Pacific Asia Journal of the Association for Information Systems

ISSN 1943-7544

Research Paper doi: 10.17705/1pais.14404 Volume 14, Issue 4 (2022)

Exploring Employees' Computer Fraud Behaviors using the Fraud Triangle Theory

Randi Jiang
Seidman College of Business Grand Valley State University, USA, jiangr@gvsu.edu

Abstract

Background: *Employee computer fraud is a costly and significant problem for firms. Using the fraud triangle theory, this study explores the extent to which an employee's perception of opportunity, rationalization, and work pressure will contribute to their likelihood of committing computer fraud (i.e., intentional, malicious, or while motivated through a self-interest gain of information systems (IS) security policy non-compliance behaviors).*

Method: *A model is proposed and empirically validated through survey data collected from various industries from 213 computer-using employees with financial responsibilities within their organizations in the U.S.*

Results: *This study's findings suggest when individual employees experience high levels of work pressure, they may be more likely to commit computer fraud. Organizations can guard against this behavior by monitoring their employees' assigned workload and performance expectations to prevent these unwanted behaviors. This study demonstrates a need for future research to investigate further the motivations employees may have besides financial greed when committing different types of computer abuse behaviors.*

Conclusion: *This study, based upon the fraud triangle theory, empirically reveals the importance of monitoring general work pressure to guard against employees committing computer fraud behaviors. Computer fraud behaviors should be considered a distinct type of information security violation behavior.*

Keywords: Fraud Triangle, Opportunity, Rationalization, Pressure, Computer Fraud.

This research article was submitted on Sep-2020 and under two revisions, accepted on Oct-2021.

Citation: Jiang, R. (2022). Exploring Employees' Computer Fraud Behaviors using the Fraud Triangle Theory. *Pacific Asia Journal of the Association for Information Systems, 14*(4), 100-121. https://doi.org/10.17705/1pais.14404

Introduction

As information technology (IT) brings unprecedented advances in communication for all users, it also offers greater reach for criminal activities (Ahmed et al., 2019). Undesirable employee security-related behaviors have been conceptualized in the information systems security (ISS) literature into two broad categories (Hu et al., 2011; Moody et al., 2018; Straub & Welke, 1998; Willison & Warkentin, 2013). Employee ISS violations may be entirely unintentional and non-malicious such as accidental data entry, failing to log off when away from the computer, and delaying backup (Stanton et al., 2005). At the other end of the spectrum is insiders' malicious and intentional misuse of computers (Willison & Warkentin, 2013; Willison et al., 2018). These particular employees are motivated by personal gain; however, the gain is at an organization's expense. This behavior is termed computer abuse, defined in this study as the unauthorized and deliberate misuse of computers inconsistent with accepted business practices (Straub & Nance, 1990). Interestingly, according to a 2020 Insider threat report, the types of insider risk threats have rose by 47% since 2018, causing over $10 million USD to be spent to resolve insider-related incidents (Ponemon Institude, 2020). Over the last decade, among other computer abuse behaviors observed, a growing number of companies have encountered computer fraud (Bissell et al., 2019) as the unauthorized and deliberate misuse of the employing organization's resources or assets for deception and misappropriation of assets. For example, employees have used accounting information systems to violate individual privacy, misappropriate assets, and falsify sensitive data (Cooper, 2009). Existing information systems (IS) security documents have traditionally focused on examining general security non-compliance behaviors. Unfortunately, the specific phenomenon of employee computer fraudulent behavior has not received its deserved attention yet, even though there have been recent calls for more research focus on this phenomenon (Chatterjee et al., 2015; Crossler et al., 2013; Willison et al., 2018).

Organizational management has found it challenging to answer the following question: "What can organizations do to aid in the prevention of IS violation activities?" Researchers have argued that the effectiveness of an information security policy (ISP) would be dependent upon the specific motivations of the employee as well as the deterrence in place towards conducting the specific ISP violation behaviors (Hu et al., 2011; Straub & Nance, 1990; Willison & Warkentin, 2013). Past studies have explored possible motivations for employees to engage in these malicious computer fraud behaviors. In the extant ISS literature, IS researchers have employed the use of several theories to explore the effects of ISP compliance, precisely that of non-malicious behavior (D'Arcy et al., 2009; Herath & Rao, 2009; Moody et al., 2018; Myyry et al., 2009). For example, studies have examined these non-malicious behaviors under the organizational justice theory, deterrence theory, and the techniques of neutralization. Organizational justice theory explains how perceptions of fairness or unfairness are created within an organizational context (Leventhal et al., 1980; Willison et al., 2018). Individuals who feel that their employer has been unfair will be more likely to engage in computer abuse behavior. Expanding upon the perceptions of fairness, researchers have examined deterrence theory to see what preventative measures organizations can employ. These studies observed procedural and technical countermeasures as deterrent mechanisms by increasing the perceived certainty, severity, and celerity of punishment for IS misuse (D'Arcy et al., 2009). The neutralization theory explains how individuals can overcome social norms and deterrent mechanisms which ultimately lead to individuals engaging in deviant behaviors (Siponen & Vance, 2010; Sykes & Matza, 1957). These theories have provided insights into our understanding of those intentional but non-malicious computer ISP violations. However, there is little guidance in understanding the motivations and reasoning behind why employees perform intentional and deceptive behavior to extract value from an organization (e.g., computer fraud).

In order to examine the intentional and malicious ISS non-compliance behaviors (e.g., computer fraud), this study follows the audit standards used in the worldwide public company

https://aisel.aisnet.org/pajais/vol14/iss4/4
DOI: 10.17705/1pais.14404

accounting oversight board (PCAOB, 2002), which describe three factors that supposedly predict the likelihood of fraud within an organization. The fraud triangle is unique to the ISS realm, as the theory is used initially to explain intentional fraud. Together, known as the fraud triangle, these three factors are opportunity, pressure, and rationalization. The opportunity arises for computer fraud when there is an absence of controls, ineffective controls, or the ability to override controls. General work pressure may give employees an incentive to commit fraud. For example, when employees perceive a general work pressure to report better results rather than their actual performance or are unable to complete their daily tasks due to unreasonable work deadlines heightening their general work pressures. Rationalization (i.e., change in attitude) to commit computer fraud happens when individuals consciously decide to use technology to present fraudulent or misrepresented information for personal gain (e.g., asset misappropriations). Studies have found that the three dimensions of the fraud triangle are all critical in explaining the likelihood of fraudulent behavior in an organization (Mui & Mailley, 2015; Sujeewa et al., 2018). An opportunity to commit fraud was found to be the necessary condition (Schuchter & Levi, 2016); however, financial pressure was found to be most significant in the accountants' fraud behaviors (Manurung & Hadian, 2013; Skousen et al., 2009). In the context of general computer fraud behaviors, we argue that general work pressure is the most critical factor. Therefore, this study proposes a computer fraud triangle model to explore the research question "will all three elements of the fraud triangle exposed to an individual be equally important to predict the likelihood of computer fraud behaviors of general employees using an organization's IS?"

