of rationalization, I argue that perceptions of organizational justice will influence rationalization as an important motivational factor to violate trust against the organization (Rae et al. 2008). Therefore, in this study, I further explore how the perceived justice of an organization during an ISP implementation could be an important condition for the employees to choose the target they blame. Perceived justice will provide situation-based influences on individual cognition and behaviors (Rupp et al. 2014). Therefore, accounting employees can further decide how to rationalize the responsibility towards their ISP intentional violations.

Organizational justice research examines various motivators that may lead to employees' perceptions of justice or injustice. Scholars have identified four dimensions of perceived organizational justice – distributive, procedural, informational, and interactional (Colquitt et al. 2001). Previous investigations of negative outcomes of perceived organizational justice have provided theoretical evidence featuring distributive and procedural injustice perceptions as driving motivations for undesirable employee behavior (Colquitt et al. 2001). In contrast, informational and interactional injustice perceptions explain employees' negative behavior after the undesirable action has been taken.

Since the focal phenomenon of this study is intentional ISP violation behavior, I focus only on two types of perceived justice, distributive justice, and procedural justice to

further understand possible antecedents to ISP violation behavior. Distributive justice focuses on whether the allocation of benefits and costs within a group should be proportional to the contributions of group members (Greenberg 1990; Greenberg and Folger 1983). In the context of my study, after organizations enforce their ISPs, the employees will make a judgment on whether the increment in the security of their computer and data is worth the inconvenience or other loss they may suffer from ISP compliance. If the inconvenience (disturbs the work of employees and reduces their work efficiency) that is perceived by the employees is found to be greater than the actual benefits (rewards), then accountants will perceive distributive injustice. This perception will cause employees to blame the organization or managers for unreasonable ISPs, which will result in ISP violations.

In contrast, procedural fairness has been referred to as the judgments about the fairness of the "rules and processes" (Greenberg and Folger 1983) to be objectively designed and applied. In the context of this study, I examine how individual accounting employees will judge whether the ISPs are applied to all accounting employees of the organization. If procedures for detecting and punishing ISP violation behaviors do not appear to be reasonable, then accounting employees may perceive procedural injustice within the organization. This reaction will further cause the accounting employee to use the justification that other employees are not required to follow the ISP for rationalizing their violating behaviors.

In this study, I expect low perceived distributive justice will enable accounting employees to adapt to the displacement responsibility. The displacement will place the blame on the organization or manager who causes their ISP pressure, causing employees

to rationalize their violating behavior further. In contrast, high perceived procedural justice will deprive the employee of adapting the diffusion responsibility therefore unable to blame their colleagues who cause their ISP pressure and further rationalizes their violating behavior. Thus, the second goal of this study is to investigate whether organizational justice will reduce the magnitude of effects from ISP pressure on accounting employees' responsibility rationalization.

I utilize the fraud triangle in this research setting to connect the theory of moral disengagement to the rationalization leg of the triangle. My research design expands on the understanding of rationalization in an individual and how rationalization impacts intentional ISP violation behavior. I also find evidence to explain how the ISP pressure will influence the ISP violation through rationalization.

Based on the analysis of 154 usable responses from professional accountants, I found displacement of responsibility and diffusion of responsibility are two significant types of responsibility rationalization that mediated the relationship between ISP pressure and intentional ISP violation behaviors. The findings verify the conditional effect of organizational justice in reducing the displacement or diffusion of ISP responsibility. These results contribute to prior accounting and ISP literature by (1) extending the responsibility rationalization into the ISP violation behavior; (2) extending the fraud triangle theory by considering the relationship between the pressure element (ISP stress) and the rationalization elements (two types of responsibility rationalization); (3) elaborating the mixed effect between two organizational justice stances and two types of responsibility rationalization on ISP stress, which bridges the connection between the organizational justice and fraud triangle theory. This research addresses several calls to

expand current accounting literature's understanding of the role of rationalizations in accountants' behaviors (Beasley et al. 2009; Bierstaker et al. 2009). My research also provides theoretical groundwork necessary to explore interventions (i.e., procedural justice and organizational justice) that reduce the harmful effects of rationalization on ISP violation behaviors (Wells 2002; Wells 2017).

Theoretical Background and Hypotheses Development

Stress itself is a complex concept that has been operationalized in terms of stimulating conditions (i.e., events impacting on the person) that produce stress reactions (Lazarus and Folkman 1984). Transactional stress models emphasize the cognitive aspects of the stress process wherein stress models view stress as part of a series of dynamic and complex interactions between an individual and the environment. Events must be appraised as stressful before they can influence an individual's psychological well-being (Daniels and Guppy 1997). An individual's stress level rises and falls as a result of assigning meaning to environmental stressors (Everly and Sobelman 1987). Excessive stress intensity manifests in individuals in both physical and psychological ways that lead to stress-related dysfunctional behavior. Conversely, the application of an effective coping strategy will restore an individual to equilibrium.

In IS literature, two types of IT related stresses had been identified, which are techno-stress and security-stress. Researchers have used the term techno-stress to describe the end-user stress caused by accelerating technology demands in the workplace (Ayyagari et al. 2011; Tarafdar et al. 2010; Weil and Rosen 1997). The term ISP security-related stress is used to describe the stressful demands imposed explicitly by security requirements. For example, routinely scheduled security maintenance tasks can

inconveniently disrupt an employee's work schedule. ISP stress is a form of psychological stress. Internal and external security-related demands can cause ISP stress, which can be taxing on one's cognitive resources and abilities. With rapid advances in technology as well as increasing changes in security requirements creates conditions that lead to ISP stress (D'Arcy et al. 2014; Tarafdar et al. 2010). In many cases, the accounting information system technology has been developed faster than advances in control practices and employees' knowledge, skills, awareness, and compliance (Abu-Musa 2006). In fact in practice and academia, accounting and financial publications warn against computer-related data errors, producing false financial statements, violations of internal controls, theft, burglaries, and internal sabotage (Balakrishnan et al. 2019; Gao and Zhang 2019; Hartman et al. 1997; Nickerson 2019).

The primary outcome variable in workplace stress studies has been a measure of employee performance in the accounting literature. In this study's security-related context, this performance measure is intentional ISP violations. An ISP is defined as a statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organization (Bulgurcu et al. 2010). Therefore in my study, an ISP violation is defined as any act by an accounting employee that is against the established ISP of the organization (D'Arcy et al. 2014; Hu et al. 2012). I focus on intentional ISP violations instead of non-intentional violation behaviors. Consistent with existing security compliance research and to a degree driven by the difficulty to obtain actual ISP violation instances, I focus on ISP violation intention rather than actual behavior (Moody et al. 2018; Siponen et al. 2010). Many ISP violations are not readily

observable or objectively measureable; furthermore, organizations are often reluctant to disclose violation behavior to researchers (Guo et al. 2011).

As a first step, I use the fraud triangle, which is a well-known conceptual framework for understanding the drivers of fraud. In this study, I extend the fraud triangle theory to examine the possibility of reducing accounting employees' dysfunctional ISP violation behavior (Albrecht et al. 1995; Morales et al. 2014). In Cressey's (1953) seminal work, he identifies three conditions that must be present for fraud to occur: opportunity, motivation, and rationalization. Opportunity is the perception that the fraud may be perpetrated undetected. Motivation reflects the pressure or need to benefit from fraud. Rationalization is the justification of the fraud in a way that mitigates any inconsistency between the action and expectations of the behavior. Professional standards encourage auditors to frame their risk assessments using the fraud triangle (i.e., SAS 99/AU Sec 316, AICPA 2002).

Prior research encourages the use of the fraud triangle as a basis for making risk assessments and identifies the importance of all three of its dimensions in influencing an individual's propensity to commit fraud (Bell and Carcello 2000; Murphy 2012; Peecher 1996; Rezaee 2005). While fraud is wrongful criminal intentional deception for personal gain involving a violation of trust (Ramamoorti 2008; Ramamoorti and Olsen 2007), dysfunctional behaviors occur when individuals knowingly make a choice that puts their interests before that of the organization (Cohen et al. 2007). When accounting employees engage in dysfunctional behavior this increases the risk of financial and reputational harm to an organization. Rationalization requires a clear development of self-interest beyond economic factors to include the preservation of one's moral self-identity. The

psychological justification allows individuals to excuse dysfunctional behaviors (Frank 1988). More specifically, rationalization includes a definition of ethical behavior or explanation of how an ethical person can perform a particular behavior (i.e. intentional ISP violations). Rationalization incorporates the justification of how a particular behavior can be defended as ethical before, during, or after its enactment. Even if emotions serve to keep individuals honest, many individuals experience cognitive dissonance reduction when choosing to partake in misreporting behavior (Chong and Monroe 2015; Chong and Wang 2019; Frank 1988; Murphy and Dacin 2011; Sykes and Matza 1957). Consistent with previous research, I present rationalization as a mechanism of coping strategy.

Literature has shown that when faced with stress/pressure, an individual will engage in some effective coping strategy to restore physical and psychological balance (Lazarus and Folkman 1984; Rodell and Judge 2009; Sutherland and Cooper 2000). In this study, when accounting employees face more ISP stress due to more ISP requirements, they will deploy more responsibility rationalization as a coping strategy to disengage themselves from the responsibility of violations. I consider both the displacement of responsibility and the diffusion of responsibility. Displacement of responsibility refers to attributing personal responsibility to an authority figure. This cognitive mechanism allows an individual to avoid responsibility by attributing his/her own responsibility for their action onto others, such as senior team members or managers. By doing this, the individual can shift the feeling of being responsible or accountable from an autonomous state to an agentic state (Bandura et al. 1996). The diffusion of responsibility refers to attributing personal responsibility to others. This mechanism allows an individual to avoid the responsibility of accepting the unfavorable

consequences of behaviors by dispersing blame among his/her peers (Bandura et al. 1996). Individuals engaging in the diffusion of responsibility rationalization will not be deterred by the consequences of their decisions (Mynatt and Sherman 1975).

Putting these rationalization types in the context of my study, I argue accounting personnel have the reputation of facing a high-pressure job (Collins and Killough 1992; Gaertner and Ruhe 1981) and their job performance is highly dependent on the extent to which they complete their assigned work. Because of this, they have limited personal resources and mental energy to comply with extra overloaded ISP requirements. Therefore, high ISP pressure will quickly force the employees to conclude they are violating the ISP to make sure they can finish their own assigned work required by the supervisor in time. This reasoning will further lead them to attribute responsibility for violations to the organizations or managers because the supervisor or organization has deployed an unreasonable workload on them. This justification becomes the displacement of responsibility to cope with the ISP pressure. Perceptions of high ISP pressure given by the organization will also motivate collective violation behavior (Greenberg and Folger 1983; Willison et al. 2018). In other words, if accounting employees perceive high levels of ISP stress, the more likely they will infer that other accounting employees will also conduct intentional ISP violations. This implication will further lead them to attribute their responsibility to other employees. This justification becomes the diffusion responsibility for coping with ISP stress. Per the arguments presented above, I present the following hypotheses:

H1: *Information Security Policy (ISP) pressure will be significantly associated with two forms of responsibility rationalization, specifically:*

H1a: *ISP pressure will be positively associated with the displacement of responsibility.*

H1b: *ISP pressure will be positively associated with the diffusion of responsibility.*

Individuals use generally accepted moral standards to self-regulate their behavior. Moral disengagement theory offers a theoretical lens to examine the psychological cost (i.e. self-condemnation) when violating these moral standards (Bandura 1990; Bandura 1999; Bandura et al. 1996). However, individuals may still engage in behavior that violates the moral standards since individuals will be able to disengage themselves. Specifically, this psychological self-regulatory mechanism does not function unless it is activated. Individuals can choose to deactivate their self-regulatory mechanisms by rationalizing their behavior to defend their deviation from morally acceptable behavior (Abelson et al. 1968; Bandura 1999; Shu et al. 2009). In other words, people do not ordinarily engage in undesirable employee conduct unless they have justified the morality of their actions. Moral disengagement theory helps explain part of the perplexing observation that most individuals perceive themselves as moral but unethical behavior (e.g. tax evasion, asset misappropriation) commonly occurs (Bersoff 1999; Clotfelter 1983; Steele 1988).

The moral disengagement process is theorized to play a critical role in explaining how humans can engage in corporate misconduct without apparent cognitive distress (Brief et al. 2001; Moore 2008). The displacement and diffusion of responsibility mechanisms allow the employee to obscure their moral standards. Displacement of responsibility refers to how individuals may designate responsibility to authority figures

who may have indirectly condoned or deliberately engaged in their behavior (Kelman and Hamilton 1989; Sykes and Matza 1957). The diffusion of responsibility works similarly but refers to dispersing responsibility for one's actions across members of an organization rather than just a single authoritative figure (Vaughan 1996).

Therefore, I argue that accounting employees with lower responsibility rationalization will generally be less likely to intentionally violate ISPs than individuals with higher responsibility rationalization. This is because the former are less able to rationalize the feeling of being personally accountable for the potentially harmful effects of their ISP violation. Accounting employees with lower responsibility rationalization will all be less able to neutralize their feelings of discomfort when intentionally violating an ISP.

However, these individuals should not be assumed to never engage in unethical behavior (i.e. ISP violations) Research suggests that individuals will weigh the benefits of their gains against the mental costs of choosing to engage in unethical behavior (Luft 1997). The psychological costs are influenced by their personal feelings of guilt, discomfort, or the consequences of lying (Gneezy 2005; Mayhew and Murphy 2014; Murphy 2012). If individuals believe that the benefits gained from unethical conduct outweigh the personal costs, then they are more likely to engage in unethical behavior (i.e. ISP violations).

Rationalization is the process an individual undergoes to characterize an act in a way that allows them to preserve their ethical persona. Individuals tend to regard themselves as virtuous people and attempt not to engage in behaviors that may conflict with this self-concept (Ramamoorti 2008). Individuals usually prefer to believe they are

rule-abiding and will self-govern their behaviors to continue to maintain a positive view of themselves (Aronson 1999; Bosse and Phillips 2016). Rationalization enables individuals to behave in ways that might otherwise be considered unethical and cognitively justify their behavior (Elliot and Devine 1994; Ramamoorti 2008).

Based upon the above discussion, I propose the following hypotheses：

H2: Two types of responsibility rationalizations processes will be significantly associated with intentional ISP violation intention, specifically:

H2a: Displacement of responsibility will be positively related to the intentional ISP violation intention.

H2b: Diffusion of responsibility will be positively related to the intentional ISP violation intention.

