Summer 7-9-2018

Investigating Information Security Policy Characteristics: Do Quality, Enforcement and Compliance Reduce Organizational Fraud?

Dennis T. Brown
Kennesaw State University

INVESTIGATING INFORMATION SECURITY POLICY CHARACTERISTICS: DO QUALITY, ENFORCEMENT AND COMPLIANCE REDUCE ORGANIZATIONAL FRAUD?

by
Dennis T. Brown

A Dissertation

Presented in Partial Fulfillment for the
Degree of
Doctor of Business Administration
In the
Coles College of Business
Kennesaw State University

Kennesaw, GA
2018

SIGNATURE PAGE

Placeholder

DEDICATION

As with most significant achievements, this journey was made possible by many other people. First thanks to my wife Suzy for her support. I would not be here to start with without the inspiration and help of my best friends Rodney and Sarah Alsup. Thank you to my committee of Humayun Zafar, Brad Schafer and Solomon Negash who guided me through this process. Also great thanks to Brian Rutherford and Torsten Pieper who helped us understand how to be successful in this field from our first class in the program. Thank you also to Joe Hair who helped me understand statistical methods. Also, a special thanks to all of the staff who provided support all along the way. I could not have completed this without your help and guidance. You have helped make me better by this experience and I will always cherish our friendship. Also thank you to Juanne Green who provided inspiration all along the way.

ACKNOWLEDGEMENTS

Thanks to all of my Cohort 6 team that worked with each other to complete this Degree. Thank you to Rodney and Sarah Alsup. Also thank you to my committee of Humayun Zafar, Brad Schafer and Solomon Negash who guided me through this process. Also great thanks to Brian Rutherford and Torsten Pieper who helped us understand how to be successful. Thank you, Joe Hair, for providing inspiration to learn statistics. Thank you Juanne Green for your inspiration.

ABSTRACT

INVESTIGATING INFORMATION SECURITY POLICY CHARACTERISTICS: DO QUALITY, ENFORCEMENT AND COMPLIANCE REDUCE ORGANIZATIONAL FRAUD?

By

Dennis T. Brown

Organizational fraud, a deceitful practice or willful device resorted to with intent to deprive another of his right, or in some manner to do harm or injury, is a growing global concern. While cyberattacks from the outside are more expected, the internal security threat from trusted insiders is responsible for significantly more information compromise than external threats. Information systems make life easier but are increasingly used by employees to perpetrate fraudulent activities. For example, a trusted insider employee with access to sensitive customer databases could misappropriate information and sell it to a competitor for personal gain. These type losses are typical of organizational fraud averaging 5% of annual revenues, and current detection and prevention methods are not fully adequate to address the threat.

This research examines how organizational fraud is affected by information security policy characteristics. We specifically study the effects of quality and enforcement as mediated by security compliance using a sampling of survey data from selected organizations. Our results show that increased quality and enforcement supports increased compliance. We found an inverse relationship between policy compliance and

organizational fraud. Additionally, our model demonstrates that compliance fully mediates between policy quality, policy enforcement, and the dependent variable fraud.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 1 - INTRODUCTION

Organizational fraud reduces every organization's ability to reach its full potential. It is a major insidious risk facing businesses and is increasingly difficult to detect and prevent (Abbasi, Albrecht, Vance, & Hansen, 2012; Cressey, 1986; Wolfe & Hermanson, 2004). Fraud is a latent crime; its true, complete impact is difficult to measure accurately (Button, Lewis, Shepherd, & Brooks, 2015; Davis & Pesch, 2013). Fraud affects society to such a degree that it has effectively reduced overall consumer and investor confidence in core business processes (Albrecht, Albrecht, & Albrecht, 2008). Computers make handling, storage and manipulation of large amounts of data much easier but have also introduced greater opportunity for organizational fraud. Wider use of information systems has opened the door to opportunistic, self-serving behavior, including fraud. Information security policy violations result in a "superhighway" to various organizational fraud activities (Trinkle, Crossler, & Warkentin, 2014; Willison & Warkentin, 2013). The purpose of this research is to examine how organizational fraud is affected by information security policy characteristics of quality, enforcement, and compliance. Significant variance has been explained in previous individual studies to predict compliance, but not in the context of fraud research. We specifically study the effects of quality and enforcement as mediated by security compliance using a sampling of survey data from selected individuals. A review of 29 quantitative studies revealed 61 antecedent variables that determine information security policy compliance. Since there are so many potential independent variables that explain only a small portion of the

variation, we chose to narrow the focus to those that potentially explain relatively more, especially those with a hypothesized interaction effect (policy quality and enforcement). Also, many of the studies using other variables present either conflicting results or a wide statistical range of similar results. For example, the predictor variable "subjective norm" ranged from a $\beta = -0.09$ to 0.45 (Sommestad, Hallberg, Lundholm, & Bengtsson, 2014). We chose to use the independent variables of policy quality and enforcement because policy quality coupled with robust enforcement are variables that directly impact the human aspect of the insider threat, which is generally considered more dangerous and potentially harmful than attacks from outside sources. Trusted individuals working inside organizations continue to be the weakest link when assessing overall security risk (Bulgurcu, Cavusoglu, & Benbasat, 2010b; Chen, Ramamurthy, & Wen, 2012; M. Siponen & Willison, 2009). Several elements of enforcement, including perceived behavioral control, perceived justice of punishment, threat appraisal, and the threat of sanctions (certainty, celerity, and severity) most significantly predicted compliance (Sommestad et al., 2014). The following sections focus on organizational fraud and the theoretical relationships between each of the specified information security policy characteristics (quality, enforcement, and compliance) included in this research study.

Organizational Fraud

Organizational fraud is defined here as "some deceitful practice or willful device, resorted to with intent to deprive another of his right, or in some manner to do him an injury. As distinguished from negligence, it is always positive, intentional" (Bryan,

2009). This is consistent with the accounting and auditing community definition set forth in the Statement on Auditing Standards (SAS) 99 (T. D. Carpenter, 2007).

Most of the current fraud detection/prevention models focus on financial measures (generally 6-10) and ratios, which work to identify and disclose certain "red flags" or other indicators of potential fraud (Abbasi et al., 2012). Our model differs significantly since we focus on antecedents that impact actions of the trusted insiders in general *before* they have a chance to act. These trusted insiders generally have the ability to inflict the most harm acting from within the organization.

There are several different types of fraud schemes discussed in the literature. Asset misappropriation is one such example in which a perpetrator steals, abuses or otherwise misuse the employing organization's resources. An example of these resources is the customer database, which contains sensitive, proprietary information critical to successful operations of the business. Customer databases are among many organizations' most valuable non-monetary assets and are a significant target of insider fraud attempts. Professional data collected and retained for business purposes poses a threat due to its very existence (Rechtman & Rashbaum, 2015). As data volume grows, organizations are increasingly targets for unauthorized use (Rechtman & Rashbaum, 2015). For example, trusted insiders may feel emboldened to violate existing security policies to steal valuable database information and use it for personal gain (DeZoort & Harrison, 2016).

Although external audits are a popular fraud tool, they are empirically among the least effective (ACFE, 2016). Despite changes to basic accounting and internal control procedures following the scandals at Enron, WorldCom and others, the problem

continues to worsen (Abbasi et al., 2012). Only a small portion of white-collar crimes and misdemeanors are discovered, including computer-related employee fraud in the workplace (Lowe, Pope, & Samuels, 2015; Straub Jr & Nance, 1990).

Information Security Policy Compliance

Extant research has not studied potential synergistic effects of policy quality and enforcement thus far. Since the main threat to information security originates with trusted employees' non-compliance with security policies, we searched for independent variables that theoretically explain more of the reasons for this lack of compliance (M. Siponen, Mahmood, & Pahnila, 2014). Non-compliance of information security policy and weak internal controls may be linked to fraudulent activity of various types (Lynch & Gomaa, 2003; Richardson & Director, 2008). Lack of policy compliance is a recognized weakness in most organizations and is increasingly becoming a management and leadership priority (Bulgurcu et al., 2010b; Coopers, 2014; Vance, Lowry, & Eggett, 2015). According to Whitman (2003), human failures and insufficient security policies ranked number three and four respectively among information security threats in order of severity (Whitman, 2003). Insider employees that leave the organization become a special threat; 59% admit to stealing privileged client information such as customer contact lists, employee records, and various forms of non-financial data contact lists (Ayyagari, 2012).

Information Security Policy Quality

Information security policy quality is the perceived level of adequacy and completeness of the guidelines that cover all information risk possibilities in an organization (Chen et al., 2012; Goo, Yim, & Kim, 2014). Past research and General

Deterrence Theory (GDT) theoretically link information security policy quality and enforcement to information security policy compliance (Goo et al., 2014); however, any potential relationship between information security policy quality leading to compliance and fraud has not been studied.

The insider threat is generally considered to have more harmful potential than attacks from outside sources (Bulgurcu et al., 2010b; Chen et al., 2012; M. Siponen & Willison, 2009). Fraud is more difficult to accomplish from the outside since the perpetrator does not know where the information resides and has to search through large amounts of data. Research indicates that security policies focusing on the insider versus external threats are more successful in preventing information losses (Posey, Roberts, Lowry, Bennett, & Courtney, 2013). Fraud surveys find that 51% of those responding have no plan in place to deal with insider threats despite the upward trend. Many companies still do not have a formal information systems threat security function and simply let the IT section handle issues (Coopers, 2014). Since computers and large volumes of data contained in information systems are common to most industries, many opportunities for fraud and other malicious activity are increasingly available to potential perpetrators (Lynch & Gomaa, 2003; Purda & Skillicorn, 2015).

Higher information quality contained in the information security policy positively affects end-user information security policy compliance (Abedin, Nessa, Al-Shaer, & Khan, 2006; Bulgurcu et al., 2010b). Effective policy forms the underlying basis for all subsequent security efforts, including security culture and enforcement (Chen et al., 2012; Lindup, 1995; M. Siponen & Vance, 2010). Employees must understand clearly the limits of their computer system's acceptable use. For example, unauthorized access to

sensitive and proprietary data and subsequent file transfers offer multiple opportunities to engage in fraud. Policy that limits employee access through internal controls removes the basic opportunity to commit fraud. Limiting the number of authorized users essentially reduces the potential for malevolent behaviors leading to fraud. (Lynch & Gomaa, 2003; Roden, Cox, & Kim, 2016; Tabuena, 2013).

Many potential fraud events originate simply with an individual's ability to download sensitive information with little perceived monitoring or accountability (opportunity). Weak institutional and/or individual pressure to comply with established policy (lack of deterrence) results in perceived fraud opportunity. Higher quality information security policies inhibit potentially malevolent activities. Quality information security policies are designed to prohibit the unauthorized download of sensitive and valuable proprietary information, including company trade secrets and intellectual property. Higher quality security policies minimize the number of vetted employees granted access to highly sensitive information based on a bona-fide job requirement and "need-to-know". Often this first line of defense is enough to prevent the opportunity to commit fraud and serves as a preemptive deterrent. Effective security monitoring and other forms of enforcement may create an environment where employees perceive they lack the opportunity to perpetrate fraud without discovery and subsequent sanctions.

Organizational fraud concealment often involves manipulation of account values to set up later theft of assets (Ngai, Hu, Wong, Chen, & Sun, 2011; Steinbart, Raschke, Gal, & Dilla, 2015). If internal security controls are weak or not enforced in the company, employees may perceive easy opportunities to perpetrate organizational fraud

while remaining anonymous. This is especially true if there is a lack of strong enforcement processes in place.