To answer the research question, we develop and test a model that evaluates the fraud triangle elements' impact on computer fraud intention of general IS users. Based upon a survey of 213 computer-using employees with financial responsibilities within their organizations in the U.S., the results show that opportunity and pressure are significantly positively related to computer fraud intention. The result of this study provides a deeper insight into the understanding of employees' computer fraud behaviors. First, it expands the existing ISP violation behaviors literature by focusing on IS users' computer fraud behaviors. Second, the results show employees' computer fraud behaviors are driven by general perceived work pressure from the organization, confirming and extending our understanding of fraud triangle theory application in the context of computer non-compliance behaviors.

In the following sections, this study outlines the previous research on computer fraud and system security. This study then presents the theoretical model to examine the fraud triangle related to the intention of committing computer fraud and present the hypotheses. Subsequently, followed by the description of the model discussion Partial Least Square (PLS) was employed for data analysis. Lastly, there will be a discussion of the findings, contributions, implications, limitations, and future directions for research.

Literature Review

IS users in an organization have been considered the weakest link for an organization's information security, especially dealing with computer systems integrating into the business process operation (Spears & Barki, 2010; Wang et al., 2015; Warkentin & Willison, 2009). As the complexity of these systems grows, organizations risk having their systems compromised by both intentional and unintentional acts of organization insiders (Maynard et al., 2018). Intentional and harmful acts have generally been classified as computer abuse (Willison & Warkentin, 2013); however, not all computer abuse can be classified as computer fraud. Table 1 highlights the main differences between the three main classifications of ISS violations.

Table 1 – Comparison of Computer Fraud and Other Security Behavior Concepts

Concepts	Definitions	Examples	References
Unintentional IS violations	Unintentional, not malicious, and no self-interest/financial gain	Accidental data entry	(Loch et al., 1992)
Intentional but non-malicious IS violations	Intentional, non-malicious, and no self-interest/financial gain	Copying sensitive data to USB drives, Password sharing, Failure to log off the computer	(Siponen & Vance, 2010)
Intentional and malicious IS violations (with no self-interest or financial gain)	Motivated with no self-interest/financial gain	writing viruses, software piracy	(Vasiu & Vasiu, 2004)
Intentional and malicious IS violations (i.e. Computer Fraud)	Motivated with self-interest/financial gain	Revealing confidential information to outsiders, Deleting or altering records and files to create false information for misappropriation of assets (i.e., manipulation of data through the use of computers)	(D'Arcy et al., 2009; Haugen & Selin, 1999; Vasiu & Vasiu, 2004)

ISS literature has focused heavily on the intentional but non-malicious violations with an emphasis on three main countermeasures: security education, training, and awareness (SETA) programs, fear appeal, and system monitoring (D'Arcy et al., 2009; Hsu et al., 2015; Johnston & Warkentin, 2010). SETA enhances users' risk awareness of their behavior and their capacity for technology threat avoidance, which is considered a valuable measure for coping with unintentional ISP violation behaviors (Tsohou et al., 2015). For these SETA programs, a significant theory behind it is that an organization's code of conduct influencing their SETA programs clarify responsibility and deter unethical behavior (Harrington, 1996; Myyry et al., 2009). Along with an organization's SETA program, sanctions and monitoring are also effective in responding to intentional but non-malicious violation behavior (Chatterjee et al., 2015). Using unethical programming behavior to represent this type of behavior, Sojer et al. (2014) discovered that informing developers of organizational repercussions to unethical programming was more effective than other deterrence methods. As such, deterrence theory has been heavily applied to investigate the effects of organizational deterrent measures on employee computer misuse (D'Arcy et al., 2009; Herath & Rao, 2009; Hu et al., 2011; Sojer et al., 2014). Although these studies and related theories have provided valuable insights into understanding the ISP violation behaviors, they did not provide guidance or explanation of computer fraud as one specific intentional and malicious behavior for two reasons. First, one common assumption for these studies is that employees will not commit a crime because the imposed severity of sanctions on information systems misuse might not hold in the context of computer fraud (D'Arcy et al., 2009). Second, countermeasures such as the SETA program, fear appeal, and system monitoring have been found to increase employees' work stress and further increase their intention for violations (D'Arcy et al., 2014). Computer fraud behaviors may be a consequence led by general work pressure placed upon employees by the organization.

In summary, despite the growing interest and research efforts in studying computer abuse-related behaviors in the ISS literature, some critical questions remain unanswered. Table 2 summarizes the theories examined in ISS literature relating specifically to computer fraud

https://aisel.aisnet.org/pajais/vol14/iss4/4
DOI: 10.17705/1pais.14404

behavior. The fraud triangle theory specifically takes a holistic point of view from the employee's perspective, providing both individuals and organizational factors to understand its influence on one's intent to commit computer fraud. The understanding of the motivational factors for end-users to engage in computer fraud is still limited. Therefore, this study aims to fill this research gap by proposing and empirically testing a computer fraud intention model based on the fraud triangle theory.