People's perception of truth and fairness depends on whether it is clear to them and others what is true or false, fair or unfair. Accounting information systems within organizations can reinforce or dissipate the perception of fairness. There is considerable evidence that employees' perception of fairness will play an important role when making business-related decisions (Colquitt et al. 2003). Fairness perceptions drive both consumer and producer behaviors (Kahneman et al. 1986; Piron and Fernandez 1995). However, employees are hesitant to engage in corporate misconduct (i.e. theft) if they perceive they are harming individual managers (Greenberg 2002). Therefore if management accounting researchers ignored considerations of fairness within organizations there would be an incomplete description of management accounting-related behavior (Luft 1997).

Managerial control systems literature implicitly recognizes that monetary rewards will not be the singular motivation for employees to work in the organization's best interest. Research has examined the use of culture controls, codes of conduct, screening for quality personnel, and "tone at the top" as supplements to govern accounting employees' organizational behavior (Davis and Militello 1994; Merchant and Otley 2006; Simons 1994). Furthermore, perceptions of fairness must be heavily considered as the outcome may affect financial reporting judgments (Evans III et al. 2001; Libby 2001). Individual perceptions of organizational justice can influence co-workers, superiors, and the compliance towards policies of the organization (Colquitt et al. 2001; Leventhal et al. 1980; Li et al. 2014; Willison et al. 2018). In my study, I argue that organizations need to examine perceptions of fairness within an organization as a possible motivator of unwanted ISP violations.

Organizational justice refers to perceptions of organizational fairness. These perceptions manifest in four specific ways; distributive, procedural, interactional, and informational (Colquitt et al. 2001; Greenberg 1987). Interactional justice is the perceived fairness of the treatment received in the explanation of formal procedures (Bies and Shapiro 1987). In other words, interactional justice reflects employees' feelings of how fairly managers treat them. Informational justice refers to fairness in the communication process of formal company procedures (Colquitt et al. 2001). For example, an employee's perception of the candidness of a supervisor's communication would reflect informational justice. Distributive justice refers to the perceived fairness of outcomes (Colquitt et al. 2003). Procedural justice is the perceived fairness of the process (e.g., policies and procedures and their enactments) of determining outcomes or resource

distributions (Colquitt et al. 2001). In this study, formal procedure refers to a company's rules, regulations, or policies that precisely guide an organization's information security management.

In my study, I focus on distributive and procedural justice rather than informational and interactional justice since research has shown greater distributive and procedural fairness is assumed to coincide with greater organizational justice (Lee 2001). Distributive justice is conceptualized as the perceived fairness of the ISP required by the managers of the organization. Employees are concerned about the fairness of outcomes in terms of whether complying with organizational ISP will result in higher rewards in proportion to costs they expend when following ISPs (Adams 1965; Leventhal et al. 1980; Willison et al. 2018). Procedural justice represents the perceived fairness of the process used to arrive at outcomes, which is conceptualized as the perceived fairness of ISP requirements allocated among the employees within one organization. Employees judge the fairness of processes used to determine outcomes in terms of whether ISPs are consistent, unbiased, accurate, and ethical (Leventhal et al. 1980; Thibaut and Walker 1975).

Attribution theory states that individuals will search for causes of specific outcomes and attribute causes to behavior in order to maintain their own positive self-image (Weiner 1985). In this study, the ISP pressure can be considered an outcome of an employee's work circumstances. Accounting employees will then make a fairness judgment in order to assess who and what caused this intentional ISP violation outcome (Folger and Cropanzano 1998). Specifically, accounting employees will assess whether the organization or other employees are accountable for their current work situation.

In this study, I argue when low distributive justice is perceived, it means the ISP distributed by the organizations or managers is unreasonable. When accounting employees perceive low distributive justice, this perception will enable accounting employees to blame their managers or organization (i.e., displacement of responsibility mechanism). On the other hand, when accounting employees perceive a higher distributive justice it will decrease the effect of ISP pressure faced by the employee. Accounting employees will be less likely to engage in the process of displacement responsibility.

In the context of my study when low procedural justice is perceived, it means that some employees who violated an ISP did not receive the punishment outlined by the organization. This perception will allow employees to rationalize their violating behavior easily. Therefore, the lower the procedural justice in an organization will increase the effect of the ISP pressure faced by the employees easily allowing accounting employees to engage in a diffusion of responsibility.

Prior research shows other corporate misconduct (i.e., embezzlement, financial misreporting) is rationalized by employees as appropriate behavior when employees feel the employer is not considered fair (Greenberg 1990; Greenberg 2002; Murphy 2012). Rather than deterring others from committing unethical acts, employees who feel mistreated will more likely conduct similar undesirable acts to correct their perceptions of inequity (Hollinger and Clark 1983). The perception of fairness of authorities and co-workers has been an essential factor when examining accounting employees' behavior (Zhang 2008). Therefore, based on the discussion above, I propose the following hypotheses:

H3a: Perceived distributive justice will negatively moderate the effect of ISP pressure on the displacement of responsibility.

H3b: Perceived procedural justice will negatively moderate the effect of ISP pressure on the diffusion of responsibility.

The resulting research model is illustrated in Figure 4-1.

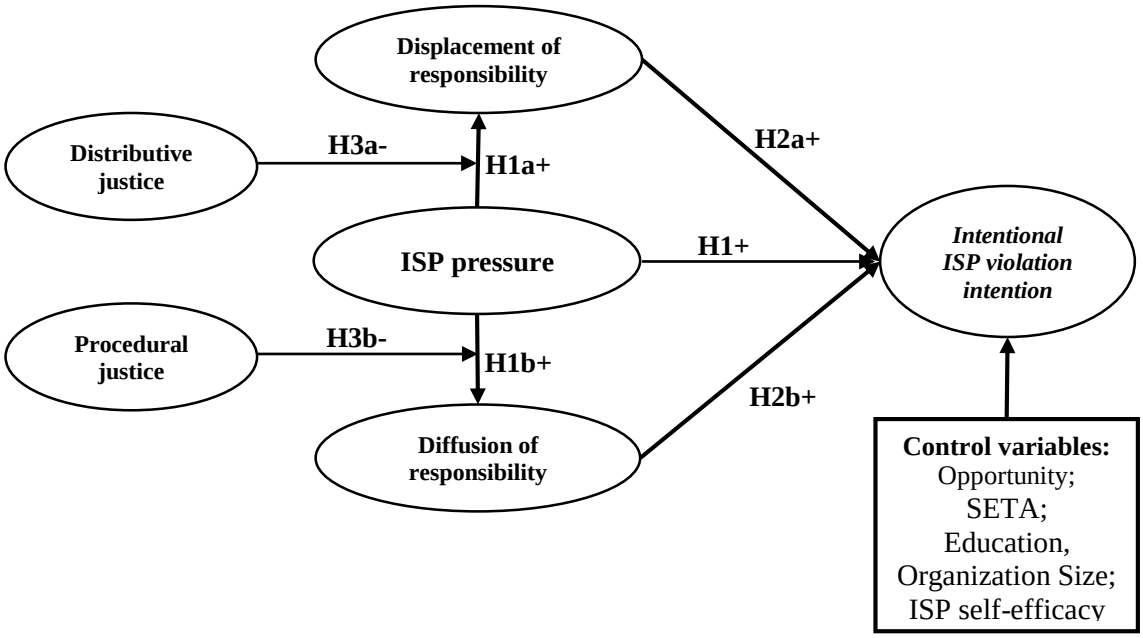


Figure 4-1: Research Model

Methodology

Measurement

The measurement items in my questionnaire were adapted from existing validated and well-tested scales in the extant literature. In addition to using previously validated questions, all measures were pretested by two business professors with expertise in survey research and ten professionals with ISP experience. The objective of the pretest was to ensure that the measures were meaningful and that they unambiguously captured

the domain of each construct. Based on detailed interviews with each professional pretester, appropriate changes were made to the measures.

All measures were pilot tested in a survey with a small portion of targeted samples, which only resulted in minor wording changes. I conducted a reliability analysis and exploratory factor analysis for each set of measures. The validity and reliability of the adapted measures fulfilled the basic requirements, which indicated all measures were clear to the targeted samples, relevant and captured the intended concepts. The data used in this study were collected from a sample of full-time professional accountants working in U.S. organizations.

The results placed sufficient confidence in the measures to proceed with the survey administration of the target sample frame. In the questionnaire, all items were measured with 5-point Likert scales, ranging from "strongly disagree" to "strongly agree." All scales used in the study are presented in Table 4-1.

In this study, the dependent variable is the respondent's self-reported intention to conduct intentional but non-malicious ISP violations. To distinguish it from the malicious ISP violations, I adopted the work of Willison and Warkentin (2013) to list "not changing password regularly," "delayed backup," and "bring materials back home" as three specific examples of intentional but not malicious ISP violations for respondents to accurately evaluate their intention. In particular, the survey emphasized "not malicious" in each statement. In addition, to avoid the social desirability bias, there was no use of the "first-person perspective" but "third-person perspective" for each statement to measure the ISP violating intention.

Table 4-1

Constructs in the Research Model

General Concept	Construct	Operational Definition	Reference
Pressure	Information Security Policy Stress	Stressful demands specifically imposed by information security policy requirements. A form of psychological stress caused by internal or external information security-related demands taxing one's cognitive resources or abilities.	(D'Arcy et al. 2014; Lazarus and Folkman 1984)
Rationalization	Diffusion of Responsibility	Attributing personal responsibility to others. The sense of responsibility towards information security policies of an organization to be diminished by divisions of labor. (Ex: When everyone is responsible for ISP requirements, nobody is)	(Bandura 1990; Bandura 1999)
	Displacement of Responsibility	Attributing personal responsibility to an authority figure, therefore accounting employees are not personally responsible for their actions regarding ISP's.	(Bandura 1990; Bandura 1999)
Organizational Justice	Distributive Justice	Employee's viewing ISP procedures as fair by determining the ratio of one's input (e.g. time) to one's outcome as equal.	(Adams 1965; Colquitt et al. 2001)
	Procedural Justice	ISP procedures should be a) applied consistently b) free from bias, c) accurately applied and used in decision making	(Colquitt et al. 2001; Leventhal et al. 1980)
Fraud Behavior (Violation of Trust)	Intentional ISP violation intention	An ISP violation is any act by an employee that is against the established ISP of the organization (e.g. not changing passwords, delayed backup, unencrypted USB)	(D'Arcy et al. 2014; Hu et al. 2011)

The response options ranged on a fully anchored scale from one to five, in which five served as ‘strongly agree’ with the statement that the respondent would engage in actions similar to those of the hypothetical employee in the scenario under circumstances that represented various levels of the antecedent variables.

For the ISP pressure, I used three items focusing on the general pressure the respondents perceived in their organization, which are adapted from the work of D’Arcy, Herath, and Shoss (2014). For two responsibility rationalization, I adapted the scale in Chong and Wang (2019) in the ISP violation context, and displacement of responsibility focuses on blaming on supervisor or organization and diffusion of responsibility focuses on blaming on other employees, each of them respectively measured by three items. To evaluate two kinds of organizational justice, I required the respondents to report their perception of the “organization distributive justice” and “organization procedural justice.” The perceived organization distributive justice aims to evaluate whether the respondents perceive the advantage of complying with ISP will exceed the convenience brought by it, measured by three items adapted from the work of Burney et al. (2009). The perceived organization procedural justice is also measured by three items adapted from Burney et al. (2009) to evaluate whether the ISP is applied in a fair manner to everyone in the respondents’ organization.

To control the potential alternative explanation on the hypothesized relationship, I consider the heterogeneity from the individual level and organizational level. First, I consider the ISP training (SETA), education, and the ISP self-efficacy of the accountants as three important individual characteristics to be controlled. In addition, I consider the organizational size (number of employees within the organization of the respondent) as

one important organizational characteristic to control. In particular, based on the fraud triangle theory, the ISP opportunity will be another important factor to influence the ISP violation intention. Therefore, I also include it as the control variable in this study. In the questionnaire, all items are measured with 5-point Likert scales, ranging from "strongly disagree" to "strongly agree."

Data Collection

I used a market research firm to invite participants to take my survey. External panelists have been used increasingly in behavioral IS research (Ayyagari et al. 2011; Bulgurcu et al. 2010) and have certain advantages over traditional methods that are key to my study. First, panels guarantee respondent anonymity. Therefore, it encourages honest responses to questions that may normally be subject to social desirability. Second, external panels contain respondents from a wide range of industries and positions. I instructed the marketing research firm to collect responses from employed computer-using accountant professionals. Respondents were paid $10 each for participating in the study. In the questionnaire, the targeted participant was first asked to indicate their computer experience in the company. If the targeted participant had not used a computer in the company, that person was excluded from further consideration. The questionnaire then asked the respondents to measure their perceptions of each research construct.

A total of 574-panel members accepted the invitation to participate in the survey by viewing the consent agreement and clicking past the first page. After excluding incomplete responses, I used a data set of 154 responses in all analyses. Table 4-2 shows additional demographics for these respondents. All employees sampled must use a computer to complete their daily work tasks.

Sample demographics reveal that 62 percent were female and tended to be well-educated (73 percent with at least a bachelor's degree).

Table 4-2

Sample Demographics

Respondents' Gender	**Percentage**	**Respondents' education**	**Percentage**	**Length of Employment at Organization**	**Percentage**
Male	42.2%	High school	15.6%	<1 Year	0.6%
Female	57.8%	2 Year Degree	11.0%	1-5 Years	29.2%
ISO certification	**Percentage**	4 Year Degree	48.7%	5-10 Years	31.8%
Yes	41.6%	Professional Degree	23.4%	10-15 Years	11.7%
No	58.4%	Doctorate	1.3%	>15 Years	26.6%

Data Analysis and Results

Following the recommendations of Lowry and Gaskin (2014), there are reasons for me to use Partial Least Squares (PLS) for building and testing my research model. First, PLS-Structural Equation Modeling (SEM) is a "silver bullet" in my research situation when models are relatively complex and representative sets of data are rather small (Ringle et al. 2012). By using PLS estimation, the variance observed in the dependent variable can be maximized, which conform to my intention to identify the explanatory power of fraud triangle on the intentional violation behavior and further compare the relative importance of the three factor of fraud triangle. Therefore, in this study, I used SmartPLS (version 2.0) as the primary statistical tool to analyze the measurement and structural models.

Results of Measurement Model

The measurement model was tested by assessing both the convergent and discriminant validity. I assessed measurement validity in three ways. First, I assessed convergent validity, which is how each item was related to its corresponding construct by examining the factor loadings. Convergent validity is considered satisfactory if the factor loading of a measure is 0.7 or higher. All factor loadings were above the cutoff point of 0.70 with a t-value higher than 1.96. The measures loaded on their appropriate factors and there was no evidence of significant cross-loading. Average variance extracted (AVE) was also examined to evaluate convergent validity. AVE is greater than 0.5, establishing convergent validity. As presented in Table 4-2, each construct has an AVE greater than 0.5, suggesting that my measures exhibited adequate convergent validity.