Information Security Policy Enforcement

Most violations are not caught by existing functional security risk management (SRM) programs but instead are discovered by accident or though whistleblowers. Information and tips from conscientious employees who witness fraud incidental to their job performance are leading sources of initial fraud discovery in organizations (ACFE, 2016). This represents a low enforcement environment and indicates that other established processes to detect fraud have failed (Cecchini, Aytug, Koehler, & Pathak, 2010). If security policies are implemented effectively, most potential breaches will be detected by a simple logging of violations tied to the fraudster. Employee attitudes toward fraud and incident reporting form over time based on perceived and empirical reinforcement in the workplace. Research indicates that only about 50% of employees overall are willing to report potential acts of fraud (Kaplan, Pope, & Samuels, 2015). These numbers could be significantly improved with increased policy quality and enforcement (Goo et al., 2014; Liu, Wright, & Wu, 2015).

Many of the accounting and behavioral “Red Flags” associated with fraud are linked to information security and policy compliance (G. M. Trompeter, Carpenter, Jones, & Riley Jr, 2014). However, these policy violations and their possible specific links to organizational fraud have not been studied significantly and require further research (Tabuena, 2013).

Examples of typical policy violations include gambling, online social networks (OSN) presence, day trading, gaming, pornographic sites, online dating, pyramid

schemes, chain-letter e-mails, sports contests, jokes, lottery pools, cyber bullying, and cyber stalking. Minimally these violations are considered pervasive forms of fraud and result in lost employee productivity during work hours. These violations are also a gateway to many more serious forms of potential fraud. Fraud could be significantly reduced if employees would strictly adhere to official information security policies (Trinkle et al., 2014; Warkentin & Willison, 2009). Organizational fraud in our study focuses on data theft because of the ubiquitous nature of data in today's "information age".

Organizations are concerned with the cost of security compromises, public image, and increases in the volume of proprietary information requiring protection. Information security developments offer the potential for significant inroads toward fraud reduction in the future (Bulgurcu et al., 2010b; M. Siponen et al., 2014; Willison & Warkentin, 2013). Empirical research data linking fraud theory to fraud in a corporate environment is sparse (Roden et al., 2016). Traditional studies of financial ratios to identify potential fraud have demonstrated limited potential. We predicted that increased quality and enforcement would result in synergistic compliance, thereby achieving the lowest level of fraud, which was supported. Practitioners will benefit from empirical evidence that industry investment in higher quality policy and enforcement increases compliance and reduces perceived fraud.

Therefore, we propose following research question (RQ):

RQ: *How is organizational fraud influenced by information security policy characteristics?*

The remainder of this study is organized as follows. Chapter 2 covers existing fraud and information security policy compliance literature and proposes hypotheses to test the model. It also reviews previous efforts to identify and prevent financial fraud and demonstrates the need for more effective and robust methods. Chapter 3 discusses the methods used, study participants and setting, data analysis procedure and risks.

The subsequent sections discuss the findings, research limitations, and recommended future research.

CHAPTER 2 LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

Literature Review

Many reasons for organizational fraud are discussed in the literature, including employee motivations, accessibility, organizational ethical climate, incentive, opportunity, rationalization, and others (Ahmad & Norhashim, 2008; Albrecht, Howe, & Romney, 1984; Lynch & Gomaa, 2003; G. M. Trompeter et al., 2014). Many of these antecedents are included in our independent variables (policy quality and enforcement). Weak governance, lax audit controls, and inconsistent oversight all create perceived opportunities for fraudsters to act and subsequently avoid detection and punishment (Hafer & Gresham, 2012). The underlying basic concept of information security is that a satisfactory policy coupled with adequate enforcement will result in an increased and satisfactory level of security in the organization (Sommestad, Hallberg, Lundholm, & Bengtsson, 2014). Of the many variables introduced from years of study, enforcement and policy quality were ranked as the most significant with the potential to explain more of what past research failed to accomplish. Our objective for this research is to make a unique contribution to the field of fraud identification and prevention by studying antecedents that relate to the trusted human insider facet of policy compliance. Here we narrow down the factors that will most explain policy enforcement. We study policy characteristics and their relationship to fraud that potentially explain the most variance and have not previously been studied.

Background

Cressey (Cressey, 1950, 1953) first studied fraud as a white-collar crime in the modern era. Systematic causation was theorized to determine and predict "the criminal violation of financial trust" among otherwise honorable employees and citizens (Cressey, 1950)(Cressey, 1950, p.740). Opportunity, incentive, and attitudes are key determinants regarding individual propensity to commit fraudulent activity (Cressey, 1950, 1953, 1986; Sitorus & Scott, 2009).

Over the years, growth of computer use and the ubiquitous nature of information databases increased the potential for more fraud opportunity. Congress passed the Computer Fraud and Abuse Act (CFAA) in 1994 to prevent fraud using unauthorized access to computers and associated data. The Act's continued relevance is highlighted by the fact that it has been amended and strengthened several times over the years. The first amendment was 1994, again in 1996, then in 2002 following the events of 9/11 as part of the USA Patriot Act. It was further updated in 2008 by the Identity Theft Enforcement and Restitution Act. There is widespread disagreement between appellate courts regarding the reach and limitations of the law, but so far all have been consistent in application of the law regarding cases of intent to engage in fraudulent activities to obtain anything of value (Thomason, 2013).

Congress also recognized the need and passed other key legislation designed to strengthen security of information collected and stored by organizations. This served to increase the awareness of top management and to increase their liability going forward. Chief among these was the Gramm-Leach-Billey Act or Financial Modernization Act of 1999 (GLBA), which was designed to regulate how financial institutions handle, store and safeguard information belonging to private citizens. The Act contains three sections

designed to regulate the collection and dissemination of individuals' private financial information. It also mandates that financial institutions must develop and implement information security programs to protect private information.

Opportunity is a key antecedent of fraud, and is theoretically more available to trusted insiders (M. Siponen et al., 2014). Tenured employees occupying key positions within organizations are trusted with greater access to a wider range and depth of information, which also gives them commensurate opportunity to perform potentially fraudulent activity (Albrecht et al., 2008; Wolfe & Hermanson, 2004). Long-term employees and other trusted agents within the organization are often in positions to most clearly understand and exploit existing security vulnerabilities using their authority (Willison & Siponen, 2009). Information systems internal controls are designed to prevent this self-serving, opportunistic behavior (Steinbart et al., 2015; Wolfe & Hermanson, 2004). Many of them also develop the potential for nefarious individual gain during years of observation and performance of their jobs. Opportunistic behavior is increasingly likely when employees with significant capabilities and privileges are allowed to operate without an effective and operational information security policy (internal controls) in place (Albrecht, Wernz, & Williams, 1995; Wang, Gupta, & Rao, 2015).

Numerous methods of fraud detection and prevention have been studied to address increasing trends of organizational fraud; current approaches and potential solutions to fraud detection and prevention continue to fall short of expectations. (Abbasi et al., 2012; Lynch & Gomaa, 2003). These methods include expanded traditional audits (including more appropriate analytical procedures), automated approaches, data analytics,

data visualization, meta-learning frameworks, data mining, and the Analytic Hierarchy Process (Abbasi et al., 2012; Debreceny & Gray, 2010; Dilla & Raschke, 2015; Ravisankar, Ravi, Rao, & Bose, 2011; G. Trompeter & Wright, 2010). More innovative, robust and improved methods are required to stem rising losses (Abbasi et al., 2012; Holton, 2009). Fraud cases average 18 months from execution to discovery, which highlights the insidious nature of the problem (Association of Certified Fraud Examiners, 2016). Most violations are not caught by existing functional security risk management (SRM) programs but instead are discovered by accident or though whistleblowers, thereby indicating weak enforcement (Cecchini et al., 2010; Straub Jr & Nance, 1990). Information and tips from conscientious employees who witness fraud incidental to their job performance are leading sources of initial fraud discovery in organizations (ACFE, 2016). Employee attitudes toward fraud and incident reporting form over time based on perceived and empirical reinforcement in the workplace. Research indicates that only about 50% of employees overall are willing to report potential acts of fraud (Kaplan et al., 2015).

Information Security Policy Quality

Information security policy quality is the perceived level of adequacy and completeness of the guidelines that cover all information risk possibilities in an organization (Chen et al., 2012; Goo et al., 2014). Policy is a comprehensive collection of rules, directives, and accepted practices that establish how an organization is to manage, protect and distribute important, sensitive information (Swanson, Hash, & Bowen, 2006). Information security policy design and implementation are important and poor quality results in more security breaches (Tarafdar, DArcy, Turel, & Gupta, 2015; Whitman,

2003). Top management involvement in policy formulation has a positive impact on information security effectiveness, and management practices have a significant role in information technology system effectiveness (Chen, Ramamurthy, & Wen, 2015; Soomro, Shah, & Ahmed, 2016). Policy provides guidance and direction to systems users and employees by specifically defining acceptable and unacceptable use of the organization's information systems and controlled information (Ashenden, 2008; Flowerday & Tuyikeze, 2016).

Security policy is the foundation and arguably the most important security layer available to organizations; it defines the security philosophy of the organization and is the basis for future security decisions and priorities. It is also an indicator of the degree to which the organization takes information security seriously (D'Arcy, Herath, & Shoss, 2014; M. T. Siponen & Oinas-Kukkonen, 2007; Whitman, 2003). These policies are the subject of discussion, study, and disagreement regarding the content as they vary significantly among organizations (Ølnes, 1994; Rees, Bandyopadhyay, & Spafford, 2003; Whitman, 2004; Wood, 1995).

Information security policy continues to evolve in order to meet emerging threats (K. Höne & J. Eloff, 2002; K. Höne & J. H. P. Eloff, 2002; Lichtenstein, 1997; Ølnes, 1994; Rees et al., 2003; Wood, 1995). The most commonly used and accepted industry guidelines are listed in Table 1. International information security standards originated to promulgate "best practices" among quality organizations in order to ensure the proper safeguarding of information in organizations (Susanto, Almunawar, & Tuan, 2012). These standards are primarily technical in nature but should form the foundation for comprehensive information security systems (Baskerville & Siponen, 2002; Susanto et

al., 2012). Organizational policies must be individually tailored and strategically aligned for consistency with the specific organizational goals and operating procedures of each (Baskerville & Siponen, 2002; Neil F Doherty & Fulford, 2006; Vroom & Von Solms, 2004). These key benchmarks allow organizations to measure their programs and policies against industry standards, but they must still be modified for organizational and industry variations (Susanto, Almunawar, Tuan, Aksoy, & Syam, 2011).

Table 1

Information Security Policy Quality Standards

Information Security Policy Quality	Studies/Reference
1. Industry Standards Factor	Price, Waterhouse, & Coopers, (2016)
2. ISO 27001/27002	International Standards Organization (ISO), (2013).
3. Control Objectives for Information and Related Technology (COBIT) 5	ISACA, 2016
4. Cybersecurity Framework	U.S. National Institute of Standards and Technology (NIST), 2016.
5. British Standard 7799-3	British Standard Institution (BSI), 1995, 1998
6. Critical Security Controls (SANS Top 20) version 6.0	SANS Institute, Council on Cybersecurity (2013).
7. Information Technology Infrastructure Library (ITIL)	British Standard Institution (BSI), 2011.
8. Payment Card Industry Data Security Standard (PCIDSS) v.3.2	Payment Card Industry Security Standards Council, 2016.