Table 2 – Theories Explored

Theory	Context of Computer Abuse	References
Organizational Justice Theory	Employee's incentive to commit computer abuse will be impacted by their perception of their organizational justice/fairness	(Colquitt et al., 2001; Willison et al., 2018)
Deterrence Theory	Employee's intention to commit computer abuse will be deterred through an organization's certainty, severity, and celerity of their information security policies	(D'Arcy & Herath, 2011; Hoffer & Straub, 1989)
Neutralization Theory	Employees may engage in neutralization techniques to dissuade their feelings of guilt and shame when committing violations towards their organization	(Siponen & Vance, 2010)
Fraud Triangle Theory	Employee's level of opportunity, pressure, and ability to rationalize their actions can influence their motivation to commit fraudulent acts	(Cressey, 1953; Dorminey et al., 2012)

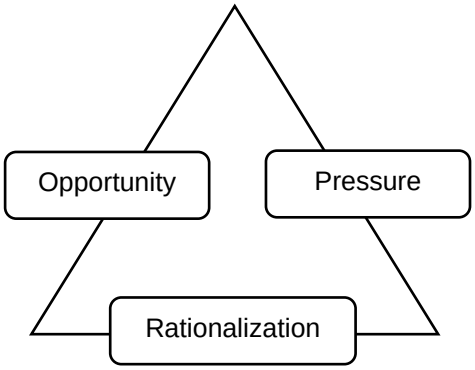
Theoretical Development

The fraud triangle literature has slowly multiplied over the last decade, and its concepts have been gradually applied to a wide array of disciplines. 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 (ACFE, 2018). Anti-fraud efforts have attracted the attention of professionals, including but not limited to internal and external auditors, members of boards of directors, management, and regulators. 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 the 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).

In the context of computer abuse, the fraud triangle theory gives this study a theoretical framework solely dependent on the employee's perception. The first point of the triangle discussed is the incentive to commit fraud. Management may have an incentive or are under pressure, which serves as a motivating factor to commit fraudulent acts against the organization. Second, circumstances exist, and these employees are placed in a position of trust within an organization—for example, the absence of controls and ineffective controls, creating a perception of opportunity. Perceived opportunity is the perception that a control weakness is present and, most importantly, the likelihood of being caught is remote. Thus, perceived opportunity requires the ability to commit the act and to do so without detection (Hollinger & Clark, 1983). Third, those involved in committing fraud 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. These rationalizations an employee may undergo will neutralize their conduct whether it violates their computer

privileges or not. Despite the intention of an otherwise honest individual, any individual can commit fraud in an environment that imposes sufficient pressure or incentives. Rationalization is an attempt to reduce the cognitive dissonance within the individual (Ramamoorti, 2008; Ramamoorti et al., 2009). The greater the incentive or pressure, the more likely an individual will rationalize the acceptability of committing fraud. The more excellent 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 1. This model highlights how an individual may separate the perpetration of the crime from the criminal act through these factors. As organizations continue to become technologically advanced, employees continually rely on computers for their daily tasks. Previous research has shown, individuals may participate in occupational fraud by using a computer (Guragai et al., 2017). Systems legitimize individual wrongdoing by allowing people to focus on their duties within the system without considering the moral impact of their actions (Adams & Balfour, 2014).



Adapted from Kassem and Higson (2012)

Figure 1 – The Fraud Triangle

Opportunity

Scholars increasingly recognize that individual users play a crucial role in the security of information systems (Furnell & Clarke, 2012; Willison & Warkentin, 2013). This is because users often represent the weakest link in the security of the organization's system—if a user can be persuaded into breaking information security policies, the security of an entire system can be compromised (Siponen & Vance, 2010). The status of users as the weakest link in the security chain is fully recognizable by both internal and external users; therefore, individuals continually find creative ways to avert technical security controls (Abraham & Chengalur-Smith, 2010; Vance et al., 2014). Given this reality, researchers and practitioners must understand how users perceive and respond to information security risk opportunities.

Opportunity in the entrepreneurship literature was defined as "alertness to changed conditions or overlooked possibilities" (Kirzner, 1979). In this study, we define opportunities for computer fraud as a perceived 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). These studies revealed employees were not proactive in preventing security threats unless eminent fear of sanctions were placed upon them. 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

https://aisel.aisnet.org/pajais/vol14/iss4/4
DOI: 10.17705/1pais.14404

action could lead to benefits (ex: profit, convenience, promotions, and other forms of individual or organization gain) (Shepherd et al., 2007).

Rationalization

In the investigative context of this study, we build rationalization from Forsyth's ethical beliefs: idealism and relativism (Forsyth, 1980). Forsyth (1980) defines idealism as the degree to which individuals assume that desirable consequences can always be obtained when making the "right" action, while relativism is the extent to which an individual rejects moral rules when making an ethical decision. Both dimensions are important as they have shown to be related to individuals' ethical decision-making (Godos-Díez et al., 2015). However, in the context of computer fraud, the focus is to gauge an individual's level of idealism which encompasses one's rationalization to obtain desirable consequences through their actions. This study examines an individual's level of idealism as their individual level of belief of how 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, unethical behaviors such as improper data input result in decreased an organization's revenues. Hence, it can be assumed that individuals with a high level of technological idealism would tend to have a negative attitude toward computer fraud behavior. Therefore, our interpretation of an individual's level of idealism will be represented by how an employee using an organization's IS will rationalize their decision making when committing computer fraud.

Work Pressure

The pressure part of the fraud triangle is construed as general work-related pressure (Cavanaugh et al., 2000; Ganster & Schaubroeck, 1991; Stanton et al., 2001). The U.S. audit standard describes it as "employees have an incentive or are under pressure, which provides a reason to commit fraud" (PCAOB, 2002). Employees may perceive large amounts of general work pressure when faced with the need to report better results than actual performance (Albrecht et al., 2008). General work pressure may lead to employees deliberately disregarding ISPs due to unreasonable deadlines to finish their assigned work. Employees may also experience frustration with work procedures, and therefore need to circumvent internal controls to complete their duties on time. General work-related pressure can manifest as signs of job dissatisfaction, burnout, accidents, loss of productivity, absenteeism, and turnover. Therefore, employees who face unreasonable work deadlines or are given many responsibilities with unmanageable expectations are considered to be under general work-related pressure.

Previous research has shown that an employee's informal social learning environment can directly influence an employee's efficacy levels (Gist & Mitchell, 1992; Mathieu et al., 1993; Warkentin et al., 2011). Evidence contends that resources provided by a company in support of desired security behaviors among their employees will influence the level of employee confidence towards information security compliance responsibilities (Leach, 2003). Table 3 presents the definitions of the fraud triangle element characteristics and the other constructs used in this study.