Second, the reliability of the measures was examined through two criteria, Cronbach's alpha (C.A.) and composite reliability (C.R.). The CA and C.R. of construct was greater than 0.7, a common threshold for signifying satisfactory construct reliability. According to my results, the minimum C.A. and C.R. values exceed the recommended threshold of 0.7, indicating acceptable reliability of the measures.

Third, discriminant validity is verified by the difference between the AVE of a construct and its correlation with other constructs. For adequate discriminant validity, the square roots of AVE of any construct should be greater than the correlations between the construct and other construct, which means the diagonal elements should be greater than corresponding off-diagonal ones. (Fornell and Larcker 1981). As presented in Table 4-3, the criterion for discriminant validity was also met in this study.

Table 4-3

Descriptive Statistics, Correlations and Reliability

Construct	***Mean(SD)***	***1***	***2***	***3***	***4***	***5***	***6***
ISP pressure	2.35(0.94)	**0.875**					
Displacement of Responsibility	*2.11(0.96)*	*0.39***	**0.890**				
Diffusion of Responsibility	*2.26(1.06)*	*0.29***	*0.32***	**0.931**			
Distributive justice	*3.33(0.88)*	*0.18**	*-0.16***	*-0.11*	**0.891**		
Procedural justice	*3.42(0.92)*	*-0.17**	*-0.38***	*-0.31***	*0.07*	**0.846**	
Intentional ISP violation intention	*2.96(1.00)*	*0.22***	*0.36***	*0.34***	*-0.04*	*-0.42***	**0.891**

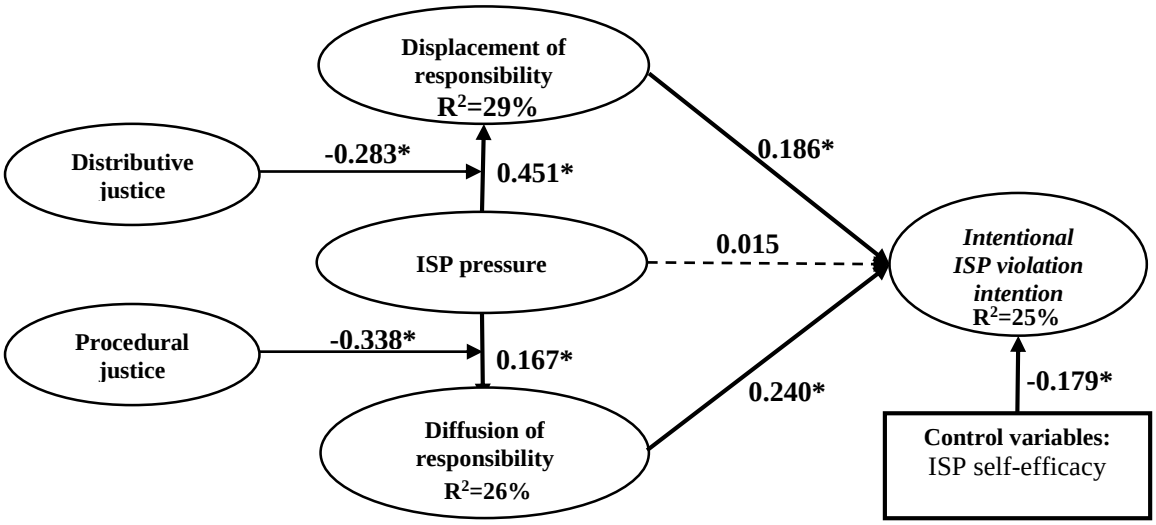
Note: * p < 0.05; ** p < 0.01; Diagonal elements (in bold) are the square root of the AVE; The off-diagonal elements are the correlations among the constructs;

Common method variance (CMV) may have confounding effects on the observed relationships between the predictors and criterion variables (Podsakoff et al. 2003). Although the data was collected in two different phases within a two-week span for independent and dependent variables, data were all rated by employees, thereby the potential CMV might not be removed completely. To further assess the potential effects of common method bias, I conducted Harman's single factor test and results showed all of the items of each constructs in my research model cannot be loaded in a single factor in an EFA. In particular, I found no high correlation between the same marker variables in time 1 and time 2. The marker variables have low and insignificant correlations with all the studied constructs, while the partial correlations between the key constructs were high and significant. Both Harman's single factor test and marker variables test make me confident that my data results will not be threatened by the common method bias.

Results of Structural Model

The structural model for testing the hypotheses is also examined through Smart PLS 2.0. I followed the steps proposed by Aiken et al. (1991) to examine the moderation hypotheses. The interaction terms were mean-centered prior to creating the interaction variables in order to reduce the potential for collinearity (Chin et al. 2003). Bootstrapping (1000 resamples) was used to determine the significance of the path coefficients. Results for the structural model are presented in Figure 4-2. The model explains 25% of the variance of intentional ISP violation intention. As shown in Figure 4-2, the ISP pressure will significantly improve the displacement of responsibility ($\beta = 0.451$, $p < 0.05$; H1a is supported), at the same time, the ISP pressure will also result in the diffusion of responsibility ($\beta = 0.167$, $p < 0.05$; H1b is supported).

Further, the two responsibility rationalizations will both significantly increase the intentional ISP violation intention (displacement of responsibility: $\beta = 0.186$, $p < 0.05$; diffusion of responsibility: $\beta = 0.240$, $p < 0.05$). H2a and H2b are both supported. Finally, the perceived distributive justice will negatively moderate the effectiveness of ISP pressure on the displacement of responsibility ($\beta = -0.283$, $p < 0.05$). In addition, the moderating effect of perceived procedural justice on the relationship between ISP pressure and diffusion of responsibility is also significant ($\beta = -0.338$, $p < 0.05$).



Notes: Paths in dash are not significant ($p > 0.05$). Nonsignificant control variables are not shown. * $p < 0.05$.

Figure 4-2: Structural Model Results

To further depict the moderating effect of two perceived organization justice constructs, the PROCESS marco for SPSS was used to make 2-way interaction plots, which are shown in Figure 4-3. The high and low lines in the interaction plot represent ±1 standard deviations from the mean value of distributive justice and procedural justice. Only when procedural justice is low (Mean minus one SD) or middle, ISP pressure will significantly result in diffusion of responsibility (Low: $\beta=0.502$, $p<0.01$, SE=0.09, LLCI=0.318, and ULCI=0.686; Middle: $\beta=0.172$, $p<0.01$, SE=0.07, LLCI=0.027, and ULCI=0.317). When there is high procedural justice, the effect of ISP pressure isn't significant anymore (High: $\beta=-0.157$, $p>0.05$, SE=0.11, LLCI=-0.384, and ULCI=0.070), seen in Figure 4-3a. Similarly, for the distributive justice, the results show that, only when distributive justice is low (Mean minus one S.D.) or middle, ISP pressure will significantly result in displacement of responsibility (Low: $\beta=0.704$, $p<0.01$, SE=0.11, LLCI=0.494, and ULCI=0.914; Middle: $\beta=0.442$, $p<0.01$, SE=0.07, LLCI=0.300, and

ULCI=0.584). When there is high distributive justice, the effect of ISP pressure isn't significant anymore (High: β=0.179, p>0.05, SE=0.10, LLCI=-0.017, and ULCI=0.376), seen in Figure 4-3b.

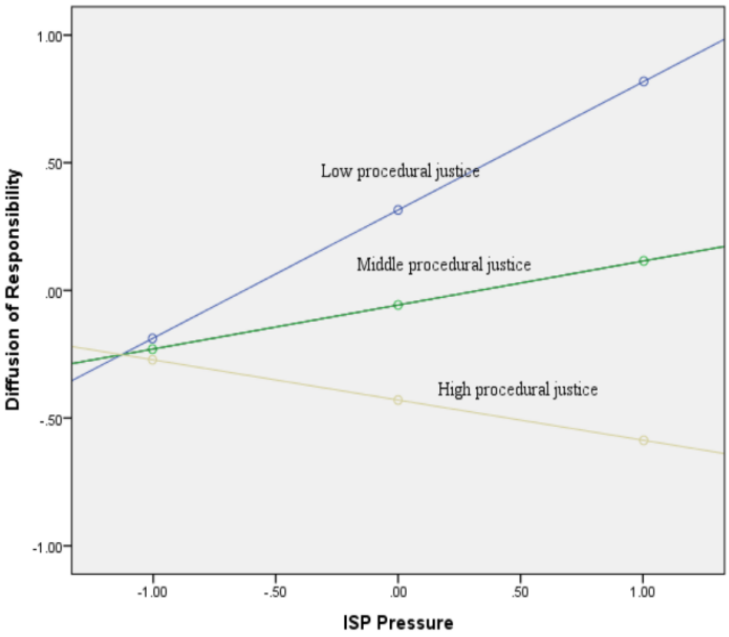


Figure 4-3a

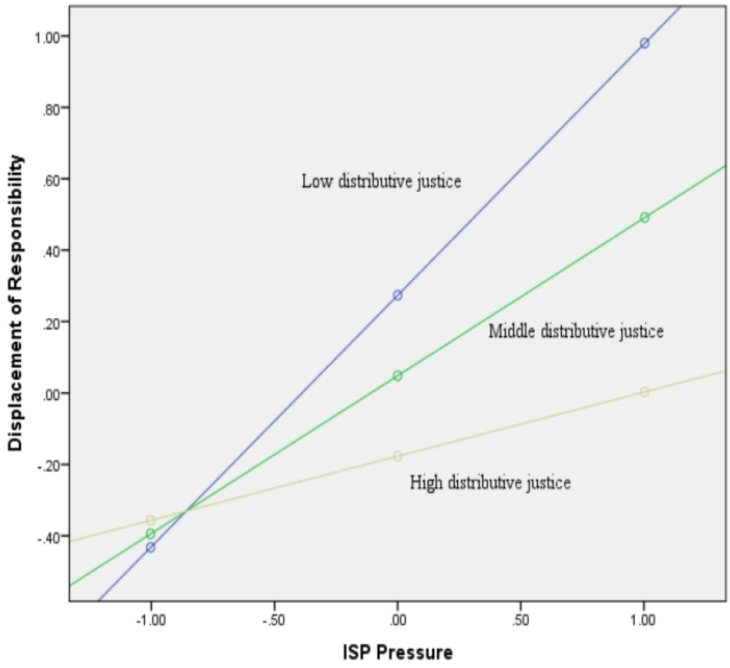


Figure 4-3b

Figure 4-3. Interaction Diagrams

Discussion and Contributions for Theory

By connecting the theory of moral disengagement to the rationalization leg of the fraud triangle, this study uses the responsibility rationalization to provide an explanation as to how ISP pressure results in the accounting employees' intentional ISP violations. Based upon a survey from 154 accounting employees, the results indicated the two types of responsibility rationalization both significantly increase the intentional ISP violation intention. Consistent with Bandura's theory of moral disengagement, when accountants use displacement of responsibility as well as diffusion of responsibility to rationalize their actions this will fully mediate the relationship between accounts' ISP pressure to their ISP violations. Furthermore, the hypothesized moderating effect of the types of perceived justice in an organization and the relationship between ISP pressure and rationalizations are negatively related to the possibility of an intentional ISP violation. That is, as accountants view their organization to have a sense of "fairness" in their ISP governing policies it plays an important role in deterring unwanted ISP violation behavior.

This study contributes to the literature in the following ways. First, this study contributes to the accounting stress literature by adding knowledge of a new type of ISP stress. Accounting studies on work-related stress have traditionally emphasized the organizational stressors such as boundary spanning and perceived environmental uncertainty, overload, role conflict, and role ambiguity (Collins and Killough 1992; Jones III et al. 2010; Viator 2001) as well as the consequences of those stressors such as job satisfaction, performance, and turnover intention (Collins 1993; Collins and Killough 1992; Fogarty et al. 2000; Gaertner and Ruhe 1981; Rodell and Judge 2009; Smith et al. 2010). This study examines a unique stress and the resulting consequences faced by

today's accountants– ISP requirement and intentional ISP violation behavior, which extends the sources of pressure influencing accounting employees and confirms current accounting literature that emphasizes that stress has a general negative effect on employees' well-being or performance. Additionally, this study contributes the first empirical evidence of this new kind of work-related stress (ISP stress) in the accounting stress literature. This study opens a new research avenue on ISP stress; ISP stress is becoming a dominant management control issue for accounting information security.

Second, this study contributes to fraud triangle framework by tentatively using the rationalization element as a coping mechanism to explain how the pressure element (the ISP pressure in this study) could result in dysfunctional behavior (ISP violations in this study). Prior studies on fraud triangle application mainly consider the individual influence or alignment of three elements of fraud triangle on the fraud or other dysfunctional behavior (Dorminey et al. 2012; Fiolleau et al. 2018), however this study shows that ISP pressure is a stimulation that could motivate the accounting employees to conduct responsibility rationalization as a coping mechanism to disengage their moral responsibility for their intentional ISP violation behaviors. This result expands the understanding of fraud triangle theory application. Future researchers are encouraged to conduct more research on the relationship among the three elements of the fraud triangle with this unique avenue of ISP violations.

Finally, this study contributes to the accounting rationalization literature by identifying the role of organizational justice on the responsibility rationalization mechanism choice and effectiveness. Multiple different rationalization mechanisms based on moral disengagement theory (Bandura 1999) and cognitive dissonance theory

(Festinger 1962) have been identified (e.g. seven categories of rationalizations of (Murphy 2012; Murphy and Dacin 2011) and entitlement (Mayhew and Murphy 2014)).

Previous research has proposed that perceptions of organizational justice are linked with an individual's rationalization and motivation to commit fraud (Rae et al. 2008). However, there is still a lack of in-depth understanding of how organizational justice can influence the rationalization process. In this study, I empirically test that not only will organizational justice climate influence the rationalization of accounting employees but also a displacement of responsibility will be more related to distributive justice while procedural justice will provide more explanation of the diffusion of responsibility. Therefore, I suggest when future studies incorporate rationalization in their research models, they may need to consider specific types of rationalization mechanisms.

Practical Implications

The results of this study provide important implications for further understanding the ISP violation phenomenon. First, this study finds supporting evidence that accountants do need ISP requirements especially with the increasing need of more technological skills in auditing techniques and accounting information systems for organizations. However, these ISP requirements should not be set so that they cause more stress due to security requirements. In such a case, accountants might be likely to rationalize these ISP violations through moral disengagement techniques, which will result in organizations that are more vulnerable to violating behavior. Therefore, accounting managers need to engage in efforts to detect and counter these types of ISP pressure. Organizations can specifically avoid excessive technical jargon and legal terms when instructing accountants to follow the ISPs. Accounting managers should carefully

consider the nature of accountants and their need to work remotely and apply security policies that will increase accountant's efficiency and effectiveness. Even if the accounting profession calls for more technological skills, accounting managers must include security education training awareness programs to describe the current regulatory security policy as well as upcoming security changes.