Acceptable use policy (AUP) standards are critical to quality information security policy since employees must completely understand their boundaries regarding

workplace privileges and limitations in order to achieve compliance. It is impossible to enforce standards if they are not quantified and codified (Neil Francis Doherty, Anastasakis, & Fulford, 2011; Räisänen, 2013; Willison & Warkentin, 2013). Acceptable use policy effectively reduces the opportunity of trusted insiders to be successful in opportunistic and self-serving behavior. Acceptable use policy includes the seven components contained in Table 2 (Neil Francis Doherty et al., 2011). For example, some companies allow employees to pay bills from work and do other tasks not related to their job within prescribed parameters during designated breaks. The exact same activity may be strictly prohibited in other companies. Acceptable use policies serve as deterrence to potential unauthorized behavior leading up to fraud. For example, if a policy prohibits downloading sensitive proprietary information (such as customer information), then a violation should immediately trigger a violation warning assuming that system monitoring and electronic logging is functioning. By setting the boundaries for employees, quality acceptable use policy affects employee attitudes as they consider malicious activity and potential punishments for offending behavior (Bridges & Stone, 1986).

Policy must be written, communicated, enforced and institutionalized in order to be effective (Kadam, 2007; Rees et al., 2003; Wood, 1995). Employees must initially and periodically sign various instruments indicating their understanding and willingness to comply with the established policy (enforcement). They must also understand that progressive disciplinary action and/or sanctions for potential policy violations will be levied quickly and surely. Recurrent employee refresher, acknowledgement and understanding of the established policy at periodic intervals affects employee attitudes

toward compliance and their expectations regarding future performance. It also ensures that everyone, from the top down, is adhering to the same standards (Neil Francis Doherty et al., 2011).

Table 2

Seven Components of Acceptable Use Policy (AUP)

Components
1. Continuous monitoring of proprietary organizational assets with activity logging.
2. Establishing a standard of "no privacy" expectations among employees (complete opposite of anonymity).
3. Clear definition of boundaries regarding improper employee use of computing assets.
4. Allowable employee uses and activities of computing assets.
5. Protection and security of sensitive company information.
6. Disciplinary action and sanctions for potential policy violations and disclosure.
7. Written employee acknowledgement and understanding of the policy

Asset misappropriations are the most common form of fraud, occurring in 85% of ACFE studies. Asset misappropriations are defined as fraud schemes where the perpetrator steals, abuses or otherwise misuse the employing organization's resources. Common asset misappropriations include theft of company cash, valuables, or other non-cash items, false billing schemes, and false or inflated expense reports (ACFE, 2016).

The top three most important contributing factors to fraud are 1) lack of internal controls; 2) lack of management review; and 3) override of existing internal controls (Association of Certified Fraud Examiners, 2016). This is consistent with information

systems literature which asserts that the most pressing threat to organizations is from trusted insiders (Johnston, Warkentin, & Siponen, 2015; Richardson & Director, 2008; G. M. Trompeter, Carpenter, Desai, Jones, & Riley Jr, 2012). Many of the most expensive and damaging information security breaches have been from trusted managerial and supervisory officials who by virtue of their duty position are exempt from adequate scrutiny (Chen et al., 2012; Vance, Lowry, & Eggett, 2013). Since only a small fraction of employees who discover fraud actually report it, other tools and controls must be employed to ensure effective enforcement in organizations (Kaplan et al., 2015; Straub Jr & Nance, 1990).

Information Security Policy Enforcement

Information security policy enforcement is the perceived level of supervisory oversight, monitoring, and organizational emphasis placed on information security with the goal of compliance (Goo et al., 2014). Organizational internal controls (policies and monitoring) increase the level of compliance and reduce the incidence of employee deviance, of which fraud is a key outcome (Dorminey, Fleming, Kranacher, & Riley Jr, 2012; Hollinger & Clark, 1982). Effective information security policy enforcement is the result of many factors, including human, physical and technological (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Shropshire, Warkentin, & Sharma, 2015). Effective enforcement requires employees to perceive that their supervisors monitor and care about following established policies. It also requires that supervisors incorporate compliance into overall performance assessments (Goo et al., 2014; Johnston et al., 2015). A significant number of breaches could be prevented if victim organizations had simply followed information systems internal controls (Corporation, 2016).

Continuous monitoring of proprietary organizational assets is the most effective when it is routine and standardized. All end-users should understand that every action on the system is monitored, logged and retrievable for future use by management if necessary for administrative and/or punitive actions; this establishes a degree of accountability and eliminates the perception of anonymity. Previous research indicates that anonymity is an inducement for potential perpetrators to engage in fraud since it allows them to avoid identification (Vance et al., 2013). All employees should understand that they have no reasonable expectation of privacy regarding any use of a company-provided information technology system.

Internal control systems are designed to reduce employee and managers' opportunity to carry out opportunistic and self-interested behavior (PCAOB, 2016). The strength of these internal controls is a key factor regarding the efficacy of preventing the undesired behavior (Tayler & Bloomfield, 2011). Policy quality and enforcement determine the strength of internal information security controls leading to less opportunity for potential fraudsters (Liu et al., 2015; Steinbart et al., 2015). Liu et al. (2015) performed research regarding links between the strength of internal controls and fraud. They found a significant correlation between weak monitoring and increased fraud levels. As strength of monitoring decreases, organizational fraud levels increase (Liu et al., 2015).

Information Security Policy Compliance

Information security policy compliance is the degree to which employees intend to comply with the rules set forth in the specific policy established by the company (Goo et al., 2014). The main threat to information security originates with employee non-compliance with information security policies (M. Siponen et al., 2014). Compliance with individual and organizational information security policies protects information assets from various forms of malfeasance, many of which are antecedents to fraud. Information assets are exploited for personal gain and are the object of various forms of fraudulent activity (Lynch & Gomaa, 2003).

Individuals make security compliance decisions based on many factors, including perceptions, beliefs, and biases (Chen et al., 2015; Q. Hu, West, & Smarandescu, 2015; Tsohou, Karyda, Kokolakis, & Kiountouzis, 2015). Both negative and positive incentives have been suggested and tested empirically to increase employee compliance with established information security policy (Bulgurcu et al., 2010b; Chen et al., 2012; D'Arcy, Hovav, & Galletta, 2009; Herath & Rao, 2009a, 2009b). These incentives, coupled with the perceived certainty, celerity and severity of sanctions to influence employee behavior, have been extensively studied in the literature (Straub & Welke, 1998; Willison & Warkentin, 2013). However, the research findings do not indicate strong support for these incentives as significantly affecting behavior, and do not always agree (Chen et al., 2012). Findings also included a strong relationship between information security policy, social controls and security culture, which suggests that policy quality and enforcement are key attributes in achieving overall compliance with organizational security objectives (Chen et al., 2015; Hsu, Shih, Hung, & Lowry, 2015;

Ifinedo, 2014). We reviewed many potential independent variables that explain smaller amounts of the overall variance, many of which are antecedents comprising policy quality and enforcement. For example, perceived risk of shame, perceived security risk, security culture, and numerous others explained small amounts of variance. Our focus here is to explain relatively more variance. Many past studies using other variables produced varying and sometimes inconsistent results. We use policy quality and enforcement because policy quality coupled with robust enforcement are variables that directly impact the human aspect of the insider threat, which is generally considered more dangerous and potentially harmful than attacks from outside sources.

Studies indicate that the perceived severity of information security threats resulted in more behavioral intention to comply with information security policies (M. Siponen et al., 2014). For example, as the perceived severity of the threat to the company increases, so does the employees' intention to comply. Employee belief as to whether they have the ability to apply and adhere to information security policies (technical ability etc.) was another significant factor. Similarly, employees' perceived vulnerability to potential security threats, their attitude toward complying with information security policies, and organizational management modeling regarding compliance also affected intention to comply (M. Siponen et al., 2014). Employee intention to comply with information security policy is significantly influenced by attitude, normative beliefs, and self-efficacy to comply (Chen et al., 2012; Chen et al., 2015). Outcome beliefs significantly affect attitudes regarding overall assessment of consequences, which in turn significantly affects employee attitudes (Chen et al., 2012). Information security awareness positively affects both attitude and outcome beliefs (Bulgurcu et al., 2010b).

Recent research indicates that information system access policy violations result in increased organizational fraud and theft. Although most information security policies limit the use of computing systems strictly for company business, non-compliance by employees is the weak link (Willison & Warkentin, 2013). Use of computing systems for other than company business is a gateway to other potentially malevolent behaviors (Trinkle et al., 2014). These actions include a range of activity from simple surfing, online social media visits, and ultimately fraud and cybercrime activities, all of which are detrimental to the organization and against established information security policy (Trinkle et al., 2014; Vance et al., 2015).

Additional studies investigating employees who violated information security policies found most managers and senior executives are personally aware of someone who has committed sabotage (Hafer & Gresham, 2012). One in five respondents reported having been a victim, at least one-half know employees who have been victimized, and one-third has personal knowledge of managers and customers who have been victimized. A key finding is that one of the purposes of information sabotage is to commit fraud of various types for personal gain (Hafer & Gresham, 2012).

General Deterrence Theory (GDT)

We selected General Deterrence Theory (Bridges & Stone, 1986; Maxwell & Gray, 2000) as the theoretical framework for the proposed model and hypotheses. General Deterrence Theory posits that sanctions, disincentives and the threat of punishments or sanctions serve to discourage would-be violators from engaging in prohibited behavior and supports policy compliance among employees. The perceived probability of discovery coupled with the severity of the potential advertised sanctions or

punishment increases, while the level of prohibited activity declines in a corresponding manner (Straub & Welke, 1998). Internal controls, including policy enforcement, serve to deter unethical behavior, and stronger controls correspondingly reduce the incidence of fraud (Board, 2002; Liu et al., 2015).

General deterrence theory serves to explain and predict individual decisions between compliance and non-compliance with established rules, policy, and law based on perceived sanctions or penalties for non-compliance (Bridges & Stone, 1986; Maxwell & Gray, 2000). Individuals make choices based on their internal assessment regarding the potential benefits and costs of their decisions, and the perceived severity and certainty of sanctions may influence individuals in their decisions to comply with security policies (Bridges & Stone, 1986; Cheng, Li, Li, Holm, & Zhai, 2013). Deterrence has predictive ability for specific behaviors of criminal activity (Bridges & Stone, 1986), has been successfully extended to the field of information systems (Chen et al., 2012; Nance & Straub, 1988), serves as a potent deterrent to potential information security policy violators, and leads to a significant decrease in violations (Straub Jr & Nance, 1990).

Past research was conducted to determine the effect that a threat of punishment or sanctions has on the intended future behavior of individuals in various social, organizational, business and contextual environments (Boss, Galletta, Lowry, Moody, & Polak, 2015; Bridges & Stone, 1986; Erickson, Gibbs, & Jensen, 1977; Maxwell & Gray, 2000). Deterrence theory posits that sanctions, disincentives and the threat of punishments or sanctions serve to discourage would-be violators from engaging in prohibited behavior and supports policy compliance among employees. Also, as the level

of certainty of being caught and severity of the sanction or punishment increases, the level of prohibited activity declines in a corresponding manner.

A key determinant of deterrence effectiveness is clear and efficient communication of the potential sanctions for violations and rewards for compliance, including multiple clearly articulated statements, and follow-up regarding penalties for violators (Chen et al., 2012; Puhakainen & Siponen, 2010; Straub Jr & Nance, 1990). Sanctions include various forms of penalties that the organization imposes on an employee for noncompliance with the established information security policy. These may range from a simple verbal warning to job termination and prosecution under criminal statutes (Bulgurcu et al., 2010b).

The insider threat continues to be one of the most significant threats to organizations (Tsohou et al., 2015; Vance et al., 2013; Willison & Siponen, 2009). Recent studies extended the deterrence theory to investigate whether perceived certainty and severity of organizational sanctions were affected by user awareness of information security countermeasures. Computer users were found to be aware of security policies through training programs and first-hand observation of computer misuse. Also the perceived severity of sanctions was found to be more effective in reducing information systems misuse than actual sanctions (D'Arcy et al., 2009).