Table 3 – Constructs Used in This Study

Construct Name	Definition	Source
Independent Variables		
Opportunity	The extent to which circumstances exist when there is an absence of controls, ineffective controls, or the ability to override control.	(PCAOB, 2002)
Idealism	The extent to which individuals believe that any technology-related action should maximize the good without harming another.	(Chatterjee et al., 2015; Forsyth, 1980)
General Work-Related Pressure	The extent to which a job involves employees perceiving general work pressure (i.e., dissatisfaction, loss of productivity)	(Sauter & Murphy, 1995; Stanton et al., 2001)
Dependent Variable		
Intention to commit Computer Fraud	The extent to which an employee will engage in fraudulent behavior connected with computerization, someone intends to gain a dishonest advantage.	(Vanasco, 1998)

There is a growing body of academic security literature with an emphasis on behavioral security issues (Siponen & Vance, 2010; Spears & Barki, 2010; Warkentin & Willison, 2009; Willison & Warkentin, 2013). By merging the issues examined in the ISS literature with the specific risk of computer fraud, this study links numerous factors, including organization sanctions, individual dispositions, and security-related attitudes and beliefs.

Hypothesis Development

The research model leverages the logic articulated in prior sections of this paper and existing research. After reviewing the components of the fraud triangle, computer fraud suggests that when employees perceive higher components of the fraud triangle, the more significant the intention to commit computer fraud will be.

The first component of the fraud triangle is opportunity. The U.S. audit standard defines opportunity as "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, 2002). Opportunities for the commission of fraudulent acts are likely to manifest themselves when employees sense that they might be safely able to use their credentials to circumvent internal IT security controls for purposes of committing computer fraud (Nakayama & Chen, 2019). Perceived opportunity is the perception (1) that a control weakness is present, and more 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 (Dorminey et al., 2012). Because one can perceive opportunities within an organization at any given point, the following hypothesis has been drawn out:

H1: Opportunity is positively associated with the likelihood of committing computer fraud.

The second component of the fraud triangle is rationalization. Rationalization happens when individuals who commit fraud desire to do so without incurring negative self-perceptions; they will typically seek to rationalize their fraudulent actions to themselves (Dorminey et al., 2012). In 1989, Sharp, an early psychologist interested in moral judgment, examined individual variations in approaches to moral judgment. This study focuses on the second significant dimension of moral judgment, which focuses on idealism in one's moral attitudes (Forsyth, 1980). Because one can rationalize or attempt to self-justify their actions to commit computer fraud, the following hypothesis has been drawn out:

H2: Idealism is negatively associated with the likelihood of committing computer fraud.

https://aisel.aisnet.org/pajais/vol14/iss4/4
DOI: 10.17705/1pais.14404

The third component of the fraud triangle is perceived pressure. The subject of unwanted pressure has been covered in the organizational and psychological literature (Hay & Gray, 1974; Rodell & Judge, 2009). This study offers a different avenue for understanding an employee's intent to commit computer fraud—namely, general work-related pressure. General work-related pressure manifests when employees are applying self-pressure to meet their work deadlines or complete their assigned duties. This 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 from 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 continually adjust to new requirements with little time to develop a normalized work routine. General 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 of committing computer fraud.

The resulting research model is illustrated in Figure 2.

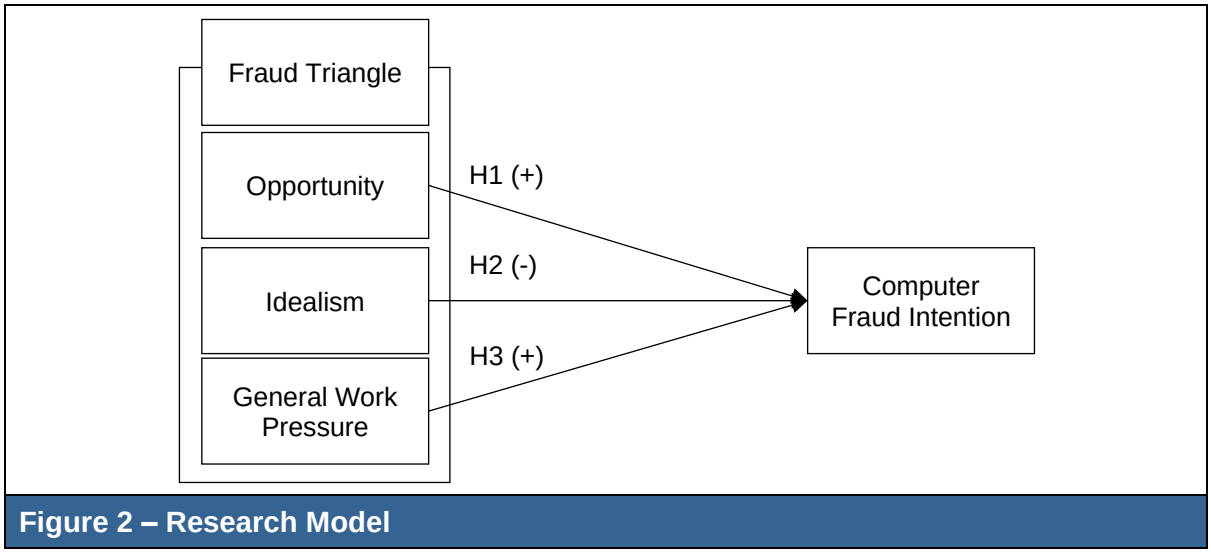


Figure 2 – Research Model

Research Methodology

Because our model incorporates socially undesirable constructs, making it difficult to find organizations that are willing to have their employees partake in such a study. For this reason, we used a market research firm to invite participants to our study, which was described as a study of daily general work feelings about their job. We instructed the firm to recruit employed, computer-using professionals knowledgeable of their organization's ISPs, and specifically given financial responsibilities from their organization located within the United States. Upon viewing the email invitation, participants are given detailed instructions on the study. These instructions contained strong language that emphasized the time commitment involved and the socially undesirable scenarios they will come across regarding computer fraud.