Second, organizations must examine their organizational justice climate towards security. Accounting employees must view their security policies are fairly and equally distributed, otherwise they are likely to consider "responsibility" disengagement, which leads to ISP violation behaviors. Accounting managers can benefit from incorporating positive, ethical norms into accounting control systems (Merchant and Van der Stede 2007; Noreen 1988). This study highlights the incremental benefit for promoting "fair" ISPs for organizations. This helps eliminate the moral buffer that accountants may use to self-justify their misbehavior.

Limitations and Future Research

There are possible limitations to this study. First, this study does not consider accountants' individual backgrounds, professional certifications for information systems, political backgrounds, level within an organization, and cultural differences. These personal factors might also affect individuals' risk propensity and capabilities. Future research should examine the types of role conflict experienced by accounting employees with all the regulatory security changes in organizations. Second, this study only examines general ISP violation intentions, and these could change as specific instances are applied. Therefore, in essence this is a self-reported intention behavior. However, since respondents were reassured of anonymity and no personally identifiable data were

collected, I believe these responses are an accurate display of intention. Future research may examine specific instances of ISP violations that occur in accounting firms that require more sophisticated technical skills (i.e. security data breaches, malicious insider behavior). Although this study intentionally chose this route, accounting literature could benefit from future research of instances that lead to computer fraud or financial statement manipulations.

Conclusion

When accountants were overwhelmed by ISP requirements it created a new ISP pressure that resulted in accountants intentionally violating ISPs. In this study, I used the rationalization element of the fraud triangle as one coping mechanism to ISP pressure. This coping mechanism allowed accountants to disengage their responsibility when committing ISP violations. I found that two responsibility rationalizations did mediate the effect of ISP pressure on the ISP violations. I also identified perceptions of organizational distributive justice that could effectively reduce the displacement of responsibility while procedural justice was able to effectively reduce the diffusion of responsibility. My research findings provide important implications for causes of accounting stress and expanding on an accountant's rationalization process. It is evident accounting managers should carefully consider the balance of benefits of enforcing ISPs to prevent specific IT threats and the ISP stress risks from overwhelming ISP requirements.

Information security management controls are an important component of an organization's internal control structure. Safeguarding and monitoring a company's sensitive data are essential aspects of IT controls. Information security management is a multifaceted task, and part of governing accountants effectively is understanding what

causes accountants to avoid ISP compliance. The results of this research not only provide a description of possible motivations for deviation from current ISPs but also suggest how future research can build on current findings to develop strategies to aid in implementing ISPS.

CHAPTER 5

DISCUSSION AND CONCLUSION

This chapter first summarizes the findings of the three essays of this dissertation. Second, I describe the limitations of the essays. Finally, the chapter concludes with directions for future research.

Essay 1: Using the Fraud Triangle to Explore Motivations for Employees' Copying Company Data

The study finds evidence to explain the possible cause and motivation for why employees willfully violate the specific ISP of copying company data to bring their work home. Using the fraud triangle as a broad framework, I examine how the components of opportunity, rationalization, and pressure will influence an employee and their intention to copy company data. The findings revealed that this intentional ISP violation is driven highly by an employee's desire to complete their assigned workload. Therefore, before organizations continue to create ISPs, they should examine the overwhelming work pressure employees may already face with their current workload.

Essay 2: The Impact of Information Security Policy Controls on Accounting Employees' Information Security Policy Violation Behavior

The accounting profession is known to be a high-pressure job and is subject to many sources of stress (e.g., work-life balance, dead-lines). Though information security management controls have the potential to protect organizations from harmful incidents (e.g., security-related data breaches), ISPs can hinder the productivity of accounting employees. I examine the levels of organizational ISP controls and how it will reduce the elements of the fraud triangle in order to prevent intentional ISP violations. The results revealed ISP controls do indeed reduce opportunities to commit violations, but they also increase ISP related stress. These findings can lead future research to explore avenues that may further explain why even with reliable ISP controls, intentional ISP violations are still occurring within an organization.

Essay 3: Examining Accounting Employees Information Security Policy Stress and Their Violation Intentions: Insights from the Coping Perspective

Organizational justice theory expands on the notion that individuals make business-related decisions whether or not they perceive their environment as fair or unfair. Building upon this theory, I examine how accounting employees will decide to violate ISPs if they feel they are not being treated fairly in regard to an organization's ISPs. One of the points of the fraud triangle is rationalization. In this study, I expand on the specific responsibility rationalization aspect an accountant undergoes when committing ISP violations. These results revealed that accounting managers should carefully consider balancing the benefits and related costs to enforcing ISPs to prevent ISP stress risks.

Dissertation Limitations

As with all empirical survey investigations, this dissertation is subject to limitations. First, this study does not consider the accountants' individual backgrounds, professional certifications for information systems or security, and level within an organization. These personal factors and others may affect an individual's risk propensity. Second, this study is limited in the type of ISP violations studied. The results could change as specific instances are applied. Third, this study examines self-reported intention behavior. Although several precautions were taken to avoid social desirability bias, this limitation can still be taken into consideration. Finally, this dissertation conceptualized elements of the fraud triangle with specific construct creation. However, the items used to measure these constructs may be further defined and expanded (e.g., rationalization) in order to capture the entirety of the concept.

Conclusion and Directions for Future Research

Future research will benefit from considering the findings of this dissertation. First, future studies should look for other characteristics of rationalization. Accounting employees may undergo different types of cognitive mechanisms when faced with different types of violation behaviors. For example, the moral disengagement theory details many other types of cognitive resources individuals may deploy other than responsibility. Second, ISP violations in my dissertation examined general violations. Future studies should investigate specific scenarios of both non-malicious and malicious ISP violations. Third, the consequences faced with an intentional ISP violation behavior will vary from the consequences of a malicious ISP violation. This deterrent of consequences can be further examined even when accounting employees are faced with

high levels of ISP pressure. Lastly, future research can benefit from an expansion of personal characteristics such as cultural norms within an organization (e.g., tone at the top) and professional certification (e.g., CISA, CPA) may impact an accounting employee's propensity to commit ISP violations.

REFERENCES

Abelson, R. P., Aronson, E. E., McGuire, W. J., Newcomb, T. M., Rosenberg, M. J., and Tannenbaum, P. H. 1968. Theories of cognitive consistency: A sourcebook, pp. 112-139.

Abramis, D. J. 1994. Work role ambiguity, job satisfaction, and job performance: meta-analyses and review, psychological reports (75:3_suppl), pp. 1411-1433.

Abu-Musa, A. A. 2006. Perceived security threats of computerized accounting information systems in the egyptian banking industry, *Journal of Information Systems* (20:1), pp. 187-203.

Adams, G. B., and D. L. Balfour. 1998. *Unmasking Administrative Evil*. Thousand Oaks, CA: Sage Publications, pp. 393-398.

Adams, J. S. 1965. Inequity in social exchange, in *Advances in Experimental Social Psychology*. Elsevier, pp. 267-299.

Aiken, L. S., and Stephen, G. 1985. West (1991), *Multiple regression: Testing and interpreting interactions*. Newbury Park, CA: Sage, pp. 139-195.

Albrecht, S., and Albrecht, W. S. 1982. *How to Detect and Prevent Business Fraud*. Prentice-Hall Englewood Cliffs, NJ, pp. 1-277.

Albrecht, W. S., Albrecht, C., and Albrecht, C. C. 2008. Current trends in fraud and its detection, *Information Security Journal*: *A Global Perspective* (17:1), pp. 2-12.

Albrecht, W. S., Howe, K. R., and Romney, M. B. 1984. Deterring fraud: The internal auditor's perspective. *Institute of Internal Auditors Research Foundation* Altamonte Springs, FL, pp. 1-169.

Albrecht, W. S., Wernz, G. W., and Williams, T. L. 1995. *Fraud: Bringing Light to the Dark Side of Business.* Irwin Professional Pub, pp. 1-150.

Alge, B. J. 2001. Effects of computer surveillance on perceptions of privacy and procedural justice, *Journal of Applied Psychology* (86:4), p. 797-804.

Alge, B. J. 2001. Effects of computer surveillance on perceptions of privacy and procedural justice, *Journal of Applied Psychology* (86:4), p. 797-804.

Allam, S., Flowerday, S. V., and Flowerday, E. 2014. Smartphone information security awareness: A victim of operational pressures, computers & security (42), pp. 56-65.

Amiram, D., Bozanic, Z., Cox, J. D., Dupont, Q., Karpoff, J. M., and Sloan, R. 2018. Financial reporting fraud and other forms of misconduct: A multidisciplinary review of the literature, *Review of Accounting Studies* (23:2), pp. 732-783.

Andries, F., Kompier, M. A., and Smulders, P. G. 1996. Do you think that your health or safety are at risk because of your work? A large european study on psychological and physical work demands, work & stress (10:2), pp. 104-118.

Ariss, S. S. 2002. Computer monitoring: Benefits and pitfalls facing management, *Information & Management* (39:7), pp. 553-558.

Aronson, E. 1999. The power of self-persuasion, *American Psychologist* (54:11), p. 875-884.

Ashton, R. H. 1990. Pressure and performance in accounting decision settings: paradoxical effects of incentives, feedback, and justification, *Journal of Accounting Research* (28), pp. 148-180.

Association of Certified Fraud Examiners. 2018. Report to the Nations 2018 Global Study on Occupational Fraud and Abuse (Austin: ACFE), pp. 2-20.

Ayyagari, R., Grover, V., and Purvis, R. 2011. Technostress: Technological antecedents and implications, *MIS Quarterly* (35:4), pp. 831-858.

Balakrishnan, K., Blouin, J. L., and Guay, W. R. 2019. Tax aggressiveness and corporate transparency, *The Accounting Review* (94:1), pp. 45-69.

Bandura, A. 1977. Self-Efficacy: Toward a unifying theory of behavioral change, *Psychological Review* (84:2), p. 191-215.

Bandura, A. 1990. Selective Activation and Disengagement of Moral Control, *Journal of Social Issues* (46:1), pp. 27-46.

Bandura, A. 1999. Moral disengagement in the perpetration of inhumanities, *Personality and Social Psychology Review* (3:3), pp. 193-209.

Bandura, A., Barbaranelli, C., Caprara, G. V., and Pastorelli, C. 1996. Mechanisms of moral disengagement in the exercise of moral agency, *Journal of Personality and Social Psychology* (71:2), p. 364-374.

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

Baron, R. A. 2006. Opportunity recognition as pattern recognition: How entrepreneurs "connect the dots" to Identify new business opportunities, *Academy of Management Perspectives* (20:1), pp. 104-119.

Bayou, M. E., Reinstein, A., and Williams, P. F. 2011. To tell the truth: A discussion of issues concerning truth and ethics in accounting, *Accounting, Organizations and Society* (36:2), pp. 109-124.

Bazerman, M. H., and Tenbrunsel, A. E. 2012. *Blind Spots: Why We Fail to Do What's Right and What to Do About It*. Princeton University Press, pp. 9-135.

Beasley, M. S., Carcello, J. V., Hermanson, D. R., and Neal, T. L. 2009. The audit committee oversight process, *Contemporary Accounting Research* (26:1), pp. 65-122.

Bell, T. B., and Carcello, J. V. 2000. A decision aid for assessing the likelihood of fraudulent financial reporting, *Auditing: A Journal of Practice & Theory* (19:1), pp. 169-184.

Berezina, K., Cobanoglu, C., Miller, B. L., and Kwansa, F. A. 2012. The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth, *International Journal of Contemporary Hospitality Management*, pp. 991-1010.

Bersoff, D. M. 1999. Why good people sometimes do bad things: Motivated reasoning and unethical behavior, *Personality and Social Psychology Bulletin* (25:1), pp. 28-39.

Besnard, D., and Arief, B. 2004. Computer security impaired by legitimate users, *Computers & Security* (23:3), pp. 253-264.

Bhimani, A., and Willcocks, L. 2014. Digitisation,'big data'and the transformation of accounting information, *Accounting and Business Research* (44:4), pp. 469-490.

Bierstaker, J. L., Cohen, J. R., DeZoort, F. T., Hermanson, D. R., Gramling, R. H., Holt, T., Homma, S., Krishnamoorthy, G., Mattiford, D., and Peters, G. 2009. The effects of audit committee compensation, fairness, and responsibility on the resolution of accounting disagreements, Available at *SSRN* 1462440, pp. 2-40.

Bies, R. J., and Shapiro, D. L. 1987. Interactional fairness judgments: The influence of causal accounts, *Social Justice Research* (1:2), pp. 199-218.

Bonner, J. M., Greenbaum, R. L., and Mayer, D. M. 2016. my boss is morally disengaged: The role of ethical leadership in explaining the interactive effect of supervisor and employee moral disengagement on employee behaviors, *Journal of Business Ethics* (137:4), pp. 731-742.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. If someone is watching, i'll do what i'm asked: mandatoriness, control, and information security, *European Journal of Information Systems* (18:2), pp. 151-164.

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

Bosse, D. A., and Phillips, R. A. 2016. Agency theory and bounded self-interest, *Academy of Management Review* (41:2), pp. 276-297.

Brief, A. P., Buttram, R. T., and Dukerich, J. M. 2001. Collective corruption in the corporate world: Toward a process model, *Groups at Work: Theory and Research*, pp. 471-500.

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

Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, L. 2003. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market, *Journal of Computer Security* (11:3), pp. 431-448.

Carayon, P. 1995. Effect of computer system performance and other work stressors on strain of office workers, in *Advances in Human Factors/Ergonomics*. Elsevier, pp. 693-698.

Carayon, P., and Zijlstra, F. 1999. Relationship between job control, work pressure and strain: studies in the USA and in the Netherlands, *Work & Stress* (13:1), pp. 32-48.

Carayon, P., Hoonakker, P., Marchand, S., and Schwarz, J. 2003. Job characteristics and quality of working life in the it workforce: The role of gender, Proceedings of the 2003 SIGMIS conference on *Computer Personnel Research: Freedom in Philadelphia*--leveraging differences and diversity in the IT workforce: ACM, pp. 58-63.

Carcello, J. V., and Hermanson, D. R. 2008. Fraudulent financial reporting: How do we close the knowledge gap, *Research Studies (*White Papers) of Institute for Fraud Prevention (IFP), pp. 2-23.

Cavanaugh, M. A., Boswell, W. R., Roehling, M. V., and Boudreau, J. W. 2000. An empirical examination of self-reported work stress among US managers, *Journal of Applied Psychology* (85:1), pp. 65-74.