Deterrence theory is especially applicable to information systems since 50-75% of all security incidents originate from within the organization by employees and other trusted agents having the access and ability to detect and carry out fraudulent activities (D'Arcy et al., 2009). Studies are consistent in finding that a majority of the potential violators are employees of the firm, and 59% of surveyed employees admit that they

actually steal company data and use it for other than official purposes (Q. Hu, Dinev, Hart, & Cooke, 2012). Early studies indicated that the presumptive certainty of the punishment or sanction by the individual was more effective in deterring undesirable behavior than was the severity (Erickson et al., 1977).

Additional research extended deterrence theory to investigate the effects of perceived certainty and severity of organizational sanctions on user awareness of information systems security countermeasures. They found that computer users were aware of security policies through training programs and observation of computer misuse, and that the perceived severity of sanctions was more effective in reducing information systems misuse than actual sanctions (D'Arcy et al., 2009).

Since the top three most important contributing factors to fraud are lack of internal controls, lack of management review and override of existing internal controls, the human aspect must be considered. However, most academic and practitioner focus has been on technical controls and financial ratios. The aim of this study is to explore the variables the impact the human aspect more, i.e., policy quality and enforcement activities (Association of Certified Fraud Examiners, 2016; Sommestad et al., 2014).

Research Model and Hypotheses

Figure 1 contains the proposed theoretical conceptual research model. Using the theoretical framework of General Deterrence Theory, we will examine how information security policy compliance mediates organizational fraud levels in a sampling of individuals from various organizations.

Four hypotheses will be tested. Table 3 contains the proposed theoretical constructs and definitions.

Table 3

Theoretical Constructs and Definitions

Construct	Definition
Information Security Policy Enforcement	The level of supervisory oversight, monitoring and organizational emphasis placed on information security (Goo et al., 2014).
Information Security Policy Quality	The perceived level of adequacy and completeness of the guidelines that cover all information risk possibilities in an organization (Goo et al, 2014; Chen Ramamurthy & Wen, 2015).
Information Security Policy Compliance	The degree to which employees actually adhere to rules set forth in the specific policy established by the company.
Fraud	Some deceitful practice or willful device resorted to with intent to deprive another of his right, or in some manner to do him an injury. As distinguished from negligence, it is always positive and intentional (Black's Law Dictionary, 2014; Lynch & Gomaa, 2003)

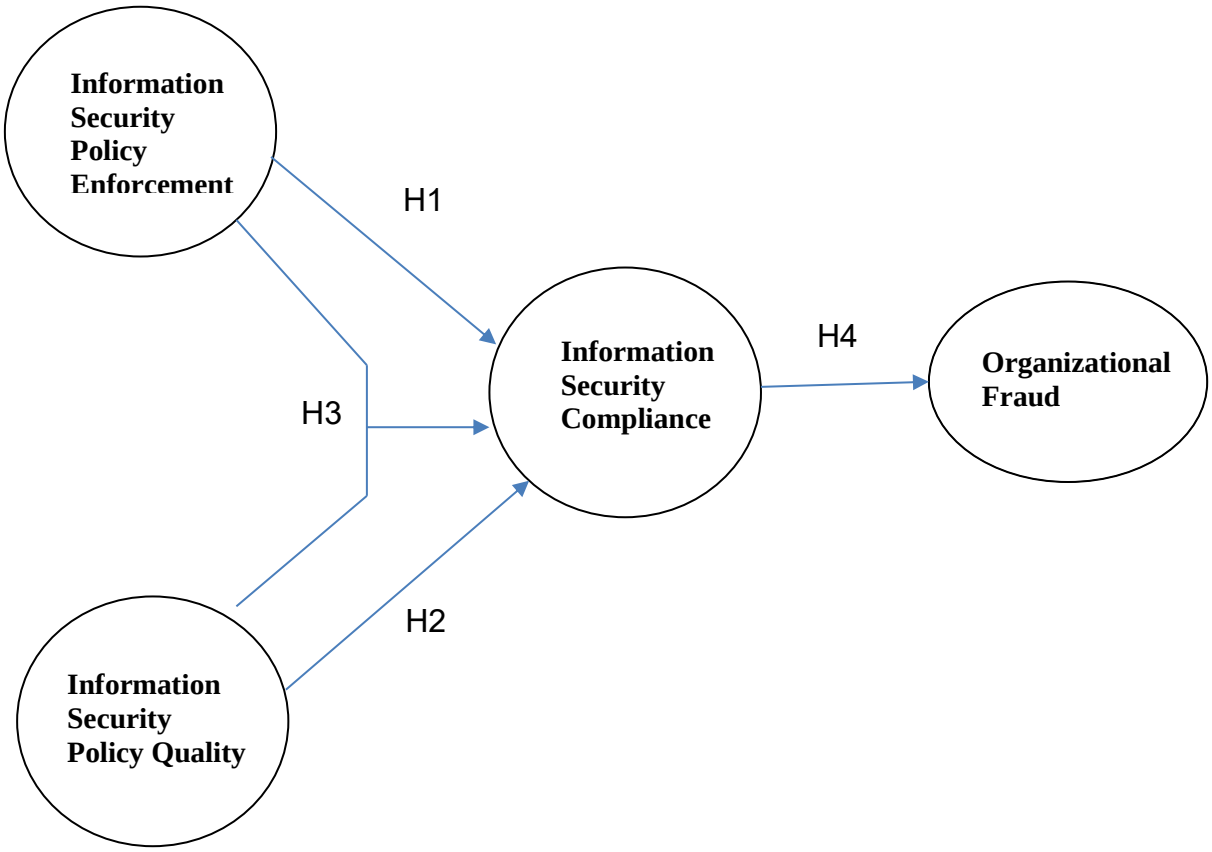
Hypotheses

One of the two main information security issues that businesses must focus on is the protection of data, including proprietary information, employee information, marketing plans, trade secrets, etc. (Dort & Criss). Employee abuse of computers and information systems represents up to 75 percent of security incidents, thereby resulting in significant loss to organizations through fraud and other malicious activities (D'Arcy et al., 2009). Computer abuse includes employee noncompliance with computer security policies, and fraud could be substantially reduced if employees would simply adhere to official

organizational information security policies (Trinkle et al., 2014; Warkentin & Willison, 2009).

Figure 1

Conceptual Model



Quality security monitoring, as one element of strong enforcement, creates an environment where employees perceive they cannot be successful in fraudulent activities. Previous research established that organizational controls (policies and monitoring) increase the level of compliance and reduce the incidence of employee deviance, of which fraud is a key component (Dorminey et al., 2012; Hollinger & Clark, 1982).

Information technology is a powerful tool for monitoring and recording workplace behavior, thereby establishing accountability (Vance et al., 2013). Comparing

daily employee behavior to established standards by monitoring policy compliance increases accountability and identifiability among employees. When employees perceive their activities are recorded, a strong deterrence effect is created, thereby supporting a reduction in antisocial behaviors (Vance et al., 2013). For example, if an employee violates policy to access a customer database outside of their authority, the action would be logged and quickly traced back to the potential fraudster. Monitoring and logging are powerful deterrence tools and research supports their reduction in policy violations (Bulgurcu et al., 2010b).

Policies must be adequately enforced and continuously checked for compliance in order to accomplish intended objectives (Kaplan et al., 2015). Siponen and Vance (2010) found that neutralization is a valid and reliable predictor of individual employee compliance decisions regarding security policies. They conclude that neutralization significantly and positively affects employee intention to violate information security policies. Neutralization enables otherwise conscientious and exacting employees to rationalize and justify violating organizational security policies, which may compromise information and damage the company (M. Siponen & Vance, 2010).

Higher information systems security policy quality positively affects end-user compliance (Bulgurcu et al., 2010b; Goo et al., 2014). When employees feel that significant effort and resources are invested in a security policy, its relevance and enforcement are heightened (Abedin et al., 2006; Bulgurcu et al., 2010b). Internal controls, including continuous monitoring and auditing tools provide strong deterrence and enhance detection of potential fraud perpetrators (Dorminey et al., 2012). Information security breaches enable bribery, embezzlement, espionage and sabotage

opportunities, which accounts for a large percentage of organizational fraud activity (Safa & Maple, 2016). Policy enforcement includes employee understanding of the penalties for noncompliance, including their certainty, celerity, and severity. Greater emphasis on these penalties by supervisors, role models, and peers results in a positive, significant increase in compliance by organizational users (D'Arcy et al., 2009).

Trusted insider employees accumulate access privileges for proprietary databases as their longevity and seniority increases during their tenure. Due to their trusted position and access to increasingly sensitive organizational information, they are often in positions to take advantage of systems and processes to commit fraud (B. W. Carpenter & Mahoney, 2001; Posey et al., 2013). For example, a senior long-term employee who perceives weak internal controls or lack of oversight may recognize the void in accountability as a potential opportunity to engage in fraud. If the appropriate incentive (pressure) is present and the employee is able to rationalize their actions as reasonable, they may be positively influenced to perpetrate fraud. This is especially true if they believe the potential for discovery and punishment with sanctions (severity, celerity and certainty) is not significant. Therefore, H1 is proposed as:

Higher levels of information security policy enforcement results in increased information security policy compliance.

The human element continues to be the top concern among security professionals and top management teams, and employees are the weakest link (Tsohou et al., 2015). Employee failure to comply with information security policies results in the opportunity and provides sufficient rationalization, thereby promoting belief that fraud can be

successfully perpetrated (Johnston et al., 2015; Lynch & Gomaa, 2003; Richardson & Director, 2008).

Many potential fraud events originate with an individual's ability to download sensitive information with little perceived monitoring or accountability. Quality security policies allow only the minimum number of highly vetted employees access to sensitive information based on a bona-fide job requirement and "need-to-know". Often this first line of defense is enough to prevent any further progress toward fraud. Policy quality may offset neutralization in some employees when they perceive strong organizational policy is also routinely enforced (Vance et al., 2013).

When institutional or individual pressure to comply with established policy is perceived as low or insignificant, employees are more likely to attempt fraud. Policy serves to shape employee beliefs regarding management's dedication toward overall information security (Tsohou et al., 2015). Higher quality policy spells out specific expectations that employees must meet; deterrence and the threat of sanctions forces conformance to these requirements and specifications (Crosby, 1979). When effectively deployed, quality information security policies prohibit the unauthorized download of sensitive and valuable proprietary information, including company trade secrets and intellectual property.

Therefore, H2 is proposed as:

Higher levels of information security policy quality increases information security policy compliance.

The strongest and most consistent predictor of actual information security policy compliance is an individual's intent to comply (Sommestad et al., 2014). Intent to comply

is established through several variables. These include having a well-established, quality standard for employees to compare with their daily actions and perceived benefits or sanctions for compliance or non-compliance (deterrence effect).

Consistent with our other hypotheses that increased security policy quality and enforcement individually result in increased compliance, we expect a greater effect when testing the interaction between higher (lower) levels of policy quality and strong (weak) enforcement of the policy. Research findings support that policy quality and enforcement are significant factors in achieving information security policy compliance within organizations (Goo et al., 2014; Tsohou et al., 2015). We hypothesize a significant effect when the constructs of security policy quality and policy enforcement are implemented simultaneously. This synergistic effect is consistent with previous studies where these constructs explained significant variance when individually tested (Sommestad et al., 2014).

General Deterrence Theory suggests that sanctions, disincentives and the threat of various punishments (sanctions) will discourage potential fraudsters from attempting prohibited behavior, thereby supporting policy compliance among employees (Straub & Welke, 1998). When employees feel their supervisors and leadership place a strong emphasis on security and lead by example, they are more likely to comply. When supervisors include elements of security in employee performance appraisals, compliance is increased (Goo et al., 2014).

Therefore, H3 is proposed as:

Higher levels of information security policy quality combined with effective enforcement increases information security policy compliance.