Participants were paid a small honorarium for taking part in the study. 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 the study. Panels guarantee

respondent anonymity and encourage honest responses to questions that may be subject to socially desirable responses, such as those related to computer fraud. Given the difficulty of measuring ethical and anti-social behaviors, we used hypothetical wording that encourages research participants to be less likely to hide their real intentions and reactions in response to the socially undesirable questions (Trevino, 1992).

According to available statistics, 574-panel members accepted the invitation to participate in the survey by viewing the consent agreement and clicking past the first page. Of the 361 respondents eliminated, 87 were eliminated based on a response of "no" to a question asking whether they were aware of what constituted an ISP in their organization (Bulgurcu et al., 2010). The remaining 274 participants were eliminated either because of response set biases (i.e., answers exhibiting certain unlikely patterns, such as all 5s, or the survey completed in an unreasonably short amount of time). This resulted in a final sample of 213 participants. Table 4 shows additional demographics for these respondents.

The measurement items in the questionnaire were adapted from existing validated and well-tested scales in the extant literature. These scales had been proved to have good validity and reliability. All scales used in the study are presented in Appendix A. All items were measured with 5-point Likert scales in the questionnaire, ranging from "strongly disagree" to "strongly agree." Respondents received a series of questions designed to measure opportunity, general work-related pressure, idealism, the perceived cost of following information security policies, and the likelihood of committing computer fraud.

In addition to perceptions of opportunity, general work pressure, and levels of idealism within an individual, it is recognized that the behavioral intention to commit computer fraud might also be influenced by respondents' characteristics such as age, gender, education, accounting responsibilities, and perception of monitoring within an organization. Workplace training may give employees the skills to commit computer fraud within the organization's information system. Therefore, we adopt a generalized with one item for employees to consider the computer skillset for employees who may consider committing computer fraud (Parker, 1998). The examination of the control variables and their influence on computer fraud intentions revealed that none of these significantly influenced how employees may formulate their intentions to commit computer fraud.

Table 4 – Sample distribution by classification

Gender	Count	Ethnicity	Count	Education	Count
Female	122	Caucasian	185	High-school	33
Male	91	Black/ African	6	2 year degree	33
		Pacific Islander	17	4 year degree	82
		Hispanic/Latino	5	Professional	54
				Doctorate	11
Total	**213**	Total	**213**	Total	**213**

Data Analysis and Results

SmartPLS (version 2.0) serves as the primary statistical tool to analyze the measurement and structural models. Partial least squares (PLS) are well suited for the study's predictive nature and allow for an assessment of the relative influence of the fraud triangle on the likelihood of computer fraud. Convergent validity is generally achieved if three criteria are met: (1) all item factor loadings should be significant and greater than 0.70, (2) average variance extracted (AVE; the amount of variance captured by a latent variable relative to the amount caused by measurement error) should be greater than 0.50 (or the square root of AVE > .707), and (3)

https://aisel.aisnet.org/pajais/vol14/iss4/4
DOI: 10.17705/1pais.14404

the composite reliability index for each construct should be greater than 0.70. All of these criteria were met for all constructs. Further evidence of the convergent validity of all remaining items comes from their significant t-statistics. Reliability was assessed) using Cronbach's alpha and composite reliability scores, with the recommended threshold of 0.70 being met for all constructs. Discriminant validity is verified by the difference between the AVE of a construct and its correlation with other constructs. To achieve sufficient discriminant validity, the square root of AVE of a construct should be greater than its correlations with all other constructs (Fornell & Larcker, 1981). As shown in Appendix C, the criterion for sufficient discriminant validity was also met in this study. In addition, since data collection was done through self-reported measures via a survey instrument, it is important to assess the potential effects of CMV. This study employs the Harman's single factor test, which showed all of the items were loaded on a single factor in exploratory factor analysis.

Afterward, hypotheses were tested through the examination of the structural model. Results for the structural model are presented in Figure 3. The results show opportunity and perceived general work pressure as determinants of the intention to commit computer fraud, but idealism does not. Overall the model explains 19.6% of the variance in the intention to commit computer fraud behavior. Table 5 summarizes the results of this study

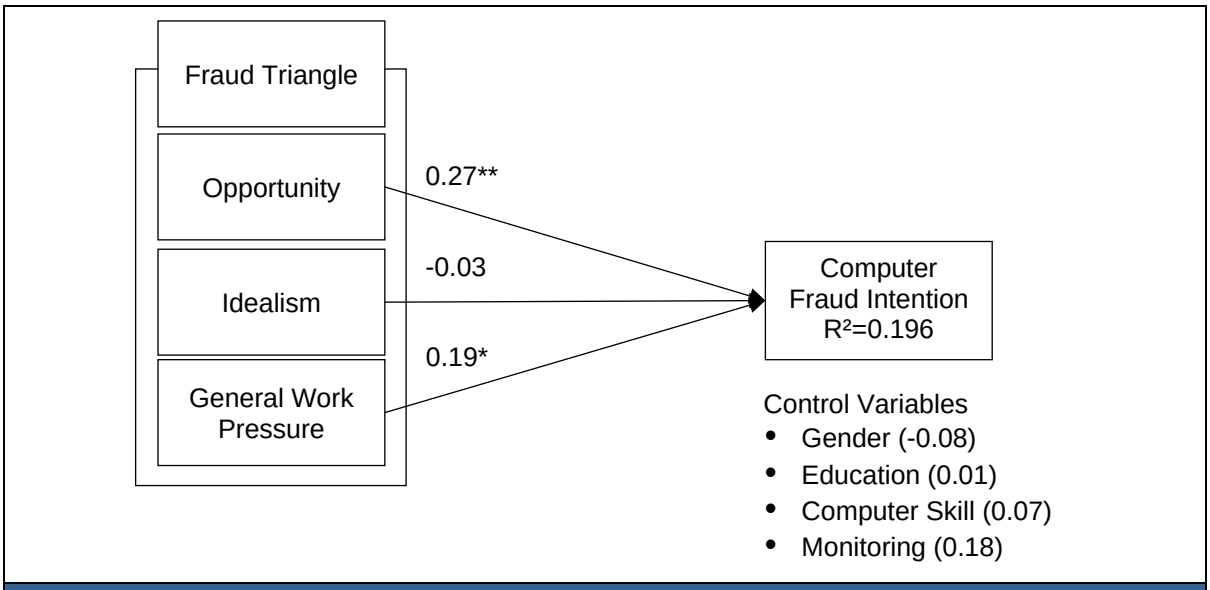


Figure 3 – Predictive Model Results

Note: *p<0.1. **p<0.05. ***p<0.01

Table 5 – Summarized hypotheses testing results

Path	Path coefficient	T-Statistic	p-value	Hypothesis Test Result
OPP → CFL	0.26	2.58	0.009*	H1: Supported
IDEAL →CFL	-0.03	0.25	0.80	H2: Not supported
GWP → CFL	0.20	2.05	0.04***	H3: Supported