Chae, B., and Poole, M. S. 2005. Mandates and technology acceptance: A tale of two enterprise technologies, *The Journal of Strategic Information System*s (14:2), pp. 147-166.

Chatterjee, S., Sarker, S., and 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), pp. 49-87.

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

Chia, A., and Lim, S. M. 2000. The effects of issue characteristics on the recognition of moral issues, *Journal of Business Ethics* (27:3), pp. 255-269.

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

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

Chong, V. K., and Monroe, G. S. 2015. The impact of the antecedents and consequences of job burnout on junior accountants' turnover intentions: A structural equation modelling approach, *Accounting & Finance* (55:1), pp. 105-132.

Chong, V. K., and Wang, I. Z. 2019. Delegation of decision rights and misreporting: the roles of incentive-based compensation schemes and responsibility rationalization, *European Accounting Review* (28:2), pp. 275-307.

Christ, M. H. 2013. An experimental investigation of the interactions among intentions, reciprocity, and control, *Journal of Management Accounting Research* (25:1), pp. 169-197.

Christ, M. H., Sedatole, K. L., Towry, K. L., and Thomas, M. A. 2008. When formal controls undermine trust and cooperation, *Strategic Finance* (89:7), pp. 39-44.

Clayton, J. 2017. Statement on cybersecurity. Retrieved from https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20, *U.S. Securities and Exchange Commission*.

Clotfelter, C. T. 1983. Tax evasion and tax rates: An analysis of individual returns, *The Review of Economics and Statistics*, pp. 363-373.

Cohen, J. R., Holder-Webb, L., Sharp, D. J., and Pant, L. W. 2007. The effects of perceived fairness on opportunistic behavior, *Contemporary Accounting Research* (24:4), pp. 1119-1138.

Collins, K. M. 1993. stress and departures from the public accounting profession: A study of gender differences, *Accounting Horizons* (7:1), pp. 29-38.

Collins, K. M., and Killough, L. N. 1992. An empirical examination of stress in public accounting, *Accounting, Organizations and Society* (17:6), pp. 535-547.

Colquitt, J. A., Conlon, D. E., Wesson, M. J., Porter, C. O., and 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), pp. 425-445.

Colquitt, J. A., Greenberg, J., and Greenberg, J. 2003. Organizational justice: A fair assessment of the state of the literature, *Organizational Behavior*: *The State of The Science*, pp. 159-200.

Colquitt, J. A., LePine, J. A., Piccolo, R. F., Zapata, C. P., and Rich, B. L. 2012. "Explaining the justice–performance relationship: Trust as exchange deepener or trust as uncertainty reducer? *Journal of Applied Psychology* (97:1), pp. 1-15.

Compeau, D. R., and Higgins, C. A. 1995. Computer self-efficacy: Development of a measure and initial test, *MIS Quarterly*), pp. 189-211.

Conner, F. W., and Coviello, A. W. 2004. Information security governance: A call to action, *The Corporate Governance Task Force*, pp. 3-49.

Coras, E. L., and Tantau, A. D. 2013. A risk mitigation model in *Sme's Open Innovation Projects, Management & Marketing* (8:2), p. 303-328.

Cory, S. N., and Pruske, K. A. 2012. Necessary skills for accounting graduates: An exploratory study to determine what the profession wants, *ASBBS Proceedings* (19:1), pp. 208-218.

Cressey, D. R. 1953. Other people's Money: A study of the social psychology of embezzlement. Glencoe, IL: Free Press, pp.1-191.

Cressey, D. R. 1954. The differential association theory and compulsive crimes, *The Journal of Criminal Law, Criminology, and Police Science* (45:1), pp. 29-40.

Cutter, H. 2018. The morning risk report: Firms go beyond tech to fight data theft. Retrieved 01/29/2018, from https://blogs.wsj.com/riskandcompliance/2018/01/29/the-morning-risk-report-firms-go-beyond-tech-to-fight-data-theft/

D'Arcy, J., and Teh, P.-L. 2019. Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization, *Information & Management* (56:7), pp. 260-281.

Daniels, K., and Guppy, A. 1997. Stressors, locus of control, and social support as consequences of affective psychological well-being, *Journal of Occupational Health Psychology* (2:2), pp. 156-174.

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

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

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

Das, T., and Teng, B. S. 2001. Strategic Risk Behaviour and Its Temporalities: Between Risk Propensity and Decision Context, *Journal of Management Studies* (38:4), pp. 515-534.

Das, T., and Teng, B.-S. 1999. Managing Risks in Strategic Alliances, *Academy of Management Perspectives* (13:4), pp. 50-62.

Davis, H. A., Militello, F. C., & Financial Executives Research Foundation. (1994). *The empowered organization: Redefining the roles and practices of finance*. Morristown, N.J: Financial Executives Research Foundation, pp. 50-225

Davis, M. A., Andersen, M. G., and Curtis, M. B. 2001. Measuring ethical ideology in business ethics: A critical analysis of the ethics position questionnaire, *Journal of Business Ethics* (32:1), pp. 35-53.

Deci, E. L. 1972. The Effects of Contingent and Noncontingent Rewards and Controls on Intrinsic Motivation, *Organizational Behavior and Human Performance* (8:2), pp. 217-229.

Denman, D. E. (2019). 2018 Report on Occupational Fraud: Results and How Companies Can Protect Their Assets. *Journal of Accounting and Finance*, *19*(4), pp. 97-112

Detert, J. R., Treviño, L. K., and Sweitzer, V. L. 2008. Moral disengagement in ethical decision making: A study of antecedents and outcomes, *Journal of Applied Psychology* (93:2), pp. 374-391.

Dhillon, G. 1999. Managing and controlling computer misuse, *Information Management & Computer Security* (7:4), pp. 171-175.

Dhillon, G. 2001. Violation of safeguards by trusted personnel and understanding related information security concerns, *Computers & Security* (20:2), pp. 165-172.

Dineen, B. R., Lewicki, R. J., and Tomlinson, E. C. 2006. Supervisory guidance and behavioral integrity: relationships with employee citizenship and deviant behavior, *Journal of Applied Psychology* (91:3), pp. 622-635.

Dobre, O.-I. 2013. Employee motivation and organizational performance, *Review of Applied Socio-Economic Research* (5:1), pp. 53-91.

Dopuch, N., Birnberg, J. G., & Demski, J. S. (1974). *Cost accounting; accounting data for management's decisions*. New York: Harcourt Brace Jovanovich, pp. 100-350.

Dorminey, J. W., Fleming, A. S., Kranacher, M.-J., and Riley Jr, R. A. 2010. Beyond the fraud triangle, *The CPA Journal* (80:7), pp. 17-23.

Dorminey, J., Fleming, A. S., Kranacher, M.-J., and Riley Jr, R. A. 2012. The evolution of fraud theory, *Issues in Accounting Education* (27:2), pp. 555-579.

Dourish, P., Grinter, R. E., De La Flor, J. D., and Joseph, M. 2004. Security in the wild: User strategies for managing security as an everyday, practical problem, *Personal and Ubiquitous Computing* (8:6), pp. 391-401.

Duncan, R. B. 1972. Characteristics of organizational environments and perceived environmental uncertainty, *Administrative Science Quarterly*, pp. 313-327.

Dunlop, P. D., and Lee, K. 2004. Workplace deviance, organizational citizenship behavior, and business unit performance: The bad apples do spoil the whole barrel, *Journal of Organizational Behavior*: *The International Journal of Industrial, Occupational and Organizational Psychology and Behavior* (25:1), pp. 67-80.

Eisenhardt, K. M. 1985. Control: Organizational and economic approaches, *Management Science* (31:2), pp. 134-149.

Elliot, A. J., and Devine, P. G. 1994. On the motivational nature of cognitive dissonance: Dissonance as psychological discomfort, *Journal of Personality and Social Psychology* (67:3), p. 382- 394.

El-Sayed, H., and Westrup, C. 2011. adopting enterprise web 2.0 collaborative technologies in business: The implications for management accountants, *CIMA* (7:4), pp. 1-8.

Enzle, M. E., and Anderson, S. C. 1993. Surveillant intentions and intrinsic motivation, *Journal of Personality and Social Psychology* (64:2), pp. 257-266.

Evans III, J. H., Hannan, R. L., Krishnan, R., and Moser, D. V. 2001. Honesty in managerial reporting, *The Accounting Review* (76:4), pp. 537-559.

Everly, G. S., & Sobelman, S. A. (1987). *Assessment of the human stress response: Neurological, biochemical, and psychological foundations*. New York: AMS Press, pp. 10-134.

Festinger, L. 1962. *A Theory of Cognitive Dissonance*. Stanford, CA: Stanford University Press, pp. 20-250.

Fiolleau, K., Libby, T., and Thorne, L. 2018. Dysfunctional behavior in organizations: Insights from the management control literature, *Auditing: A Journal of Practice & Theory* (37:4), pp. 117-141.

Fisher, R. T. 2001. Role stress, the type a behavior pattern, and external auditor job satisfaction and performance, *Behavioral Research in Accounting* (13:1), pp. 143-170.

Fogarty, T. J., Singh, J., Rhoads, G. K., and Moore, R. K. 2000. Antecedents and consequences of burnout in accounting: Beyond the role stress model, *Behavioral Research in Accounting* (12), pp. 31-68.

Folger, R., & Cropanzano, R. (1998). *Organizational justice and human resource management*. Thousand Oaks: Sage Publications, pp. 5-270.

Fornell, C., and Larcker, D. F. 1981. Evaluating structural equation models with unobservable variables and measurement error, *Journal of Marketing Research* (18:1), pp. 39-50.

Forsyth, D. R. 1980. A Taxonomy of ethical ideologies, *Journal of Personality and Social Psychology* (39:1), p. 175.

Frank, R. H. 1988. *Passions Within Reason: The Strategic Role of the Emotions*. New York: WW Norton & Co, pp. 1-304.

Free, C. (2015). Looking through the fraud triangle: a review and call for new directions, *Meditari Accountancy Research*, *23*(2), pp. 175-196.

Free, C., Macintosh, N., and Stein, M. 2007. Management controls: The organizational fraud triangle of leadership, culture and control in Enron, *Ivey Business Journal* (71:6), pp. 1-5.

Fritz, B., Schwartzel, E., & Barrett, D. (2014, December 18). Sony Pulls Korea Film 'The Interview;' U.S. Blames Pyongyang for Hack. Retrieved from https://www.wsj.com/articles/sony-cancels-release-of-the-interview-us-blames-pyongyang-for-hack-1418844906.

Gaertner, J. F., and Ruhe, J. A. 1981. Job-related stress in public accounting: Cpas who are under the most stress and suggestions on how to cope, *Journal of Accountancy* (pre-1986) (151:6), pp. 68-74.

Gao, P., and Zhang, G. 2019. Accounting manipulation, peer pressure, and internal control, *The Accounting Review* (94:1), pp. 127-151.

Gattiker, U. E., and Kelley, H. 1999. Morality and computers: Attitudes and differences in moral judgments, *Information Systems Research* (10:3), pp. 233-254.

Gefen, D., Rigdon, E. E., and Straub, D. 2011. Editor's comments: An update and extension to sem guidelines for administrative and social science research, *Mis Quarterly*, pp. iii-xiv.

George, J. F. 1996. Computer-based monitoring: Common perceptions and empirical results, *MIS Quarterly*, pp. 459-480.

Ghoshal, S. 2005. Bad management theories are destroying good management practices, *Academy of Management Learning & Education* (4:1), pp. 75-91.

Gist, M. E., and Mitchell, T. R. 1992. Self-efficacy: A theoretical analysis of its determinants and malleability, *Academy of Management Review* (17:2), pp. 183-211.

Gneezy, U. 2005. Deception: The role of consequences, *American Economic Review* (95:1), pp. 384-394.

Goles, T., White, G. B., Beebe, N., Dorantes, C. A., and Hewitt, B. 2006. Moral intensity and ethical decision-making: A contextual extension, ACM SIGMIS Database: the DATABASE for *Advances in Information Systems* (37:2-3), pp. 86-95.

Gorge, M. 2005. USB & other portable storage device usage: Be aware of the risks to your corporate data in order to take pre-emptive and/or corrective action, *Computer Fraud & Security* (2005:8), pp. 15-17.

Greenberg, J. 1987. A taxonomy of organizational justice theories, *Academy of Management Review* (12:1), pp. 9-22.

Greenberg, J. 1990. Organizational justice: Yesterday, today, and tomorrow, *Journal of Management* (16:2), pp. 399-432.

Greenberg, J. 2002. Who stole the money, and when? individual and situational determinants of employee theft, *Organizational Behavior and Human Decision Processes* (89:1), pp. 985-1003.

Greenberg, J., and Folger, R. 1983. Procedural justice, participation, and the fair process effect in groups and organizations, in *Basic Group Processes*. Springer, pp. 235-256.

Guo, K. H. 2013. Security-related behavior in using information systems in the workplace: A review and synthesis, *Computers & Security* (32), pp. 242-251.

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

Guragai, B., Hunt, N. C., Neri, M. P., and Taylor, E. Z. 2015. Accounting information systems and ethics research: Review, synthesis, and the future, *Journal of Information Systems* (31:2), pp. 65-81.

Guzzo, R. A. 1979. Types of rewards, cognitions, and work motivation, *Academy of Management Review* (4:1), pp. 75-86.

Hackett, G., and Betz, N. E. 1981. A self-efficacy approach to the career development of women, *Journal of Vocational Behavior* (18:3), pp. 326-339.

Haines, R., and Leonard, L. N. 2007a. Individual characteristics and ethical decision-making in an it context, *Industrial Management & Data Systems* (107:1), pp. 5-20.

Haines, R., and Leonard, L. N. 2007b. Situational influences on ethical decision-making in an it context, *Information & Management* (44:3), pp. 313-320.

Hamdan, M. N. M. 2017. The relationship between network security policies and audit evidence documentation: The accounting information security culture as a mediator, *International Journal of Business and Management* (12:12), pp. 168-180.

Haried, P., Claybaugh, C., and Dai, H. 2019. Evaluation of health information systems research in information systems research: A meta-analysis, *Health Informatics Journal* (25:1), pp. 186-202.

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

Hartman, S. W., Qureshi, A., and Siegel, J. G. 1997. Online databases: Information available electronically, *The CPA Journal* (67:4), pp. 46-54.

Hay, R., and Gray, E. 1974. Social responsibilities of business managers, *Academy of Management Journal* (17:1), pp. 135-143.

Heales, J., Susilo, A., and Rohde, F. 2007. Project management effectiveness: The choice-formal or informal controls, *Australasian Journal of Information Systems* (15:1), pp. 153-167.

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

Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. Design science in information systems research, *MIS Quarterly*, pp. 75-105.