Incentives, opportunity, and rationalization are antecedents that increase the potential for fraud (Accountants, 2002; Cressey, 1950, 1953). Noncompliance weakness is a leading predictor of detrimental incidents, including fraud (Steinbart et al., 2015). Based on current literature, we propose that information security compliance decreases individual opportunity and rationalization, thereby resulting in corresponding decreases in organizational fraud (Otero, 2015).

Computer abuse includes employee noncompliance with computer security policies; fraud could be substantially reduced if employees would adhere to organizational information security policies (Trinkle et al., 2014; Warkentin & Willison, 2009). This “insider threat” is so pervasive that the U.S. Department of Defense (DoD) announced implementation of a new regulation specifically to address the problem. The policy requires organizations doing business with DoD to develop and implement individual programs to detect, deter and mitigate potential insider threats (Tadjdeh, 2016).

A culture of compliance may develop when employees feel that understanding and following established policy is desirable. Past research indicates that information security policy design and implementation are important, and that poor quality results in more security breaches (D'Arcy et al., 2014; Whitman, 2003). The American Institute of Certified Public Accountants (AICPA) clarified auditing standards in AU-C 240 in order to improve auditor effectiveness by enabling them to better identify potential fraud based on the Fraud Triangle. Many of the standards in AU-C 240 specifically address opportunity and motivation and support the proposition that increased levels of policy

enforcement reduces reported organizational fraud levels (Cressey, 1953; Roden et al., 2016).

Information security internal controls serve to limit and reduce the incidence of unethical behavior in organizations predicted by the Fraud Triangle by increasing compliance (Accountants, 2002; Liu et al., 2015). Information technology controls consist of two categories, general and application. General controls are comprehensive and include restricting access, separation of duties based on need, and physical controls. Application controls affect later modification of IT programs (Dickins & Reisch, 2012). The degree of internal control compliance achieved affects the overall fraud levels reported (Liu et al., 2015).

Empirical data supports the proposition that unauthorized access to data and subsequent file transfers offer multiple opportunities to engage in fraud (Lynch & Gomaa, 2003; Tabuena, 2013). Fraud perpetrators having access to valuable account databases often change account values in order to conceal fraud and steal from clients (Steinbart et al., 2015). Limiting access to information systems is one of the most basic forms of control instituted through security policies to protect information resources. Enforcing a policy effectively limiting the number of authorized users also limits the potential for malevolent behaviors leading to fraud. For example, an employee scheming to misappropriate a customer database must violate several policies in order to carry out the fraud. If an employee lacks basic access privileges to the database, then there is no fraud opportunity regardless of their incentive (pressure) and rationalization. Since fraudulent activities are “deliberate and non-random”, there is a tendency for individuals

who do not follow established policy to deviate in other areas of security enforcement (Dilla & Raschke, 2015; Lynch & Gomaa, 2003).

Therefore, H4 is proposed as: *Information security policy compliance is inversely related to reported organizational fraud*.

CHAPTER 3 METHODS

Participants

Data was obtained from a nationwide pool using Qualtrics respondents. The first data set was solicited from various partners in industry whom we knew personally and were willing to participate. This included a wide range of business interests and industries. This initial data is used to perform a pilot survey and an Exploratory Factor Analysis (EFA) for a reliability check of the proposed instrument and to validate the scales (n=360) and derive a more parsimonious model. The second data set is used for the main study (n=400).

Operationalization of the variables

A 7-point Likert Survey Scale was chosen as the appropriate method because the focus of our study seeks individual (employee and management) attitudes and opinions regarding attributes of selected policy characteristics. Survey instruments will assess attitudes and perceptions from both the managerial and employee perspectives toward organizational policy quality, policy enforcement, compliance, and organizational fraud. Survey instruments were adapted using techniques specified by Mackenzie et al. (2011) and Steinbart et al., (2016) (MacKenzie, Podsakoff, & Podsakoff, 2011; Steinbart et al., 2015). Constructs were developed using exacting definitions to capture key aspects of policy security, enforcement, compliance and organizational fraud (MacKenzie et al., 2011). Items were selected to fully represent each information security construct to ensure that the concepts represented by each covary with the pilot test results.

Independent Variables

Information security policy quality.

Information security policy quality is the perceived level of adequacy and completeness of the guidelines that cover all information risk possibilities in an organization (Chen et al., 2012; Chen et al., 2015; Goo et al., 2014). Policy quality is a function of how complete and adequate the policy serves to cover all potential risk situations in the organization (Bulgurcu et al., 2010b; Crosby, 1979). For example, high quality policies require written, mandatory guidelines regarding acceptable parameters for use of organizational computer resources.

The information security policy quality construct measures the extent to which employees perceive that their company's information security policy is comprehensive, effective, protects sensitive information from disclosure, and protects employees and the company from liability due to compromise. Twelve items were adapted from Chen, Ramamurthy & Wen (2015). Each item will be measured on a 7-point Likert scale: 1=strongly disagree, 7=strongly agree.

Information security policy enforcement.

The enforcement construct measures the extent to which employees perceive that employees are aware of, trained to standard, and comply with various rules set forth in the specific policy on a continuous basis. Seven items were adapted from Bulgurcu (2010) to represent the construct). Each item will be measured on a 7-point Likert scale: 1=strongly disagree, 7=strongly agree.

Information security policy compliance.

Information security policy compliance consists of employee perceptions of the degree to which employees actually conform with and abide by the established organizational security policies. Seven items were initially adapted from Herath and Rao (2010) to represent the construct. Each item will be measured on a 7-point Likert scale: 1=strongly disagree, 7=strongly agree.

Dependent Variable – Organizational Fraud

The dependent variable is organizational fraud, which we define here from Black's Law Dictionary as "some deceitful practice or willful device, resorted to with intent to deprive another of his right, or in some manner to do him an injury. As distinguished from negligence, it is always positive, intentional" (Bryan, 2009). Organizational frauds are generally classified into three primary categories: asset misappropriations, corruption and financial statement fraud (ACFE, 2016).

The fraud construct measures the extent to which employees perceive that fraud is possible in their company because of violations of organizational information security policies (lack of compliance). Five items were adapted from Lynch and Gomaa (2003), who performed studies of information technology and its impact on employee behavioral attitudes in predicting computer fraud. Each item will be measured on a 7-point Likert scale: 1=strongly disagree, 7=strongly agree.

Analysis

To analyze the data, we performed Ordinary Least Squares (OLS) Regression to determine if employee perceptions of quality and enforcement are main effects and to determine the extent of their interaction. OLS regression was selected since it minimizes the residuals or differences between predicted and empirical values pertaining to the

dependent variable (JFJ Hair, Black, Babin, & Anderson, 2010). We found significant synergy and interaction effects between policy quality and enforcement as hypothesized. Baker and Wallace (2015) found significant positive correlations between security policy implementation, including enforcement, and lower violation outcomes. They also found that organizations reporting higher quality and levels of technical control were more likely to experience incidents than those with high scores across all three types of controls. This study also supports that an incomplete security program, i.e., less enforcement, is less effective than a more comprehensive program (Baker & Wallace, 2007). We are also testing to see if there is full or partial mediation between the independent variables and the dependent variable by a potential mediating variable (compliance).

CHAPTER 4 RESULTS

This chapter will provide data analysis and findings from the empirical study. First, we discuss the pilot study and associated Exploratory Factor Analysis (EFA). Next, we evaluate the data for assumptions required for Ordinary Least Squares (OLS) regression. We then test each hypothesis using OLS regression and analyze the model for potential partial or full mediation. Finally, we provide findings and results for each of the hypotheses tested.

Issues with the Survey Method

White noise and other potential issues have been discussed in the literature regarding the use of online surveys to collect data (Bertrand & Mullainathan, 2001; Hunter, 2012; Ravallion & Chen, 1997). Cognitive measurement error and "White Noise Error" may be associated with survey questions that potentially affect the validity of survey questions and ultimately the research's outcome. Our Pilot Survey was designed to assess and minimize the effects of white noise within our survey and the results.

Pilot Study and Data Collection

A pilot study was conducted prior to the main study using data from 360 respondents. The number of respondents chosen for the pilot study is based on the minimum number of factor loadings needed for significance, in this case 350 (assuming a minimum factor loading of 0.30). The pilot study was included to reduce measurement error by validating the selected instrument's effectiveness and the value of questions to ensure the research questions are answered adequately (reliability and validity)

(JFJ Hair et al., 2010). Any problems identified with the instrumentation or elements of the data collection technique were corrected prior to the main study. All respondents were employed by various companies nationally. Respondents had the ability to choose from several categories including entry level/junior management/ supervisory, mid-level management, senior-level management (COO, CIO, CFO, etc.), military or academic as listed in Table 4. All respondents were required to use a computer as part of their daily duties and to have a current mandatory information security policy (ISP). The response rate was 63.56% for the pilot survey.

Table 4

Descriptive Statistics for the Pilot Study (N=360)

				Valid	Cumulative
Age		Frequency	Percent	Percent	Percent
Valid	18-30 Years	58	16.1	16.1	16.1
	31-40 Years	101	28.1	28.1	44.2
	41-50 Years	77	21.4	21.4	65.6
	50+ Years	124	34.4	34.4	100.0
	Total	360	100.0	100.0	
Sex					
Valid	Male	258	71.7	71.7	71.7
	Female	102	28.3	28.3	100.0
	Total	360	100.0	100.0	
Time employed by the Company					
Valid	Less than one year	51	14.2	14.2	14.2
	1-3 Years	87	24.2	24.2	38.3
	3-5 Years	60	16.7	16.7	55.0
	More than 5 years	162	45.0	45.0	100.0
	Total	360	100.0	100.0	
Current Job Position					
Valid	Entry-Level/Junior management or supervisory	80	22.2	22.2	22.2

Mid-Level Management	147	40.8	40.8	63.1
Senior-Level Management (COO, CIO, CFO, etc.).	67	18.6	18.6	81.7
Military	13	3.6	3.6	85.3
Academic	53	14.7	14.7	100.0
Total	360	100.0	100.0	

An Exploratory Factor Analysis (EFA) was performed using data from the pilot study on the three independent variables: quality, enforcement, and compliance. A separate EFA was run using the dependent variable (fraud) alone. The purpose was to examine the relationships among the variables and to identify the factors with common patterns in order to reduce the number of factors to the minimum number that will explain the most variance (JFJ Hair et al., 2010; JF Hair, Money, Samouel, & Page, 2011).

The EFA included the original 26 independent variables using Principal Components Analysis with Varimax rotation and Kaiser Normalization (JFJ Hair et al., 2010). Factors with eigenvalues of 1.0 and above were selected from the total variance explained. This initial solution included several variables that had more than one significant loading, i.e., loading on more than one component (PQ8, PQ9, PQ10, PQ11, PQ12). An intermediate step of factor analysis is to reduce or eliminate the significant cross-loadings so that only one significant loading remains for each row of the factor matrix (JFJ Hair et al., 2010). These cross-loading variables were removed from the initial list since they had dual loadings exceeding the threshold of 0.40. The threshold of 0.40 was chosen because factor loadings in the 0.30 to 0.40 range are the minimum for

structure interpretation. Loadings of 0.50 and above are practically significant; and loadings exceeding 0.70 are considered to represent a well-defined structure (JFJ Hair et al., 2010). The next iteration was run after removal of the five significant cross-loading variables. The next iteration resulted in removal of two more cross-loading variables (PQ5, PQ7). The final run resulted in removal of PQ4 and PQ6, which were the final remaining variables cross-loading at a significant level (0.40 and above). None of the remaining independent variables cross-loaded at a significant level and were retained. This resulted in 17 of the original 26 independent variables used for our regression as listed below in Table 5.