Note: *p<0.1. **p<0.05. ***p<0.01

Discussion

Based upon the fraud triangle theory, this research examines the factors that may motivate an employee's intention to commit computer fraud. The results from a survey of 214 respondents suggest that the proposed model can explain substantial variance in the intention to commit computer fraud. Specifically, the results revealed that perception of opportunity and general work pressure significantly affected behavioral intention (H1 and H3). When an individual's level of idealism is high, their view of the use of technology should be used to maximize the good consequences and reduce the harmful consequences. The higher an individual's level of idealism is expected to prevent their intention to commit computer fraud. However, interestingly, an individual's level of idealism did not affect the behavioral intention (H2). Our non-significant result indicates the consequences of committing computer fraud may be dehumanized through the use of technology, an idea presented in prior research (Postmes et al., 1998). Another possible explanation for this is that the intent to commit computer fraud may not always be a premeditated act. Therefore, rational thoughts may be absent (Rook & Fisher, 1995). Furthermore, no significant impact was found on control variables – gender, education, computer skills, and monitoring (Posey et al., 2011). It suggests that computer fraud behavior can be explained by factors rooted in the presented theoretical model rather than computer monitoring.

The findings of this study provide new insights and important theoretical implications for researchers. First, this study provided evidence on employees' computer fraud behaviors, which is critical but often overlooked in the existing ISS literature. Investigating employee behavior motivation is especially important when employees actively seek nonconformance opportunities to harm organizational information security. However, the antecedents to actual intent to commit computer fraud behavior remain elusive. The finding of this study reveals a direct relationship between an individual's perception of opportunity, general work pressure, and their intention to commit computer fraud behavior. This result indicates that intentions to commit computer fraud are not entirely stable, and fluctuations in an individual's intent can be partially explained in an employee's levels of stress and perceptions of the work environment. Since the ultimate goal of ISS compliance is to avoid information security threats, literature has examined various motivational factors as the reasons why an employee may decide to deviate from security policies (Liang & Xue, 2009). For example, the mixture of an individual's self-determination and psychological reactance to controls as intrinsic motivations to willingly adopt an organization's ISPs (Ke & Zhang, 2010; Lowry et al., 2010), and individuals' self-efficacy to secure organizational information (Johnston & Warkentin, 2010; Vance et al., 2012). The finding of this study confirms the importance of motivational factors in determining the effectiveness of ISP, as suggested in the existing literature. It also extends our understanding of computer fraud behaviors' critical motivation factor – ISP general work pressure.

Secondly, from a theoretical standpoint, this study uses the fraud triangle theory as a theoretical lens to empirically investigate the intent to commit computer fraud. Previous research has examined computer abuse intentions by measuring perceptions of fairness through the organizational justice theory (Willison et al., 2018). Others have studied how an organization's information security policies may deter individuals from committing violations against an organization (D'Arcy et al., 2009; Herath & Rao, 2009; Hu et al., 2011). Scholars have also shed insight on how technology can influence an individual's unethical IT use (Chatterjee et al., 2015; Limayem et al., 2004). The fraud triangle theory offers an alternative theoretical explanation, including an individual's perception of organization controls, work environment, and individual's rationalization regarding technology. Our results suggest organizations can alleviate the general work pressures perceived by employees by providing proper resources and work performance expectations. The findings in this study suggest there is an expansion in the processes of organizations that span across the boundaries of organizations, professions, and groups of experts (Miller et al., 2008), showing how ideas move across disciplines, specifically in the field of information systems and accounting. This

https://aisel.aisnet.org/pajais/vol14/iss4/4
DOI: 10.17705/1pais.14404

study also implies it may be fruitful for further examination into different aspects of an individual's rationalization. This may have additional findings towards computer fraud intention. Specifically, it may explain why employees choose not to comply with information security policies.

Implications for Practice

This study provides valuable insight to organizations and managers. The results suggest checking on the employee's perceptions of an opportunity and work pressure may mitigate the intention to commit computer fraud. Traditionally, managers often adopt rewards and sanctions to reinforce their ISP compliance behaviors. However, our results indicate that employees are practical and care about their own work responsibilities; as a consequence, work pressure becomes a critical role in their intention of committing computer fraud. Therefore, managers may utilize periodic training for their employees to reduce work stress regarding their organization's information security policies and work demands. Furthermore, managers may also evaluate their employee's work pressure to contribute to a less stressful work environment.

The findings also suggest that organizations should employ different effective information security techniques to eliminate computer fraud opportunities instead of relying upon strongly-worded security policies. Organizations often place strong security policies to enhance security compliance behaviors. However, the findings in this study regarding the significance of opportunities on determining the individual intention of committing computer fraud indicate that having strong security policies may not be enough to prevent intentional and malicious non-compliance behaviors. In other words, robust information security policies may deter an employee's perception of an opportunity to commit computer fraud; however, to reduce employees' intentional and malicious non-compliance behaviors, the opportunities for computer fraud should be eliminated as much as possible. Management must treat the computer fraud opportunities separately from the general security compliance behaviors.

Limitations and Additional Future Research

As with many other studies, this study has limitations. Much behavioral security research 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 that respondents self-reported their intention to commit computer fraud. Some may conceal their true intentions because they perceive this behavior as socially undesirable (Trevino, 1992). One way to alleviate this limitation is to use scenarios that provide a more detailed description of a hypothetical employee and indirectly ask about the individual's beliefs through the employee's situation in the hypothetical scenario (Siponen & Vance, 2010). To enrich the computer fraud literature, future research related to computer fraud should consider detailed scenarios.