Hollinger, R. C., & Clark, J. P. (1985). *Theft by employees*. Lexington, Ma.: Lexington Books, pp. 1-160.

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

Hu, Q., Dinev, T., Hart, P., and Cooke, D. 2012. Managing employee compliance with information security policies: The critical role of top management and organizational culture, *Decision Sciences* (43:4), pp. 615-660.

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

Mui, G., and Mailley, J. 2015. A tale of two triangles: Comparing the fraud triangle with criminology's crime triangle, *Accounting Research Journal* (29:1), pp. 45-58.

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), pp. 83-95.

Iverson, R. D., and Maguire, C. 2000. The relationship between job and life satisfaction: Evidence from a remote mining community, *Human Relation*s (53:6), pp. 807-839.

Jamal, M. 1984. Job stress and job performance controversy: An empirical assessment, *Organizational Behavior and Human Performance* (33:1), pp. 1-21.

Johnson, E. N., Kuhn Jr, J. R., Apostolou, B. A., and Hassell, J. M. 2013. Auditor perceptions of client narcissism as a fraud attitude risk factor, *Auditing: A Journal of Practice & Theory* (32:1), pp. 203-219.

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

Johnston, A. C., Warkentin, M., McBride, M., and Carter, L. 2016. Dispositional and situational factors: Influences on information security policy violations, *European Journal of Information Systems* (25:3), pp. 231-251.

Jones III, A., Norman, C. S., and Wier, B. 2010. Healthy lifestyle as a coping mechanism for role stress in public accounting, *Behavioral Research in Accounting* (22:1), pp. 21-41.

Kahneman, D., Knetsch, J. L., and Thaler, R. 1986. Fairness as a constraint on profit seeking: Entitlements in the market, *The American Economic Review*, pp. 728-741.

Kelloway, E. K., Loughlin, C., Barling, J., and Nault, A. 2002. Self-Reported counterproductive behaviors and organizational citizenship behaviors: Separate but related constructs, *International Journal of Selection and Assessment* (10:1-2), pp. 143-151.

Kelman, H. C., & Hamilton, V. L. (1989). *Crimes of obedience: Toward a social psychology of authority and responsibility*. New Haven: Yale University Press, pp. 20-300.

Kirlappos, I., Beautement, A., and Sasse, M. A. 2013. Comply or die is dead: Long live security-aware principal agents, *International Conference on Financial Cryptography and Data Security*, Springer, pp. 70-82.

Kirsch, L. J. 1996. The management of complex tasks in organizations: Controlling the systems development process, *Organization Science* (7:1), pp. 1-21.

Kirzner, I. M. (1979). *Perception, opportunity, and profit: Studies in the theory of entrepreneurship*. Chicago: University of Chicago Press, pp. 142-143.

Kranacher, M.-J., Riley, R., & Wells, J. T. (2011). *Forensic accounting and fraud examination*. Hoboken, N.J: John Wiley.

Kranacher, M.-J., and Stern, L. 2004. Enhancing fraud detection through education, *The CPA Journal* (74:11), pp. 66-67.

Kwon, J., and Johnson, M. E. 2013. Health-care security strategies for data protection and regulatory compliance, *Journal of Management Information Systems* (30:2), pp. 41-66.

Latham, G. P., Mitchell, T. R., and Dossett, D. L. 1978. Importance of participative goal setting and anticipated rewards on goal difficulty and job performance, *Journal of Applied Psychology* (63:2), p. 163-171.

Lawrence, P. R., and Lorsch, J. W. 1967. *Organization and Environment*. Boston, Ma: Harvard Business School, Division of Research.

Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping*. New York: Springer Pub. Co.

Lee, J. 2001. Leader-member exchange, perceived organizational justice, and cooperative communication, *Management Communication Quarterly* (14:4), pp. 574-589.

Lee, S.-H., Kwak, J., and Lee, I.-Y. 2009. The study on the security solutions of USB memory, *Proceedings of the 4th International Conference on Ubiquitous Information Technologies & Applications*. IEEE, pp. 1-4.

Lee, Y., Lee, J., and Lee, Z. 2006. Social influence on technology acceptance behavior: self-identity theory perspective, *ACM SIGMIS Database: The Database for Advances in Information Systems* (37:2-3), pp. 60-75.

Leiwo, J., and Heikkuri, S. 1998. An analysis of ethics as foundation of information security in distributed systems, *Proceedings of the Thirty-First Hawaii International Conference on System Sciences*. IEEE, pp. 213-222.

Leventhal, G. S., Karuza, J., and Fry, W. R. 1980. "Beyond Fairness: A Theory of Allocation Preferences," Justice and social interaction (3:1), pp. 167-218.

Li, H., Sarathy, R., Zhang, J., and Luo, X. 2014. "Exploring the Effects of Organizational Justice, Personal Ethics and Sanction on Internet Use Policy Compliance," Information Systems Journal (24:6), pp. 479-502.

Libby, R. 1983. Comments on weick, *The Accounting Review* (58:2), pp. 370-374.

Libby, T. 2001. Referent cognitions and budgetary fairness: A research note, *Journal of Management Accounting Research* (13:1), pp. 91-105.

Loch, K. D., Carr, H. H., and Warkentin, M. E. 1992. Threats to information systems: Today's reality, yesterday's understanding, *MIS Quarterly*, pp. 173-186.

Locke, E. A., Shaw, K. N., Saari, L. M., and Latham, G. P. 1981. Goal setting and task performance: 1969–1980, *Psychological Bulletin* (90:1), p. 125.

Lokanan, M. E. 2015. Challenges to the fraud triangle: Questions on its usefulness, *Accounting Forum*. Taylor & Francis, pp. 201-224.

Longenecker, C. O., Sims Jr, H. P., and Gioia, D. A. 1987. Behind the mask: The politics of employee appraisal, *Academy of Management Perspectives* (1:3), pp. 183-193.

Lou, Y.-I., and Wang, M.-L. 2009. Fraud risk factor of the fraud triangle assessing the likelihood of fraudulent financial reporting, *Journal of Business & Economics Research* (7:2), pp. 61-78.

Low, M., Davey, H., and Hooper, K. 2008. Accounting scandals, ethical dilemmas and educational challenges, *Critical perspectives on Accounting* (19:2), pp. 222-254.

Lowry, P. B., and Gaskin, J. 2014. Partial least squares (pls) structural equation modeling (sem) for building and testing behavioral causal theory: When to choose it and how to use it, *IEEE* transactions on professional communication (57:2), pp. 123-146.

Lowry, P. B., and Moody, G. D. 2015. Proposing the control-reactance compliance model (crcm) to explain opposing motivations to comply with organisational information security policies, *Information Systems Journal* (25:5), pp. 433-463.

Luft, J. L. 1997. Fairness, ethics and the effect of management accounting on transaction costs, *Journal of Management Accounting Research* (9), pp. 199-216.

Malhotra, Y., and Galletta, D. 2005. A multidimensional commitment model of volitional systems adoption and usage behavior, *Journal of Management Information Systems* (22:1), pp. 117-151.

Malmi, T., and Brown, D. A. 2008. Management control systems as a package—opportunities, challenges and research directions, *Management Accounting Research* (19:4), pp. 287-300.

Marsden, D., & French, S. (1998). *What a performance: Performance related pay in the public sector*. London: Centre for Economic Performance, London School of Economics and Political Science.

Martins, A., and Elofe, J. 2002. *Information Security Culture, in Security in the Information Society*. Springer, pp. 203-214.

Mayhew, B. W., and Murphy, P. R. 2014. The impact of authority on reporting behavior, rationalization and affect, *Contemporary Accounting Research* (31:2), pp. 420-443.

McKimmie, B. M., Terry, D. J., Hogg, M. A., Manstead, A. S., Spears, R., and Doosje, B. 2003. I'm a hypocrite, but so is everyone else: Group support and the reduction of cognitive dissonance, *Group Dynamics: Theory, Research, and Practice* (7:3), pp. 214-224.

Merchant, K. A., and Otley, D. T. 2006. A review of the literature on control and accountability, *Handbooks of Management Accounting Research* (2), pp. 785-802.

Merchant, K. A., & Van, . S. W. A. (2012). *Management control systems: Performance measurement, evaluation and incentives*. Harlow, England: Financial Times/Prentice Hall.

Moody, G. D., Siponen, M., and Pahnila, S. 2018. Toward a unified model of information security policy compliance, *MIS Quarterly* (42:1), pp. 285-311.

Moore, A. P., Cappelli, D. M., and Trzeciak, R. F. 2008. The 'big picture' of insider it sabotage across US critical infrastructures, in *Insider Attack and Cyber Security*. Springer, pp. 17-52.

Moore, C. 2008. Moral disengagement in processes of organizational corruption, *Journal of Business Ethics* (80:1), pp. 129-139.

Morales, J., Gendron, Y., and Guénin-Paracini, H. 2014. The construction of the risky individual and vigilant organization: A genealogy of the fraud triangle, *Accounting, Organizations and Society* (39:3), pp. 170-194.

Motowidlo, S. J., Packard, J. S., and Manning, M. R. 1986. Occupational stress: Its causes and consequences for job performance, *Journal of Applied Psychology* (71:4), pp. 618-629.

Murphy, P. R. 2012. Attitude, machiavellianism and the rationalization of misreporting, *Accounting, Organizations and Society* (37:4), pp. 242-259.

Murphy, P. R., and Dacin, M. T. 2011. Psychological pathways to fraud: Understanding and preventing fraud in organizations, *Journal of Business Ethics* (101:4), pp. 601-618.

Murphy, P. R., and Free, C. 2015. Broadening the fraud triangle: Instrumental climate and fraud, *Behavioral Research in Accounting* (28:1), pp. 41-56.

Mynatt, C., and Sherman, S. J. 1975. Responsibility attribution in groups and individuals: A direct test of the diffusion of responsibility hypothesis, *Journal of Personality and Social Psychology* (32:6), pp. 1111-1118.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. What levels of moral reasoning and values explain adherence to information security rules? An empirical study, *European Journal of Information Systems* (18:2), pp. 126-139.

Nevins, J. L., Bearden, W. O., and Money, B. 2007. Ethical values and long-term orientation, *Journal of Business Ethics* (71:3), pp. 261-274.

Nickerson, M. A. 2019. Fraud in a world of advanced technologies: The possibilities are (unfortunately) endless, *The CPA Journal* (89:6), pp. 28-34.

Noreen, E. 1988. The economics of ethics: A new perspective on agency theory, *Accounting, Organizations and Society* (13:4), pp. 359-369.

Padayachee, K. 2016. An assessment of opportunity-reducing techniques in information security: An insider threat perspective, *Decision Support Systems* (92), pp. 47-56.

Pan, G., and Seow, P.-S. 2016. Preparing accounting graduates for digital revolution: a critical review of information technology competencies and skills development, *Journal of Education for Business* (91:3), pp. 166-175.

Paradice, D. B., and Dejoie, R. M. 1991. The ethical decision-making processes of information systems workers, *Journal of Business Ethics* (10:1), pp. 1-21.

Paternoster, R. 2010. How much do we really know about criminal deterrence, *Journal of Criminal Law & Criminology* (100), pp. 765-824.

Podsakoff, P. M., MacKenzie, S. B., and Podsakoff, N. P. 2012. Sources of method bias in social science research and recommendations on how to control it, *Annual Review of Psychology* (63), pp. 539-569.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. Common method biases in behavioral research: A critical review of the literature and recommended remedies, *Journal of Applied Psychology* (88:5), pp. 879-903.

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

Posey, C., Bennett, R. J., and Roberts, T. L. 2011b. Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes, *Computers & Secu*rity (30:6-7), pp. 486-497.

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

Pratt, T. C., and Cullen, F. T. 2000. The empirical status of gottfredson and hirschi's general theory of crime: A meta-analysis, *Criminology* (38:3), pp. 931-964.

PricewaterhouseCoopers. (2018). The Global State of Information Security Survey 2018. Retrieved from https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

Puhakainen, P., and Ahonen, R. 2006. *Design Theory for Information Security Awareness* (Dissertation), pp. 10-140.

Puhakainen, P., and Siponen, M. 2010. Improving employees' compliance through information systems security training: An action research study, *MIS Quarterly*, pp. 757-778.

Rae, K., Subramaniam, N., and Sands, J. 2008. Risk management and ethical environment: Effects on internal audit and accounting control procedures, *Journal of Applied Management Accounting Research* (6:1), pp. 11-30.

Ragu-Nathan, T., Tarafdar, M., Ragu-Nathan, B. S., and Tu, Q. 2008. The consequences of technostress for end users in organizations: Conceptual development and empirical validation, *Information Systems Research* (19:4), pp. 417-433.

Ramamoorti, S. 2008. The psychology and sociology of fraud: Integrating the behavioral sciences component into fraud and forensic accounting curricula, *Issues in Accounting Education* (23:4), pp. 521-533.

Ramamoorti, S., and Olsen, W. 2007. Fraud: The human factor, *Financial Executive* (23:6), pp. 53-56.

Ramamoorti, S., Morrison, D., & Koletar, J. W. (2009). Bringing Freud to Fraud: Understanding the state-of-mind of the C-level suite/white collar offender through "ABC" analysis. *Institute for Fraud Prevention (IFP) at West Virginia University*, pp. 1-35.

Rebele, J. E. 1985. An examination of accounting students' perceptions of the importance of communication skills in public accounting, *Issues in Accounting Education* (3:1), pp. 41-50.

Renaud, K. 2011. Blaming noncompliance is too convenient: What really causes information breaches? *IEEE Security & Privacy* (10:3), pp. 57-63.

Rezaee, Z. 2005. Causes, consequences, and deterence of financial statement fraud, *Critical Perspectives on Accounting* (16:3), pp. 277-298.

Rhee, H.-S., Kim, C., and Ryu, Y. U. 2009. Self-efficacy in information security: Its influence on end users' information security practice behavior, *Computers & Security* (28:8), pp. 816-826.

Ringle, C. M., Sarstedt, M., and Straub, D. W. 2012. Editor's comments: A critical look at the use of pls-sem in mis quarterly, *MIS Quarterly*, pp. iii-xiv.

Robin, D. P., Reidenbach, R. E., and Forrest, P. 1996. The perceived importance of an ethical issue as an influence on the ethical decision-making of ad managers, *Journal of Business Research* (35:1), pp. 17-28.

Rockness, H., and Rockness, J. 2005. Legislated ethics: From enron to sarbanes-oxley, the impact on corporate America, *Journal of Business Ethics* (57:1), pp. 31-54.

Rodell, J. B., and 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), pp. 1438-1451.

Rowe, A. 2019. Study reveals security risk of remote working, from https://tech.co/news/remote-workers-security-risks-2019-03

Ruighaver, A. B., Maynard, S. B., and Warren, M. 2010. Ethical decision making: Improving the quality of acceptable use policies, *Computers & Security* (29:7), pp. 731-736.