Table 5

Cross-Loadings – Final Rotated Solution (EFA)

Constructs	Question Items	*Policy Enforcement (PE)	*Policy Quality (PQ)	*Policy Compliance (COMP)	**FRAUD
*Policy Enforcement (ENF)	E1	**0.58**	0.27	0.03	n/a
	E2	**0.66**	0.32	-0.04	n/a
	E3	**0.81**	0.25	-0.04	n/a
	E4	**0.80**	0.21	-0.07	n/a
	E5	**0.79**	0.24	0.03	n/a
	E6	**0.92**	-0.04	0.02	n/a
	E7	**0.92**	0.04	0.05	n/a
*Policy Quality (PQ)	PQ1	0.32	**0.79**	0.14	n/a
	PQ2	0.22	**0.86**	-0.03	n/a
	PQ3	0.34	**0.71**	0.01	n/a

*Policy Compliance (COMP)	C1	0.23	0.01	**0.81**	**n/a**
	C2	9.17	0.02	**0.80**	**n/a**
	C3	0.12	0.01	**0.84**	**n/a**
	C4	0.12	-0.01	**0.89**	**n/a**
	C5	0.11	0.06	**0.88**	**n/a**
	***C6 Rev Coded	0.13	0.14	**0.87**	**n/a**
	***C7 Rev Coded	0.23	0.11	**0.84**	**n/a**
**FRAUD	F1	n/a	n/a	n/a	**0.69**
	F2	n/a	n/a	n/a	**0.81**
	F3	n/a	n/a	n/a	**0.80**
	F4	n/a	n/a	n/a	**0.81**
	***F5 Rev Coded	n/a	n/a	n/a	**-0.40**

*First EFA using independent variables
**Second EFA using dependent variable, no Varimax rotation
***Three items were reverse-coded

These remaining variables were then used to compute new summated score variables for each construct. These newly computed variables were then used for OLS regression to test each of the hypotheses. Summated score variables are used to help reduce measurement error and to achieve parsimony with the number of variables in the model (JFJ Hair et al., 2010).

After analysis of the scales, three variables (C6, C7 & F5) were identified for reverse coding. This was performed due to the variables being negatively coded, i.e., lower values indicated higher agreement or more positive sentiments (Krosnick, 1999).

A second EFA was performed to analyze the dependent variable (fraud). This was performed separately since it is inappropriate to mix independent and dependent variables in a single EFA and subsequently use the derived factors to support dependence relationships (JF Hair et al., 2011). Since there was only one dependent variable, the solution obtained was not Varimax rotated.

Table 6

Descriptive Statistics (N=400)

Age		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-30 Years	104	26.0	26.0	26.0
	31-40 Years	146	36.5	36.5	62.5
	41-50 Years	76	19.0	19.0	81.5
	50+ Years	74	18.5	18.5	100.0
	Total	400		100.0	100.0
Sex					
Valid	Male	200	50.0	50.0	50.0
	Female	200	50.0	50.0	100.0
	Total	400		100.0	100.0
Time Employed					
Valid	Less than one year	40	10.0	10.0	10.0
	1-3 Years	81	20.3	20.3	30.3
	3-5 Years	85	21.3	21.3	51.3
	More than 5 years	194	48.7	48.7	100.0
	Total	400			100.0
Current Job Position					
Valid	Entry-Level/Junior management or supervisory	149	37.3	37.3	37.3
	Mid-Level Management	160	40.0	40.0	77.3
	Senior-Level Management (COO, CIO, CFO, etc.).	56	14.0	14.0	91.3
	Military	2	5.0	.5	91.8
	Academic	33	8.3	8.3	100.0
	Total	400	100	100.0	100.0

Collection and Analysis

As in the pilot study, all respondents were employed by various companies nationally. Respondents had the ability to choose from several categories including entry level/junior management/ supervisory, mid-level management, senior-level management (COO, CIO, CFO, etc.), military or academic as listed in Table 6. All respondents were

required to use a computer as part of their daily duties and to have a current mandatory information security policy (ISP). 400 respondents answered the survey questions completely, with a response rate of 77.57%.

A test of internal consistency reliability (Cronbach's Alpha) was performed with each of the factors separately. This is to determine whether the items in each scale combined into a single index captures in a consistent manner the respective constructs being measured. The results are reflected below in Table 7. Cronbach's Alpha should be at least 0.70 (0.60 acceptable for exploratory). The overall Cronbach's Alpha is 0.82 which is considered acceptable for our study.

Table 7

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
*0.82	0.83	22

*0.60 acceptable for exploratory research, 0.70 otherwise.

The KMO statistic measures sampling adequacy overall and for each individual variable (Kaiser 1970; Cerny and Kaiser 1977; Dziuban & Shirkey, 1974). KMO values greater than 0.8 are considered good and less than 0.5 must be remediated, possibly by removing the values. Since the overall measure is 0.95, the sample is considered adequate and statistically significant (p = 0.05). Each of the individual Measures of Sampling Adequacy (MSA) produced on the Anti-Image Matrices (Appendix) range from 0.68 to 0.96 and are therefore all considered acceptable measures for our research (Table 8).

Table 8

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.95
Bartlett's Test of Sphericity	Approx. Chi-Square	5138.219
	df	325
	Sig.	.000

Evaluation for Assumptions of Regression Analysis

We evaluated the regression model for assumptions of linearity, homoscedasticity, independence of the residuals, and normality (JFJ Hair et al., 2010). First, we performed Levene's Test of Equality of Error Variances with the results indicated in Table 9 and found no significant difference in the error variance across groups (0.67, p = 0.05).

Table 9

Levene's Test of Equality of Error Variances

Dependent Variable: FRAUD

F	df1	df2	p	Sig.
0.90	379	20	0.05	0.67

Tests the null hypothesis that the error variance of the dependent variable is equal across groups.

a. Design: Intercept + QUALITY + ENFORCEMENT + COMPLIANCE

We then performed an initial check for normality of the error term of the variate by visually examining the normal probability plots of the residuals. The values fall generally along the diagonal line with no substantial or significant departures, meaning that the residuals may represent a normal distribution and the variate meets the assumption of normality (JFJ Hair et al., 2010). A visual inspection of their histograms,

normal Q-Q plots, and box plots demonstrated that the data were approximately normally distributed. In Table 10 we analyzed the standardized residuals for kurtosis and skewness. The z-values were computed by dividing the skewness and kurtosis statistic by the standard error, resulting in z = -1.139 for skewness and z = 1.687, respectively (Cramer & Howitt, 2004; Doane & Seward, 2011). Both of the computed z-values fall within the range of -1.96 to 1.96. Based on these results, our data does not differ significantly from normality. From this we conclude that our data are approximately normally distributed in terms of skewness and kurtosis.

Table 10

Descriptives for Standardized Residuals (Dependent Variable-Fraud)

			Statistic	Std. Error
Standardized Residual for FRAUD	Mean		0.00	0.04
	95% Confidence Interval for Mean	Lower Bound	0.00	
		Upper Bound	0.08	
	5% Trimmed Mean		0.00	
	Median		0.00	
	Variance		0.69	
	Std. Deviation		0.84	
	Minimum		-3.15	
	Maximum		2.24	
	Range		5.38	
	Interquartile Range		0.96	
	*Skewness		-0.14	0.12
	*Kurtosis		0.41	0.24
	Kurtosis z-score		-1.14	
	Skewness z-score		1.69	

*Values within -1.96 to 1.96 support conclusion of normally distributed data

Table 11 lists the Cronbach's Alpha, composite reliability (where provided) and Average Variance Extracted (AVE) for instruments used in past research. Although our values are not quite as high as the constructs previously used, they are well within the acceptable

limits for our research. The fraud construct has not been used as extensively so no data was given for reliability in previous research.

Table 11

Cronbach's Alpha, CFR and AVE for Constructs

Construct	Definition	Cronbach's Alpha	CFR	AVE	Cronbach's Current Study
Information Security Policy Enforcement	The level of supervisory oversight, monitoring and organizational emphasis placed on information security (Bulgurcu, Cavusoglu, & Benbasat, 2010).	0.92 (composite)	n/r	0.90	0.77
Information Security Policy Quality	The perceived level of adequacy and completeness of the guidelines that cover all information risk possibilities in an organization (Chen Ramamurthy & Wen, 2015).	0.79	0.80	0.68	0 .79
Information Security Policy Compliance	The degree to which employees actually adhere to rules set forth in the specific policy established by the company (Herath & Rao, 2009).	0.92	n/r	0.87	0.88
Fraud	Some deceitful practice or willful device resorted to with intent to deprive another of his right, or in some manner to do him an injury. As distinguished from negligence, it is always positive, intentional (Black's Law Dictionary, 2016; Lynch & Gomaa, 2003).	0.78	n/a	n/a	0.75

Regression Model

The initial regression model was stated as: Predicted compliance $Y = b_o + v_1 + v_2 + v_3 + e$

Where:

b_o = constant rate of compliance.
v_1 = change in compliance associated with change in policy enforcement
v_2 = change in compliance associated with change in policy quality
v_3 = (v_1*v_2) change in compliance associated with interaction of quality and enforcement
e = Prediction error (residual)

A simple linear regression was run to evaluate if the enforcement construct predicts compliance, B = 0.73, p = 0.05, (Table 12). A significant regression equation was found, F (1, 398) = 290.75, p = 0.05 with an adjusted R^2 of 0.53. The model indicates a statistically significant relationship between the independent variable (policy enforcement) and compliance (p = 0.05). The Pearson Correlation (Table 12) is 0.74, indicating a significant correlation between enforcement and compliance. Policy enforcement is a significant predictor of compliance. This supports our first hypothesis (H1) that higher levels of information security policy enforcement results in increased information security policy compliance.

Next, a simple linear regression was run to evaluate if the quality construct predicts compliance, B = 0.55, p = 0.05, (Table 12). A significant regression equation was found, F (1, 398) = 114.09, p = 0.05 with an adjusted R^2 of 0.30. The model indicates a statistically significant relationship between the independent variable (policy quality) and compliance (p = 0.05). The Pearson Correlation (Table 12) is 0.54, indicating a significant correlation between quality and compliance. Policy quality is a significant predictor of compliance. This supports our second hypothesis (H2) that higher levels of

information security policy quality results in increased information security policy compliance.

Next, a simple linear regression was run to evaluate the relationship and potential significant interaction effect between quality and enforcement on compliance, B = 0.71, p = 0.05, (Table 12). A significant regression equation was found, F (1, 398) = 265.41, p = 0.05 with an adjusted R^2 of 0.51. The model indicates a statistically significant relationship between the independent variable (interaction effect between policy quality and enforcement) and compliance (p = 0.05). This interaction effect is a significant predictor of compliance. This supports our third hypothesis (H3) that higher levels of information security policy quality combined with increased enforcement results in increased information security policy compliance.

A simple linear regression was run to evaluate if the compliance construct predicts fraud, B = -0.61, p = 0.05, (Table 12). A significant regression equation was found, F (1, 398) = 27.36, p = 0.05 with an adjusted R^2 of 0.28 The model indicates a statistically significant negative relationship between the independent variable (compliance) and fraud, p = 0.05. The Pearson Correlation (Table 12) is -0.530, indicating a significant negative correlation between compliance and fraud. Therefore, our fourth hypothesis (H4) that higher levels of information security policy compliance results in decreased organizational fraud is supported.