Third, comparing the existing general work pressure examined, such as financial pressure driven by internal greed or external pressure given by management (Kassem & Higson, 2012), this study only examined the employees' general work pressure. One possible direction for future research is to investigate whether other specific pressures play roles in shaping employee attitudes toward computer fraud behavior. Finally, this study focused on individual factors leading to the intention to commit computer fraud. Still, future research might investigate the impact of organizational factors such as sanctions (e.g., facing litigation, financial detriments) or rewards on an employee's attitude towards computer fraud. Another

extension of the research along this line can incorporate both individual factors and institutional factors (e.g., corporate tone) to explain the computer fraud intentions and study the relative importance of those factors in shaping an employee's computer fraud behaviors.

Conclusion

Most computer frauds are perpetrated by people in positions of trust such as accounting, finance, and IT functions. Therefore, it is critical to understand the motivation for an employee to engage in computer fraud behavior, especially if organizations are to test their security policy effectiveness (Bélanger et al., 2017). Based on the fraud triangle theory, this study surveyed 213 computer-using employees with financial responsibilities within their organizations in U.S., indicating that work pressure plays a critical role in determining their computer fraud intention, in addition to opportunity. These findings suggest the importance of monitoring the work pressure to guard against employees committing computer fraud behaviors and employing different security techniques to eliminate the computer fraud behaviors. In summary, when designing an organization's information security policies, computer fraud behaviors should be considered separately from other security compliance behaviors.

https://aisel.aisnet.org/pajais/vol14/iss4/4
DOI: 10.17705/1pais.14404

References

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society, 32*(3), 183-196.

ACFE. (2018). Report to the Nations on Occupational Fraud and Abuse (Association of Certified Fraud Examiners) (A.o.C.F. Examiners Ed.). Austin (USA). ACFE 2018 Report to the Nations - International Fraud Group

Adams, G. B., & Balfour, D. L. (2014). *Unmasking Administrative Evil*. Routledge.

Ahmed, A., Yusof, S. A. M., & Oroumchian, F. (2019). Understanding the business value creation process for business intelligence tools in the UAE. *Pacific Asia Journal of the Association for Information Systems, 11*(3), 55-88.

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

Albrecht, W. S., Howe, K. R., & Romney, M. B. (1984). Deterring fraud: The internal auditor's perspective. *Journal of Accountancy (pre-1986)*, *158*(000005), 184.

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

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

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), 104-119.

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management, 54*(7), 887-901.

Bissell, K., Lasalle, R. M., & Cin, P. D. (2019). Ninth annual cost of cybercrime study. *Ponemon Institute: Dublin, Ireland*, *6*.

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

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

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

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

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

Cooper, C. (2009). *Extraordinary Circumstances: The Journey of a Corporate Whistleblower.* John Wiley & Sons.

Cressey, D. R. (1953). Other people's money; a study of the social psychology of embezzlement. New York: Free Press.

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

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

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

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

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

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

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

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

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 31*(8), 983-988.

Ganster, D. C., & Schaubroeck, J. (1991). Work stress and employee health. *Journal of Management, 17*(2), 235-271.

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

Godos-Díez, J.-L., Fernández-Gago, R., & Cabeza-García, L. (2015). Business education and idealism as determinants of stakeholder orientation. *Journal of Business Ethics, 131*(2), 439-452.

Greller, M., & Parsons, C. K. (1988). Psychosomatic complaints scale of stress: Measure development and psychometric properties. *Educational and Psychological Measurement, 48*(4), 1051-1065.

Guragai, B., Hunt, N. C., Neri, M. P., & Taylor, E. Z. (2017). Accounting information systems and ethics research: Review, synthesis, and the future. *Journal of Information Systems, 31*(2), 65-81.

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

Haugen, S., & Selin, J. R. (1999). Identifying and controlling computer crime and employee fraud. *Industrial Management & Data Systems, 99*(8), 340-4.

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

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

Hoffer, J. A., & Straub, D. W. (1989). The 9 to 5 underground: Are you policing computer crimes? *MIT Sloan Management Review, 30*(4), 35.

Hollinger, R. C., & Clark, J. P. (1983). *Theft by employees*. Lexington, MA: Lexington Books. *126*.

https://aisel.aisnet.org/pajais/vol14/iss4/4
DOI: 10.17705/1pais.14404

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

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

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

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

Kassem, R., & Higson, A. (2012). The new fraud triangle model. *Journal of Emerging Trends in Economics and Management Sciences, 3*(3), 191-195.

Ke, W., & Zhang, P. (2010). The effects of extrinsic motivations and satisfaction in open source software development. *Journal of the Association for Information Systems, 11*(12), 5.

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

Leach, J. (2003). Improving user security behaviour. *Computers & Security, 22*(8), 685-692.

Leventhal, G. S., Karuza, J., & Fry, W. R. (1980). Beyond fairness: A theory of allocation preferences. *Justice and Social Interaction, 3*(1), 167-218.

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

Limayem, M., Khalifa, M., & Chin, W. W. (2004). Factors motivating software piracy: a longitudinal study. *IEEE transactions on engineering management, 51*(4), 414-425.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly, 16*(2), 173-186.

Lowry, P. B., Teh, N., Molyneux, B., & Bui, S. N. (2010). Using theories of formal control, mandatoriness, and reactance to explain working professionals' intent to comply with new IT security policies. In *Roode Workshop on IS Security Research, Boston, MA, USA*, 278-316.

Manurung, D. T., & Hadian, N. (2013). Detection fraud of financial statement with fraud triangle. In *Proceedings of 23rd International Business Research Conference*.

Mathieu, J. E., Martineau, J. W., & Tannenbaum, S. I. (1993). Individual and situational influences on the development of self-efficacy: Implications for training effectiveness. *Personnel Psychology, 46*(1), 125-147.

Maynard, S., Tan, T., Ahmad, A., & Ruighaver, T. (2018). Towards a framework for strategic security context in information security governance. *Pacific Asia Journal of the Association for Information Systems, 10*(4), 65-88.

Miller, P., Kurunmäki, L., & O'Leary, T. (2008). Accounting, hybrids and the management of risk. *Accounting, Organizations and Society, 33*(7-8), 942-967.