Rupp, D. E., Shao, R., Jones, K. S., and Liao, H. 2014. The utility of a multifoci approach to the study of organizational justice: A meta-analytic investigation into the consideration of normative rules, moral accountability, bandwidth-fidelity, and social exchange, *Organizational Behavior and Human Decision Processes* (123:2), pp. 159-185.

Safa, N. S., Maple, C., Watson, T., and Von Solms, R. 2018. Motivation and opportunity based model to reduce information security insider threats in organisations, *Journal of Information Security and Applications* (40), pp. 247-257.

Schuchter, A., and Levi, M. 2016. The fraud triangle revisited, *Security Journal* (29:2), pp. 107-121.

Sewell, G., and Barker, J. R. 2006. Coercion versus care: using irony to make sense of organizational surveillance, *Academy of Management Review* (31:4), pp. 934-961.

Shepherd, D. A., McMullen, J. S., and Jennings, P. D. 2007. The formation of opportunity beliefs: Overcoming ignorance and reducing doubt, *Strategic Entrepreneurship Journal* (1:1-2), pp. 75-95.

Shropshire, J. 2009. A canonical analysis of intentional information security breaches by insiders, *Information Management & Computer Security* (17:4), pp. 296-310.

Shu, L. L., Gino, F., and Bazerman, M. H. 2009. Dishonest deed, clear conscience: self-preservation through moral disengagement and motivated forgetting, *Harvard Business School NOM Unit Working Paper*:09-078, pp. 1-53.

Simons, R. (1995). *Levers of control: How managers use innovative control systems to drive strategic renewal*. Boston, Mass: Harvard Business School Press, pp. 10-210.

Sindhav, B., Holland, J., Rodie, A. R., Adidam, P. T., and 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), pp. 323-335.

Siponen, M., and Iivari, J. 2006. Is security design theory framework and six approaches to the application of ISPS and guidelines, *Journal of the Association for Information Systems* (7:7), pp. 445-472.

Siponen, M., and Vance, A. 2010. Neutralization: New insights into the problem of employee information systems security policy violations, *MIS Quarterly*, pp. 487-502.

Siponen, M., and Vance, A. 2014. Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations, *European Journal of Information Systems* (23:3), pp. 289-305.

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

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

Skaife, H. A., Veenman, D., and Wangerin, D. 2013. Internal control over financial reporting and managerial rent extraction: Evidence from the profitability of insider trading, *Journal of Accounting and Economics* (55:1), pp. 91-110.

Smith, K. J., Derrick, P. L., and Koval, M. R. 2010. Stress and its antecedents and consequences in accounting settings: An empirically derived theoretical model, in *Advances in Accounting Behavioral Research*. Emerald Group Publishing Limited, pp. 113-142.

Snyder, C. R. 1985. The excuse: An amazing grace, *The Self and Social Life*, pp. 235-260.

Sojer, M., Alexy, O., Kleinknecht, S., and Henkel, J. 2014. Understanding the drivers of unethical programming behavior: The inappropriate reuse of internet-accessible code, *Journal of Management Information Systems* (31:3), pp. 287-325.

Sorunke, O. A. 2016. Personal ethics and fraudster motivation: The missing link in fraud triangle and fraud diamond theories, *International Journal of Academic Research in Business and Social Sciences* (6:2), pp. 159-165.

Spears, J. L., and Barki, H. 2010. User participation in information systems security risk management, *MIS Quarterly*, pp. 503-522.

Stanciu, V., and Tinca, A. 2016. Students' awareness on information security between own perception and reality–an empirical study, *Accounting & Management Information Systems/Contabilitate Si Informatica De Gestiune* (15:1), pp. 112-130.

Stanton, J. M., & Stam, K. R. (2006). *The visible employee: Using workplace monitoring and surveillance to protect information assets--without compromising employee privacy or trust*. Medford, N.J: Information Today.

Stanton, J. M., Balzer, W. K., Smith, P. C., Parra, L. F., and Ironson, G. 2001. A general measure of work stress: The stress in general scale, *Educational and Psychological Measurement* (61:5), pp. 866-888.

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

Steele, C. M. 1988. The psychology of self-affirmation: Sustaining the integrity of the self, *Advances in Experimental Social Psychology* (21:2), pp. 261-302.

Steinbart, P. J., Raschke, R. L., Gal, G., and Dilla, W. N. 2018. The influence of a good relationship between the internal audit and information security functions on information security outcomes, *Accounting, Organizations and Society* (71), pp. 15-29.

Straub Jr, D. W. 1990. Effective is security: An empirical study, *Information Systems Research* (1:3), pp. 255-276.

Straub Jr, D. W., and Nance, W. D. 1990. Discovering and disciplining computer abuse in organizations: A field study, *MIS Quarterly*, pp. 45-60.

Sutherland, V. J., & Cooper, C. L. (2000). *Strategic stress management: An organizational approach*. Basingstoke: Macmillan Busines, pp. 15-200.

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

Tarafdar, M., Tu, Q., and Ragu-Nathan, T. 2010. Impact of technostress on end-user satisfaction and performance, *Journal of Management Information Systems* (27:3), pp. 303-334.

Taylor, R. 2006. Management perception of unintentional information security risks, *ICIS 2006 Proceedings*, p. 1581-1598.

Taylor, S. E., Repetti, R. L., and Seeman, T. 1997. Health psychology: What is an unhealthy environment and how does it get under the skin? *Annual Review of Psychology* (48:1), pp. 411-447.

Tetmeyer, A., and Saiedian, H. 2010. Security threats and mitigating risk for usb devices, *IEEE Technology and Society Magazine* (29:4), pp. 44-49.

Thibaut, J., & Walker, L. (1975). *Procedural justice: a psychological analysis*. Hillsdale: Erlbaum, pp. 50-100.

Trompeter, G. M., Carpenter, T. D., Desai, N., Jones, K. L., and Riley Jr, R. A. 2013. A synthesis of fraud-related research, *Auditing: A Journal of Practice & Theory* (32:sp1), pp. 287-321.

Vaughan, D. (1996). *The Challenger launch decision: Risky technology, culture, and deviance at NASA*. Chicago: University of Chicago Press.

Viator, R. E. 2001. The association of formal and informal public accounting mentoring with role stress and related job outcomes, *Accounting, Organizations and Society* (26:1), pp. 73-93.

Wallace, L., Lin, H., and Cefaratti, M. A. 2011. Information security and sarbanes-oxley compliance: An exploratory study, *Journal of Information Syst*ems (25:1), pp. 185-211.

Walters, L. M. 2007. A draft of an information systems security and control course, *Journal of Information Systems* (21:1), pp. 123-148.

Wang, J., Shan, Z., Gupta, M., and Rao, H. R. 2019. A longitudinal study of unauthorized access attempts on information systems: The role of opportunity contexts, *MIS Quarterly* (43:2), pp. 601-622.

Wang, J., Xiao, N., and Rao, H. R. 2015. Research note—an exploration of risk characteristics of information security threats and related public information search behavior, *Information Systems Research* (26:3), pp. 619-633.

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

Warman, A. R. 1992. Organizational computer security policy: The reality, *European Journal of Information Systems* (1:5), pp. 305-310.

Weick, K. 1969. *Ed 2*. (1979), *The Social Psychology of Organizing*. New York: McGraw-Hill.

Weil, M. M., & Rosen, L. D. (1997). *Technostress: Coping with technology@ work@ home@ play*. New York: Wiley, pp. 29-32.

Weiner, B. 1985. An *Attributional Theory of Achievement Motivation and Emotion*, *Psychological Review* (92:4), p. 548-573.

Wells, J. T. 2002. Occupational fraud: The audit as deterrent, *Journal of Accountancy* (193:4), p. 24-29.

Wells, J. T. (2011). *Corporate fraud handbook: Prevention and detection*. Hoboken, N.J: Wiley.

Wenzel, M. 2005. Motivation or rationalisation? Causal relations between ethics, norms and tax compliance, *Journal of Economic Psychology* (26:4), pp. 491-508.

Wessels, P. 2005. Critical information and communication technology (Ict) skills for professional accountants, *Meditari: Research Journal of the School of Accounting Sciences* (13:1), pp. 87-103.

White, S. 2016. Why your employees are overworked, burnt out, and unmotivated. from https://www.cio.com/article/3097283/why-your-employees-are-overworked-burnt-out-and-unmotivated.html

Wilks, T. J., and Zimbelman, M. F. 2004. Decomposition of fraud-risk assessments and auditors' sensitivity to fraud cues, *Contemporary Accounting Research* (21:3), pp. 719-745.

Willison, R., and Warkentin, M. 2013. Beyond deterrence: An expanded view of employee computer abuse, *MIS Quarterly*, pp. 1-20.

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

Wood, R. E., and Mitchell, T. R. 1981. Manager behavior in a social context: The Impact of impression management on attributions and disciplinary actions, organizational behavior and human performance *Computers in Human Behavior* (28:3), pp. 356-378.

Workman, M., Bommer, W. H., and 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), pp. 2799-2816.

Zhang, Y. 2008. The effects of perceived fairness and communication on honesty and collusion in a multi-agent setting, *The Accounting Review* (83:4), pp. 1125-1146.

Zimmerman, R. D. (2006). *Understanding the impact of personality traits on individuals' turnover decisions*, Dissertation. University of Iowa, pp. 1-90.

Zimmermann, V., and Renaud, K. 2019. Moving from a human-as-problem" to a 'human-as-solution" cybersecurity mindset, *International Journal of Human-Computer Studies* (131), pp. 169-187.

APPENDIX A

SCALE ITEMS

Constructs	Items	Reference
General Work Pressure	GenPress1: Overall, I often feel stressful because of their work. GenPress2: Overall, the work allocated to me makes me feel stressful.	(Stanton et al. 2001)
Rationalization/Idealism	Ideal1: People should make certain that their actions never intentionally harm another even to a small degree. Ideal2: One should never psychologically or physically harm another person. Ideal3: If an action could harm an innocent other, then it should not be done. Ideal4: The dignity and welfare of the people should be the most important concern in any society.	(Forsyth 1980)
Opportunity	Opp1: Having other employee's information systems' credentials is easy. Opp3: Having access to other employees' information systems may provide competitive edge. Opp5: In general, there is an opportunity to exploit the company's information systems.	(Pratt and Cullen 2000)
Work Completion Justification	1. It is alright to violate certain information security policies to get work done quicker. 2. It is alright to violate certain information security policies if it helps you do your job more efficiently. 3. It is alright to violate certain information security policies when you are in a hurry and the work needs to get done	(D'Arcy et al. 2014)

Intentional but non malicious ISP violation intention	**Scenario: USB Copy Scenario** Chris is an accounting employee in your organization and is currently working on a report that requires the analysis of sensitive company financial data. He is extremely busy and wants to continue working on the report later that evening at home. Chris is aware of your company's policy that prohibits users from copying company data to portable media, such as USB drives, to avoid security problems. However, Chris copies several company files to his personal, unencrypted USB drive so that he can work on the report at home. • How likely is it that you would have done the same as Chris in that situation? • I could see myself copying the data as Chris did.	(D'Arcy et al. 2009)

Notes: Data collected from general employees who use a computer for their daily work tasks.

APPENDIX B

ITEM LOADINGS

Item	Factor Loading	AVE **(0.50)**	Composite Reliability **(0.80)**	t-stat.
	General Work Pressure	0.90	0.95	
GenPress1	.96			68.89
GenPress2	.94			55.79
	Rationalization/Idealism	0.71	0.91	
Ideal1	.82			11.78
Ideal2	.88			24.79
Ideal3	.90			28.84
Ideal4	.76			13.50
	Opportunity	0.66	0.85	
Opp1	.83			23.98
Opp2	.82			17.72
Opp3	.78			12.86
	Work Completion Justification	0.91	0.97	
MJ1	.95			54.40
MJ2	.95			81.37
MJ3	.95			62.91
	Intentional ISP Violation	0.87	0.95	
InV1	.98			225.46
InV2	.98			179.56

APPENDIX C

CORRELATIONS AND SQUARED ROOTS OF AVES

	1.	2.	3.	4.	5.
1. ISP Violation Intent	**0.93**				
2. General Pressure	0.28	**0.95**			
3. Opportunity	0.36	0.18	**0.81**		
4. Rationalization/Idealism	-0.24	0.02	-0.17	**0.84**	
5. Moral justification	0.56	0.20	0.41	-0.33	**0.95**

Notes: Square root AVE is shown on the main diagonal.

APPENDIX D

MEASUREMENT OF THE CONSTRUCTS A

Constructs	Measurement
Time point 1: *Perceived ISP control (*Hsu et al., 2015*)*	1. Overall, I perceive high extent of organization controls on our compliance on information security policy (λ = 0.945). 2. Overall, I perceive the organization use all kinds of control mechanisms to force us follow the information security policy (λ = 0.903). **Composite reliability: 0.921; Cronbach's alpha: 0.832; AVE: 0.854**
Time point 1: *ISP Stress (***D'Arcy et al., 2014***)*	**Complexity:** 1. I often find it difficult to understand my organization's information security policies (λ = 0.934). 2. It takes me awhile to understand my organization's information security policies and procedures (λ = 0.864). 3. I sometimes do not have time to comply with my organization's information security policies (λ = 0.869). **Composite reliability: 0.919; Cronbach's alpha: 0.868; AVE: 0.792** **Overload:** 1. I am forced by information security policies and procedures to do more work than I can handle (λ = 0.865). 2. My organization's information security policies and procedures hinder my very tight time schedules (λ = 0.926). 3. I have a higher workload due to increased information security requirements (λ = 0.912). 4. I am forced to change my work habits to adapt to my organization's information security requirements (λ = 0.865). **Composite reliability: 0.940; Cronbach's alpha: 0.914; AVE: 0.796** **Uncertainty:** 1. There are constant changes in information security policies and procedures in my organization (λ = 0.857). 2. There are frequent upgrades to information security procedures in my organization (λ = 0.842). 3. There are always new information security requirements in my job (λ = 0.888). 4. There are constant changes in security-related technologies in my organization (λ = 0.913). **Composite reliability: 0.929; Cronbach's alpha: 0.899; AVE: 0.766**
Time point 1: *ISP violation Opportunity (***Pratt and Cullen, 2000***)*	1. Having other employee's information systems' credentials is easy (λ = 0.926). 2. Having other employee's information systems' credentials is not risky (λ = 0.925). 3. In general, there is an opportunity to exploit the company's information systems (λ = 0.955). **Composite reliability: 0.955; Cronbach's alpha: 0.929; AVE: 0.876**
Time point 1:	1. Risks to another should never be tolerated, irrespective of how

Constructs	Measurement
Idealism ***(*Forsyth, 1980*)***	small the risks might be (λ = 0.867). 2. The existence of potential harm to others is always wrong, irrespective of the benefits gained (λ = 0.877). 3. If an action could harm an innocent other, then it should not be done (λ = 0.830). **Composite reliability: 0.893; Cronbach's alpha: 0.823; AVE: 0.736**
Time point 1: *Work uncertainty* ***(*Colquitt et al., 2012*)***	1. There is a lot of uncertainty at work right now (λ = 0.922). 2. Many things seem unsettled at the organization currently (λ = 0.936). 3. If I think about work, I may feel a lot of uncertainty (λ = 0.914). 4. I cannot predict how things will go at work (λ = 0.784). **Composite reliability: 0.939; Cronbach's alpha: 0.912; AVE: 0.794**
Time point 1: *ISP self-efficacy* ***(Compeau and Higgins, 1995)***	***I could complete my job using technology and follow the ISP requirements if:*** 1. There was no one around to tell me what to do (λ = 0.793). 2. I had never used a software package like it before (λ = 0.840). 3. I had only the software manuals for reference (λ = 0.920). **Composite reliability: 0.888; Cronbach's alpha: 0.820; AVE: 0.727**
Time point 2: *Intentional ISP violation intention* ***(*Willison and Warkentin, 2013*)***	***Please indicate the extent to which you agree or disagree with the following statements.*** ***Someone like you working at a company may feel:*** 1. All things considered, it is high likely that one might carry out **intentional but not malicious** ISP violation (such as not changing password regularly, delayed backup, bring materials back home et al.) in the future (λ = 0.891). 2. Depending on situation, the possibility that one will carry out **intentional but not malicous** ISP violation (such as not changing password regularly, delayed backup, bring materials back home et al.) in the future is high (λ = 0.907). 3. One will often conduct **intentional but not malicious** ISP violation (such as not changing password regularly, delayed backup, bring materials back home et al.) in the future (λ = 0.889). **Composite reliability: 0.924; Cronbach's alpha: 0.877; AVE: 0.803.**

Note: λ is the item factor loadings.