Table 12

Regression Results

Variable	Coefficient	Std. Error	t-stat	p-value	Adj. R^2	F-Statistic
ENF-COMP	0.73	0.05	17.05	0.00	0.53	290.75
QUAL-COMP	0.55	0.05	10.68	0.00	0.30	114.09
INTERACT_QUAL_ENF	0.71	0.01	16.29	0.00	0.51	265.41
COMP-FRAUD	-0.61	0.443	-6.739	0.00	0.28	27.36

Table 13

Correlation Matrix

		FRAUD	COMP	ENF	QUAL
Pearson Correlation	FRAUD	1.00	-0.53	-0.36	-0.23
	COMP	-0.53	1.00	0.74	0.54
	ENF	-0.36	0.74	1.00	0.56
	QUAL	-0.23	0.54	0.56	1.00
Sig. (1-tailed)	FRAUD_	.	0.00	0.00	0.00
	COMP	0.00	.	0.00	0.00
	ENF	0.00	0.00	.	0.00
	QUAL	0.00	0.00	0.00	.

A summary of regression results and hypotheses is contained in Table 14. H1, H2 and H3 and H4 were supported. Full mediation was also supported.

Table 14

Summary of Regression Results

Construct	Definition	Supported or Non-Supported
H1	*Higher levels of information security policy enforcement results in increased information security policy compliance.*	Supported
H2	*Higher levels of information security policy quality increases information security policy compliance.*	Supported
H3	*Higher levels of information security policy quality combined with effective enforcement increases information security policy compliance.*	Supported
H4	*Information security policy compliance is inversely related to reported organizational fraud.*	Supported
Mediation	Full Mediation	Supported
	Partial Mediation	Not Supported

CHAPTER 5

DISCUSSION, LIMITATIONS, CONCLUSIONS, AND CONTRIBUTION

This chapter begins with a discussion of the limitations we experienced in conducting our research. We then discuss both the academic and practitioner contributions derived from the research and how it may be used in industry. Next, we discuss future potential research related to information security policy characteristics. Finally, we finish with our conclusions from the research.

Limitations

Empirical data has historically been difficult to obtain in fraud research as respondents are consistently hesitant to report based on fears of compromise and attribution (Moody, Siponen, & Pahnila, 2018). We experienced this phenomenon to be true in our study. However, we were able to somewhat overcome this problem using Qualtrics survey data, which provided an anonymous platform to gather information from respondents who are currently in the workforce. This anonymity served to assuage the respondents inherent fear of attribution, traceability and perceived ramifications potentially resulting from participating in our survey.

We discovered some potential shortcoming of using this anonymous data. Among these were the lack of face-to-face interaction with potential respondents and the ability to glean additional insights beyond the scope of the designed study. For example, face-to-face contact using open-ended questions would allow respondents to volunteer additional information that could lead to further studies and research avenues. However, based on

our initial pilot test of the survey instruments, we were able to validate the instruments and then obtain sufficient data to complete the study. Also, we were not able to analyze and compare the different levels of information security policy quality by actually viewing and rating various organizational policies as we had originally planned.

Another potential limitation is the respondents' lack of vesting and accountability for the outcomes obtained as a result of the answers provided. Since we could not capture specific relationships between the respondents' answer and specific organizations, the data has less overall meaning than if we could pair the results with specific companies, their level of supervisory and managerial security competence, and other variables.

Academic Contribution

There is a shortage of articles related to fraud examination especially as it relates to information systems (Brody, Melendy, & Perri, 2012; G. M. Trompeter et al., 2014). Originally, we set out to provide a unique contribution to the field of fraud study by examining an innovative and unprecedented insight into how the many characteristics of information security policy influences organizational fraud. Our contribution is a modest beginning to exploring additional ways of solving the growing fraud problem in organizations.

A significant finding of this research is that policy compliance reduces organizational fraud. We also found that compliance fully mediates between the independent variables of policy quality and enforcement with fraud. This has practical relevance indicating that more research is needed to determine potential links between fraud and other information security policy characteristics, such as more focus on specific business units. For example, policies that are tailored and provide a much narrower focus

on specific business units may serve to provide the differentiation need to identify and track potential abuses. This is also consistent with past research that the most significant threat from fraud and systems compromise is carried out by trusted insiders (Bulgurcu, Cavusoglu, & Benbasat, 2010a).

Practitioner Contribution

Potential solutions to fraud are increasingly valuable to boards, management, and organizations, both for-profit and not-for-profit. Empirical data is consistent in finding that trusted individuals within the organization are the most likely to violate existing policies and engage in fraudulent activity. The trusted insider is more significant than any known external threats. Focus on the human element within organizations continues to be a top priority and finding improved solutions to the insider threat may be enhanced by closer examination of information security policy characteristics combined with other analytical tools.

Our research could provide significant insight into compliance with the new General Data Protection Regulations (GDPR) by examination in further detail those aspects of security policy characteristics identified (Desai, 2013; Diker Vanberg & Maunick, 2018; Tikkinen-Piri, Rohunen, & Markkula, 2017). Our research indicates that the human element is very important in reducing malicious activities by trusted insiders. The GDPR is “common sense” data security which is directed at controlling the insider threat. It minimizes collection of private personal data and requires that personal data no longer needed must be deleted. It also restricts data access through enforcement of policies, procedures, and processes. Unlike many other security programs, GDPR targets the human side of security, including enforcement and compliance issues. GDPR applies

to all organizations storing and/or processing EU resident's personal data, regardless of the geographic location. Many organizations are unaware that the EU GDPR regulation apply globally. The impact to businesses is comprehensive and will permanently change the way customer data is collected, stored, and used. Organizations offering goods or services to EU residents must comply with GDPR requirements. There are many mandatory policy compliance features in the regulation where our research could be applied, including opt-in consent, data storage and transfer, and many others.

Theoretical Contribution

Our study contributes to General Deterrence Theory (Bridges & Stone, 1986; Maxwell & Gray, 2000) by supporting the premise that sanctions, disincentives and the threat of punishment and/or sanctions serve to discourage potential violators from performing prohibited behavior. Our research supports that the perceived probability of discovery coupled with the severity of the potential advertised sanctions or punishment increases compliance, while the level of prohibited activity declines in a corresponding manner as posited by Straub (Straub & Welke, 1998). Stronger internal controls, better quality policies and more robust policy enforcement serves to deter unethical behavior. Stronger controls may correspondingly reduce the incidence of fraud, especially with enhanced internal monitoring of trusted employees.

Future Research

Our research opens the door to other potential behavioral research areas that are just beginning to be explored. For example, information security policy characteristics could be examined in the context of solo versus collusive frauds and the degree to which these internal controls could serve to reduce anonymity and therefore potential fraud

activities (Bishop, Hermanson, & Riley Jr, 2017). Research that studies specific behaviors of employees when they have greater input into the design and implementation of information security policy would also be a possibility.

Conclusion

As a result of this research, we can conclude that there are significant relationships between certain information security policy characteristics and the degree to which they are enforced. Enforcement may be enhanced if policies are more comprehensive and tailored to the specific duty or function of the employee. The synergistic effect of higher quality policies coupled with increased enforcement may enhance overall compliance. Potential links between compliance and organizational fraud still warrants further study.

The just-released AFCE Report to the Nations indicates that fraud is continuing to increase globally, both in scope and scale. As such, it is imperative that academia, government and business exhaust all efforts to glean effective deterrents and solutions to the problem. Our research is a significant first-step to analyze these relationships since they have not been studied significantly in the past. Gauging from the interest generated from our research, we are confident that this will open up further opportunities to explore possible links between information security policy characteristics and fraud.

REFERENCES

Abbasi, A., Albrecht, C., Vance, A., & Hansen, J. (2012). Metafraud: a meta-learning framework for detecting financial fraud. *Mis Quarterly, 36*(4), 1293-1327.

Abedin, M., Nessa, S., Al-Shaer, E., & Khan, L. (2006). *Vulnerability analysis for evaluating quality of protection of security policies.* Paper presented at the Proceedings of the 2nd ACM workshop on Quality of protection.

Accountants, A. I. o. C. P. (2002). Consideration of fraud in a financial statement audit. Statement on auditing standards 99. 22.

ACFE, A. o. C. F. E. (2016). Report to the Nations on Occupational Fraud and Abuse.

Ahmad, Z., & Norhashim, M. (2008). The control environment, employee fraud and counterproductive workplace behaviour: An empirical analysis. *Communications of the IBIMA, 3*, 145-155.

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*: Inst of Internal Auditors.

Albrecht, W. S., Wernz, G. W., & Williams, T. L. (1995). *Fraud: Bringing light to the dark side of business*: Irwin Professional Pub.

Ashenden, D. (2008). Information Security management: A human challenge? *Information security technical report, 13*(4), 195-201.

Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy and Security, 8*(2), 33-56.

Baker, W. H., & Wallace, L. (2007). Is information security under control?: Investigating quality in information security management. *IEEE Security & Privacy, 5*(1).

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

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management, 15*(5/6), 337-346.

Bertrand, M., & Mullainathan, S. (2001). Do people mean what they say? Implications for subjective survey data.

Bishop, C. C., Hermanson, D. R., & Riley Jr, R. A. (2017). Collusive Fraud: Leader, Incident, and Organizational Characteristics. *Journal of Forensic Accounting Research, 2*(1), A49-A70.

Black's Law Dictionary, H. (2014). Black's law dictionary. In.

Board, P. C. A. O. (2002). Consideration of Fraud in a Financial Statement Audit. AU Section 316. In: PCAOB Washington, DC.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & 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), 151-164.

Bridges, G. S., & Stone, J. A. (1986). Effects of criminal punishment on perceived threat of punishment: Toward an understanding of specific deterrence. *Journal of Research in Crime and Delinquency, 23*(3), 207-239.

Brody, R. G., Melendy, S. R., & Perri, F. S. (2012). Commentary from the American Accounting Association's 2011 annual meeting panel on emerging issues in fraud research. *Accounting Horizons, 26*(3), 513-531.

Bryan, A. G. (2009). Black's Law Dictionary. *St. Paul, MN: West Publishing Company, 9*, 1428.

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

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010b). *Quality and fairness of an information security policy as antecedents of employees' security engagement in the workplace: an empirical investigation.* Paper presented at the System Sciences (HICSS), 2010 43rd Hawaii International Conference on.

Button, M., Lewis, C., Shepherd, D., & Brooks, G. (2015). Fraud in overseas aid and the challenge of measurement. *Journal of Financial Crime, 22*(2), 184-198.

Carpenter, B. W., & Mahoney, D. P. (2001). Analyzing organizational fraud. *Internal auditor, 58*(2), 33-33.

Carpenter, T. D. (2007). Audit team brainstorming, fraud risk identification, and fraud risk assessment: Implications of SAS No. 99. *The Accounting Review, 82*(5), 1119-1140.

Cecchini, M., Aytug, H., Koehler, G. J., & Pathak, P. (2010). Detecting management fraud in public companies. *Management Science, 56*(7), 1146-1160.

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

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems, 55*(3), 11-19.

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

Coopers, P. W. (2014). Global Information Security Survey (2014). In.

Corporation, V. (2016). 2016 Data Breach Investigations Report. 1-85.

Cramer, D., & Howitt, D. L. (2004). *The Sage dictionary of statistics: a practical resource for students in the social sciences*: Sage.

Cressey, D. R. (1950). The criminal violation of financial trust. *American Sociological Review, 15*(6), 740.

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

Cressey, D. R. (1986). Why managers commit fraud. *Australian & New Zealand Journal of Criminology, 19*(4), 195-209.

Crosby, P. B. (1979). Quality is free: The art of marketing quality certain. *New York: New American Library*.

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.

Davis, J. S., & Pesch, H. L. (2013). Fraud dynamics and controls in organizations. *Accounting, Organizations and Society, 38*(6), 469-483.

Debreceny, R. S., & Gray, G. L. (2010). Data mining journal entries for fraud detection: An exploratory study. *International Journal of Accounting Information Systems, 11*(3), 157-181.

Desai, D. (2013). Beyond location: data security in the 21 st century. *Communications of the ACM, 56*(1), 34-36.