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

Mui, G., & Mailley, J. (2015). A tale of two triangles: Comparing the Fraud Triangle with criminology's Crime Triangle. *Accounting Research Journal, 28*(1), 45-58.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & 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), 126-139.

Nakayama, M., & Chen, C. C. (2019). Length of cloud application use on functionality expectation, usability, privacy, and security: A case of Google Docs. *Pacific Asia Journal of the Association for Information Systems, 11*(3), 5-27.

Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information.* John Wiley & Sons, Inc.

Paternoster, R. (2010). How much do we really know about criminal deterrence. *Journal of Criminal Law and Criminology, 100*(3), 765-824.

Ponemon Institute. (2020). *Cost of Insider Threats Global Report.* Ponemon Institute. https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2020/12/UK-VR-Proofpoint-Report-2020-Cost-of-Insider-Threats.pdf

Public Company Accounting Oversight Board (PCAOB). (2002). AU 316: Consideration of fraud in a financial statement audit. http://au-00316.pdf.

Posey, C., Bennett, B., Roberts, T., & 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), 24-47.

Postmes, T., Spears, R., & Lea, M. (1998). Breaching or building social boundaries? SIDE-effects of computer-mediated communication. *Communication Research, 25*(6), 689-715.

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

PricewaterhouseCoopers (2018), "Strengthening digital society against cyber shocks", The Global State of Information Security Survey 2018. https://www.pwc.com/us/en/cybersecurity/assets/pwc-strengthening-digital-society-against-cyber-shocks.pdf

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), 521-533.

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*.

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

Rook, D. W., & Fisher, R. J. (1995). Normative influences on impulsive buying behavior. *Journal of Consumer Research, 22*(3), 305-313.

Sauter, S. L., & Murphy, L. R. (1995). *Organizational Risk Factors for Job Stress.* American Psychological Association.

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

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

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

Skousen, C. J., Smith, K. R., & Wright, C. J. (2009). Detecting and predicting financial statement fraud: The effectiveness of the fraud triangle and SAS No. 99. In *Corporate governance and firm performance*. Emerald Group Publishing Limited. 53-81.

Sojer, M., Alexy, O., Kleinknecht, S., & Henkel, J. (2014). Understanding the drivers of unethical programming behavior: The inappropriate reuse of internet-accessible code.

Journal of Management Information Systems, 31(3), 287-325.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34*(3), 503-522.

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

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

Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly, 14*(1), 45-60.

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

Sujeewa, G. M. M., Yajid, M., Azam, S., & Dharmaratne, I. (2018). The new fraud triangle Theory-Integrating ethical values of employees. *International Journal of Business, Economics and Law, 16*(5), 52-57.

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

Trevino, L. K. (1992). Moral reasoning and business ethics: Implications for research, education, and management. *Journal of Business Ethics, 11*(5-6), 445-459.

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security, 52*, 128-141.

Vanasco, R. R. (1998). Fraud auditing. *Managerial Auditing Journal, 13*(1), 4-71.

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems, 15*(10), 679-722.

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

Vasiu, L., & Vasiu, I. (2004, January). Dissecting computer fraud: From definitional issues to a taxonomy. In *37th Annual Hawaii International Conference on System Sciences.*

Wang, J., Xiao, N., & 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), 619-633.

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

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

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

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

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

Appendix A. Construct and Measurement Items

Construct and Scale Indicators		
Constructs	Items	Reference
Opportunity	• Having other employee's information systems' credentials is easy. • Having access to other employees' information systems may provide competitive edge. • Having access to other employee's information systems may enhance effectiveness of the job. • In general, there is an opportunity to exploit the company's information systems.	(Pratt & Cullen, 2000)
Rationalization/ Idealism	• People should make certain that their actions never intentionally harm another even to a small degree. • One should never psychologically or physically harm another person. • If an action could harm an innocent other, then it should not be done. • The dignity and welfare of the people should be the most important concern in any society.	(Forsyth, 1980)
General Work Pressure	• Overall, I often feel stressful because of my work. • Overall, the work allocated to me makes me feel stressful. • Overall, my work will not stress me out.	(Greller & Parsons, 1988; Stanton et al., 2001)
Computer Fraud Intention	• It is highly likely the employees will compromise a computer system through computer fraud. • The likelihood of computer fraud occurring caused by employees is high. • In general, the probability of computer fraud occurring within the organization will be very high.	(Hovav & D'Arcy, 2012)
Computer Skill	• Computer skill of employee who is likely to attempt computer fraud	(Parker, 1998)
Monitoring	• An employee is closely monitored while using the organization's computer system. • The organization closely monitors employee performance for errors in the computer system. • There is constant surveillance for computer security policy violations. • There is supervision to see that an employee obeys all computer security policies pertaining to their job.	(Posey et al., 2011)

https://aisel.aisnet.org/pajais/vol14/iss4/4
DOI: 10.17705/1pais.14404

Appendix B. Item Loadings

Item Loadings				
Item	Factor Loading	AVE **(0.50)**	Composite Reliability **(0.80)**	t-stat.
Opportunity		0.58	0.84	
Opp1	.72			6.43
Opp2	.77			8.12
Opp3	.73			7.41
Opp4	.81			14.76
Rationalization/Idealism		0.71	0.91	
Ideal1	.92			4.43
Ideal2	.78			3.36
Ideal3	.89			4.50
Ideal4	.77			3.14
General Work Pressure		0.78	0.91	
GenPress1	.95			6.23
GenPress2	.94			5.88
GenPress3	.72			4.95
Computer Fraud Likelihood		0.87	0.95	
CPUI1	.92			36.37
CPUI2	.93			29.98
CPUI3	.95			67.68

About the Author

Dr. Randi Jiang is an Assistant Professor of Accounting in the School of Accounting in the Seidman College of Business at Grand Valley State University. Her research interests are in judgment and decision-making in accounting information systems related to the detection of fraud and deception, cybersecurity, and managerial ethics. Her work has been presented at numerous conferences and published in outlets including *Communications of the Association for Information Systems, Information and Software Technology, and Information Systems Management.*

https://aisel.aisnet.org/pajais/vol14/iss4/4
DOI: 10.17705/1pais.14404