APPENDIX E

MEASUREMENT OF THE CONSTRUCTS B

Table 2

Measurement of the Constructs

Constructs	Measurement
*ISP pressure (*D'Arcy et al., 2014*)*	1. Overall, I feel high pressure because of requirements information security policy (λ = 0.917). 2. Overall, the requirements of information security policy make me often feel stressful (λ = 0.944). 3. Overall, the requirements of information security policy won't add stress to me (λ = 0.771). **Composite reliability: 0.929; Cronbach's alpha: 0.900; AVE: 0.765**
Displacement of responsibility **(Chong and Wang 2019; D'Arcy et al. 2014))**	1. Employees cannot be blamed violating information security policies if they are overloaded with work tasks (λ = 0.919). 2. If management believed all information security policies were all important, they would have put place better controls (λ = 0.850). 3. Employees cannot be blamed violating certain information security policies because it is difficult to get the job done otherwise (λ = 0.900). **Composite reliability: 0.920; Cronbach's alpha: 0.868; AVE: 0.792**
Diffusion of responsibility **(Chong and Wang 2019; D'Arcy et al. 2014))**	1. An employee cannot be blamed for violating certain information security policies because many factors contribute to this action (λ = 0.929). 2. It is unfair to blame one employee for violating certain information security policies when many others do the same (λ = 0.933). 3. It is unfair to blame one employee for sharing a password because he/she has limited responsibility for information security (λ = 0.929). **Composite reliability: 0.951; Cronbach's alpha: 0.922; AVE: 0.866**
Perceived distributive justice **(Li et al. 2014; Sindhav et al. 2006)**	1. The increase in the security of my computer and data is worth the inconvenience or other loss that I may suffer from restricting non-work-related Internet usage (λ = 0.767). 2. The increase in my productivity is worth the inconvenience or other loss that I may suffer from restricting nonwork-related Internet usage (λ = 0.764). 3. The potential improvement in my performance evaluation is likely to compensate for the inconvenience or other loss that I may suffer from restricting non-work-related Internet usage (λ = 0.985). **Composite reliability: 0.939; Cronbach's alpha: 0.912; AVE: 0.794**
Perceived Procedural justice **(Li et al. 2014; Sindhav et**	1. The security procedures for detecting and punishing non-work-related Internet usage are applied in a fair manner to everyone in my organization (λ = 0.773). 2. The security procedures for detecting and punishing non-work-related Internet usage are applied consistently to everyone in my organization (λ = 0.958).

Constructs	Measurement
al. 2006)	3. The security procedures for detecting and punishing non-work-related Internet usage are designed fairly in my organization (λ = 0.924). **Composite reliability: 0.881; Cronbach's alpha: 0.875; AVE: 0.715**
Intentional ISP violation intention ***(*Willison and Warkentin, 2013*)***	***Please indicate the extent to which you agree or disagree with the following statements.*** ***Someone like you working at a company may feel:*** 4. All things considered, it is high likely that one might carry out **intentional** ISP violation (such as (such as not changing password regularly, delayed backup, bring materials back home et al.)) in the future (λ = 0.893). 5. Depending on situation, the possibility that one will carry out **intentional** ISP violation (such as not changing password regularly, delayed backup, bring materials back home et al.) in the future is high (λ = 0.897). 6. One will often conduct **intentional** ISP violation (such as not changing password regularly, delayed backup, bring materials back home et al.) in the future (λ = 0.881). **Composite reliability: 0.920; Cronbach's alpha: 0.870; AVE: 0.793**

Note: λis the item factor loadings.

APPENDIX F

HUMAN USE APPROVAL LETTER

LOUISIANA TECH
UNIVERSITY

MEMORANDUM

OFFICE OF SPONSORED PROJECTS

TO: Ms. Randi Jiang, Dr. Jae Ung Lee and Dr. Selwyn Ellis

FROM: Dr. Richard Kordal, Director of Intellectual Property & Commercialization (OIPC)
rkordal@latech.edu

SUBJECT: HUMAN USE COMMITTEE REVIEW

DATE: January 25, 2019

In order to facilitate your project, an EXPEDITED REVIEW has been done for your proposed study entitled:

"The Role of the Fraud Triangle in Information Security Effectiveness"

HUC 19-065

The proposed study's revised procedures were found to provide reasonable and adequate safeguards against possible risks involving human subjects. The information to be collected may be personal in nature or implication. Therefore, diligent care needs to be taken to protect the privacy of the participants and to assure that the data are kept confidential. Informed consent is a critical part of the research process. The subjects must be informed that their participation is voluntary. It is important that consent materials be presented in a language understandable to every participant. If you have participants in your study whose first language is not English, be sure that informed consent materials are adequately explained or translated. Since your reviewed project appears to do no damage to the participants, the Human Use Committee grants approval of the involvement of human subjects as outlined.

Projects should be renewed annually. ***This approval was finalized on January 25, 2019 and this project will need to receive a continuation review by the IRB if the project continues beyond January 25, 2020.*** **ANY CHANGES** to your protocol procedures, including minor changes, should be reported immediately to the IRB for approval before implementation. Projects involving NIH funds require annual education training to be documented. For more information regarding this, contact the Office of Sponsored Projects.

You are requested to maintain written records of your procedures, data collected, and subjects involved. These records will need to be available upon request during the conduct of the study and retained by the university for three years after the conclusion of the study. If changes occur in recruiting of subjects, informed consent process or in your research protocol, or if unanticipated problems should arise it is the Researchers responsibility to notify the Office of Sponsored Projects or IRB in writing. The project should be discontinued until modifications can be reviewed and approved.

Please be aware that you are responsible for reporting any adverse events or unanticipated problems.

APPENDIX G

SURVEY INSTRUMENTS

Survey Instruments

General Work Pressure Scale (Stanton et al., 2001)

1. Overall, I often feel stressful because of their work.
2. Overall, the work allocated to me makes me feel stressful.
3. Overall, my work won't stress me out.

Rationalization/Idealism Scale (Forsyth, 1980)

1. People should make certain that their actions never intentionally harm another even to a small degree.
2. Risks to another should never be tolerated, irrespective of how small the risks might be.
3. The existence of potential harm to others is always wrong, irrespective of the benefits gained.
4. One should never psychologically or physically harm another person.
5. One should not perform an action which might in any way threaten the dignity and welfare of another individual.
6. If an action could harm an innocent other, then it should not be done.
7. Deciding whether or not to perform an action by balancing the positive consequences of the act against the negative consequences is immoral.
8. The dignity and welfare of the people should be the most important concern in any society.

Information Security Policy Violation Opportunity Scale (Pratt and Cullen, 2000)

1. Having other employee's information systems' credentials is easy.
2. Using other employees' workstations that was unlocked is not difficult.
3. Having other employee's information systems' credentials is not risky.
4. Overcoming company's information systems protection is considered as an unsafe activity.
5. Having access to other employees' information systems may provide competitive edge.
6. Having access to other employee's information systems may enhance effectiveness of the job.
7. In general, there is an opportunity to exploit the company's information systems.

Work Completion Justification Scale (Bandura et al., 1996)

1. It is alright to violate certain information security policies to get work done quicker.
2. It is alright to violate certain information security policies if it helps you do your job more efficiently.
3. It is alright to violate certain information security policies when you are in a hurry and the work needs to get done

Perceived Information Security Policy Control Scale (Hsu et al., 2015)

1. Overall, I perceive high extent of organization controls on our compliance on information security policy.
2. Overall, I perceive the organization use all kinds of control mechanisms to force us follow the information security policy.
3. Overall, I feel lack of controls my organization adopt to force us comply with information security policy.

Information Security Policy General Pressure Scale (D'Arcy et al., 2014)

1. Overall, I feel high pressure because of requirements information security policy.
2. Overall, the requirements of information security policy make me often feel stressful.
3. Overall, the requirements of information security policy won't add stress to me.

Information Security Policy Stress Scale (D'Arcy et al., 2014)

A. Complexity

1. I sometimes feel pressure in my job due to information security requirements.
2. I find that new employees often know more about information security than I do.
3. I do not know enough about information security to comply with my organization's policies in this area.
4. I often find it difficult to understand my organization's information security policies.
5. It takes me awhile to understand my organization's information security policies and procedures.
6. I sometimes do not have time to comply with my organization's information security policies.

B. Overload

1. I am forced by information security policies and procedures to do more work than I can handle.
2. My organization's information security policies and procedures hinder my very tight time schedules
3. I have a higher workload due to increased information security requirements.
4. I am forced to change my work habits to adapt to my organization's information security requirements.

C. Uncertainty

1. There are constant changes in information security policies and procedures in my organization.
2. There are frequent upgrades to information security procedures in my organization.
3. There are always new information security requirements in my job.
4. There are constant changes in security-related technologies in my organization.

Work Uncertainty Scale (Colquitt et al., 2012)

1. There is a lot of uncertainty at work right now.
2. Many things seem unsettled at the organization currently.
3. If I think about work, I may feel a lot of uncertainty.
4. I cannot predict how things will go at work.

Information Security Policy Self Efficacy Scale (Compeau and Higgins, 1995)

1. I could complete my job using technology if:
2. There was no one around to tell me what to do.
3. I had never used a software package like it before.
4. I had only the software manuals for reference.
5. I had seen someone else using it before trying it myself.
6. I could call someone for help if I got stuck.
7. I had a lot of time to complete the job for which the software was provided.
8. I had just the built-in help facility for assistance.
9. Someone showed me how to do it first.
10. I had used similar software packages like this one before to do my job.

Intentional Information Security Policy Violation Scale *(*Willison and Warkentin*,* 2013*)*

1. All things considered, it is high likely that one might carry out intentional ISP violation (such as (such as not changing password regularly, delayed backup, bring materials back home et al.)) in the future.
2. Depending on situation, the possibility that one will carry out intentional ISP violation (such as not changing password regularly, delayed backup, bring materials back home et al.) in the future is high.
3. One will often conduct intentional ISP violation (such as not changing password regularly, delayed backup, bring materials back home et al.) in the future.

Displacement of Responsibility Scale (Chong and Wang, 2019; D'Arcy et al., 2014))

1. Employees cannot be blamed violating information security policies if they are overloaded with work tasks.
2. If management believed all information security policies were all important, they would have put place better controls.
3. Employees cannot be blamed violating certain information security policies because it is difficult to get the job done otherwise.

Diffusion of Responsibility Scale (Chong and Wang, 2019; D'Arcy et al., 2014))

1. An employee cannot be blamed for violating certain information security policies because many factors contribute to this action.
2. It is unfair to blame one employee for violating certain information security policies when many others do the same.
3. It is unfair to blame one employee for sharing a password because he/she has limited responsibility for information security.

Perceived Distributive Justice Scale (Li et al., 2014; Sindhav et al., 2006)

1. The increase in the security of my computer and data is worth the inconvenience or other loss that I may suffer from restricting non-work-related Internet usage.
2. The increase in my productivity is worth the inconvenience or other loss that I may suffer from restricting nonwork-related Internet usage.
3. The potential improvement in my performance evaluation is likely to compensate for the inconvenience or other loss that I may suffer from restricting non-work-related Internet usage.

Perceived Procedural Justice Scale (Li et al., 2014; Sindhav et al., 2006)

1. The security procedures for detecting and punishing non-work-related Internet usage are applied consistently to everyone in my organization.
2. The security procedures for detecting and punishing non-work-related Internet usage are applied in a fair manner to everyone in my organization.
3. The security procedures for detecting and punishing non-work-related Internet usage are designed fairly in my organization

Intentional but non-malicious ISP Violation Intention Scale (Scenario USB Copy) (D'Arcy et al., 2014)

USB Copy Scenario

Chris is an accounting employee in your organization and is currently working on a report that requires the analysis of sensitive company financial data. He is extremely busy and wants to continue working on the report later that evening at home. Chris is aware of your company's policy that prohibits users from copying company data to portable media, such
as USB drives, to avoid security problems. However, Chris copies several company files to his personal, unencrypted USB drive so that he can work on the report at home.

1. How likely is it that you would have done the same as Chris in that situation?
2. I could see myself copying the data as Chris did.
3. I won't do the same as Chris in that situation
4. It is morally unacceptable to do what Chris did in that situation.
5. It is against my moral belief to do what Chris did in that situation.
6. Certainty of Punishment Scale
    - What is the likelihood that an employee violating information security policies would be formally punished?
    - An employee would be reprimanded at some point for violating information security policies.
7. Severity of Punishment Scale
    - If punished, how severe would the employee's punishment be?
    - An employee would receive harsh sanctions for violating information security policies.
8. Celerity of Punishment Scale
    - If punished, an employee's punishment would be immediate.

If punished, an employee's punishment would be timely