DeZoort, F. T., & Harrison, P. D. (2016). Understanding auditors' sense of responsibility for detecting fraud within organizations. *Journal of Business Ethics*, 1-18.

Dickins, D., & Reisch, J. T. (2012). Enhancing Auditors' Ability to Identify Opportunities to Commit Fraud: Instructional Resource Cases. *Issues in Accounting Education, 27*(4), 1153-1169.

Diker Vanberg, A., & Maunick, M. (2018). Data protection in the UK post-Brexit: the only certainty is uncertainty. *International Review of Law, Computers & Technology*, 1-17.

Dilla, W. N., & Raschke, R. L. (2015). Data visualization for fraud detection: Practice implications and a call for future research. *International Journal of Accounting Information Systems, 16*, 1-22.

Doane, D. P., & Seward, L. E. (2011). Measuring skewness: a forgotten statistic? *Journal of Statistics Education, 19*(2).

Doherty, N. F., Anastasakis, L., & Fulford, H. (2011). Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy. *International Journal of Information Management, 31*(3), 201-209.

Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & Security, 25*(1), 55-63.

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.

Dort, K. K., & Criss, J. T. Computer Internet. *The Computer & Internet Lawyer, 33*(7), 9.

Erickson, M. L., Gibbs, J. P., & Jensen, G. F. (1977). The deterrence doctrine and the perceived certainty of legal punishments. *American Sociological Review*, 305-317.

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security*, *61*, 169-183.

Goo, J., Yim, M.-S., & Kim, D. J. (2014). A path to successful management of employee security compliance: an empirical study of information security climate. *IEEE Transactions on Professional Communication*, *57*(4), 286-308.

Hafer, J. C., & Gresham, G. (2012). Managers' and Senior Executives' Perceptions of Frequency and Type of Employee-Perpetrated Information Sabotage and Their Attitudes toward It-The Results of a Pilot Study. *Journal of Behavioral and Applied Management*, *13*(3), 151.

Hair, J., Black, W., Babin, B., & Anderson, R. (2010). Multivariate Data Analysis Seventh Edition Prentice Hall.

Hair, J., Money, A., Samouel, P., & Page, J. (2011). Essentials of business research methods. New York: ME Sharpe. *Inc. New York*.

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

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

Hollinger, R., & Clark, J. (1982). Employee Deviance A Response to the Perceived Quality of the Work Experience. *Work and Occupations*, *9*(1), 97-114.

Holton, C. (2009). Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion dollar problem. *Decision Support Systems*, *46*(4), 853-864.

Höne, K., & Eloff, J. (2002). What makes an effective information security policy? *Network Security*, *2002*(6), 14-16.

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

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, P. J.-H., Hu, H.-f., & Fang, X. (2017). Examining the Mediating Roles of Cognitive Load and Performance Outcomes in User Satisfaction with a Website: A Field Quasi-Experiment. *Management Information Systems Quarterly, 41*(3), 975-987.

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

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

Hunter, L. (2012). Challenging the reported disadvantages of e-questionnaires and addressing methodological issues of online data collection. *Nurse Researcher, 20*(1), 11-20.

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

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

Kadam, A. W. (2007). Information security policy development and implementation. *Information Systems Security, 16*(5), 246-256.

Kaplan, S. E., Pope, K. R., & Samuels, J. A. (2015). An examination of the effects of managerial procedural safeguards, managerial likeability, and type of fraudulent act on intentions to report fraud to a manager. *Behavioral Research in Accounting, 27*(2), 77-94.

Krosnick, J. A. (1999). Survey research. *Annual review of psychology, 50*(1), 537-567.

Lichtenstein, S. (1997). *Developing Internet security policy for organizations.* Paper presented at the System Sciences, 1997, Proceedings of the Thirtieth Hawaii International Conference.

Lindup, K. R. (1995). A new model for information security policies. *Computers & Security, 14*(8), 691-695.

Liu, X. K., Wright, A. M., & Wu, Y.-J. (2015). Managers' Unethical Fraudulent Financial Reporting: The Effect of Control Strength and Control Framing. *Journal of Business Ethics, 129*(2), 295-310.

Lowe, D. J., Pope, K. R., & Samuels, J. A. (2015). An examination of financial sub-certification and timing of fraud discovery on employee whistleblowing reporting intentions. *Journal of Business Ethics, 131*(4), 757-772.

Lynch, A., & Gomaa, M. (2003). Understanding the potential impact of information technology on the susceptibility of organizations to fraudulent employee behavior. *International Journal of Accounting Information Systems, 4*(4), 295-308.

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

Maxwell, S. R., & Gray, M. K. (2000). Deterrence: Testing the effects of perceived sanction certainty on probation violations. *Sociological Inquiry, 70*(2), 117-136.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward A Unified Model of Information Security Policy Compliance. *MIS Quarterly, 42*(1).

Nance, W. D., & Straub, D. W. (1988). *An investigation into the use and usefulness of security software in detecting computer abuse*: University of Minnesota.

Ngai, E., Hu, Y., Wong, Y., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems, 50*(3), 559-569.

Ølnes, J. (1994). Development of security policies. *Computers & Security, 13*(8), 628-636.

Otero, A. R. (2015). An information security control assessment methodology for organizations' financial information. *International Journal of Accounting Information Systems, 18*, 26-45.

PCAOB, P. C. A. O. B. (2016). Auditing Standards *PCAOB Release, 2015*(002), 1-203.

Posey, C., Roberts, T., Lowry, P. B., Bennett, B., & Courtney, J. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors.

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

Purda, L., & Skillicorn, D. (2015). Accounting variables, deception, and a bag of words: assessing the tools of fraud detection. *Contemporary Accounting Research, 32*(3), 1193-1223.

Räisänen, K. (2013). *Standard-Making in Information Security: A.* Paper presented at the Proceedings of the Eighth Pre-ICIS Workshop on Information Security and Privacy.

Ravallion, M., & Chen, S. (1997). What can new survey data tell us about recent changes in distribution and poverty? *The World Bank Economic Review, 11*(2), 357-382.

Ravisankar, P., Ravi, V., Rao, G. R., & Bose, I. (2011). Detection of financial statement fraud and feature selection using data mining techniques. *Decision Support Systems, 50*(2), 491-500.

Rechtman, Y., & Rashbaum, K. N. (2015). Cybersecurity Risks to CPA Firms. *The CPA Journal, 85*(5), 54.

Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIRES: a policy framework for information security. *Communications of the ACM, 46*(7), 101-106.

Richardson, R., & Director, C. (2008). CSI computer crime and security survey. *Computer Security Institute, 1*, 1-30.

Roden, D. M., Cox, S. R., & Kim, J. Y. (2016). The Fraud Triangle as a Predictor of Corporate Fraud. *Academy of Accounting and Financial Studies Journal, 20*(1), 80.

Safa, N. S., & Maple, C. (2016). Human errors in the information security realm–and how to fix them. *Computer Fraud & Security, 2016*(9), 17-20.

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

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

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

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267-270.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM Sigmis Database, 38*(1), 60-80.

Sitorus, T., & Scott, D. (2009). Integrated fraud risk factors and robust methodology: a review and comment. *International Journal of Auditing, 13*(3), 281-297.

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

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2015). SECURQUAL: An instrument for evaluating the effectiveness of enterprise information security programs. *Journal of Information Systems*, *30*(1), 71-92.

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

Straub Jr, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: a field study. *Mis Quarterly*, 45-60.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2012). I-SolFramework: as a Tool for Measurement and Refinement of Information Security Management Standard. *On review paper*.

Susanto, H., Almunawar, M. N., Tuan, Y. C., Aksoy, M., & Syam, W. P. (2011). Integrated solution modeling software: a new paradigm on information security review and assessment.

Swanson, M., Hash, J., & Bowen, P. (2006). *Guide for developing security plans for federal information systems*.

Tabuena, J. (2013). Controls for Protecting Against the Enemy Within. *Compliance Week, 10*(117), 5.

Tadjdeh, Y. (2016). Industry Prepares for New Insider Threat Regulation *National Defense*, *10*(12), 3.

Tarafdar, M., DArcy, J., Turel, O., & Gupta, A. (2015). The dark side of information technology. *MIT Sloan Management Review, 56*(2), 61.

Tayler, W. B., & Bloomfield, R. J. (2011). Norms, conformity, and controls. *Journal of Accounting Research*, *49*(3), 753-790.

Thomason, C. (2013). United States v. Nosal: Separating Violations of Employers' Computer-Use Policies from Criminal Computer Hacking Invasions. *Golden Gate UL Rev.*, *43*, 163.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2017). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*.

Trinkle, B. S., Crossler, R. E., & Warkentin, M. (2014). I'm game, are you? Reducing real-world security threats by managing employee activity in online social networks. *Journal of Information Systems*, *28*(2), 307-327.

Trompeter, G., & Wright, A. (2010). The world has changed—Have analytical procedure practices? *Contemporary Accounting Research*, *27*(2), 350-350.

Trompeter, G. M., Carpenter, T. D., Desai, N., Jones, K. L., & Riley Jr, R. A. (2012). A synthesis of fraud-related research. *Auditing: A Journal of Practice & Theory*, *32*(sp1), 287-321.

Trompeter, G. M., Carpenter, T. D., Jones, K. L., & Riley Jr, R. A. (2014). Insights for research and practice: What we learn about fraud from other disciplines. *Accounting Horizons*, *28*(4), 769-804.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, *24*(1), 38-58.

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

Vance, A., Lowry, P. B., & Eggett, D. (2015). Increasing Accountability Through User-Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations. *Mis Quarterly*, *39*(2), 345-366.

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

Wang, J., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *Mis Quarterly*, *39*(1), 91-112.

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

Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM, 46*(8), 91-95.

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management, 24*(1), 43-57.

Willison, R., & Siponen, M. (2009). Overcoming the insider: reducing employee computer crime through Situational Crime Prevention. *Communications of the ACM, 52*(9), 133-137.

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

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal, 74*(12), 38.

Wood, C. C. (1995). Writing infosec policies. *Computers & Security, 14*(8), 667-674.

Zhao, X., Lynch Jr, J. G., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *Journal of consumer research, 37*(2), 197-206.

APPENDIX 1

EMPLOYEE MEASUREMENT ITEMS AND SCALES

All items use 7-point Likert scales: 1=strongly disagree, 7=strongly agree

Strongly disagree (1)	Disagree (2)	Somewhat disagree (3)	Neither agree nor disagree (4)	Somewhat agree (5)	Agree (6)	Strongly agree (7)

* Denotes survey questions used as a result of Exploratory Factor Analysis (EFA).

Fraud Survey - Qualtrics Respondents

Are you currently working full time? Yes or No.

Skip To: End of Block If Working = No

Do you use a computer for work? Yes or No.

Skip To: End of Block If Work = No

Please complete the following demographic questions. This is very important for us to be able to draw conclusions from the data. Answering these questions will not link your answer to any individual data.

Sex: Male or Female.

Time employed by the company:

Less than one year

1-3 Years

3-5 Years

More than 5 years

The approximate number of personnel employed by my company is:

_____

My current age as of today is:

18-30 Years

31-40 Years

41-50 Years

50+ Years

My current job position is classified as:

Entry-Level/Junior management or supervisory

Mid-Level Management

Senior-Level Management (COO, CIO, CFO, etc.).

Military

Academic

KSU IRB Study #18-021: INVESTIGATING INFORMATION SECURITY POLICY CHARACTERISTICS: DO QUALITY, ENFORCEMENT AND COMPLIANCE REDUCE ORGANIZATIONAL FRAUD? Thank you very much for assisting with this research!

Title of Research Study: Investigating information security policy characteristics: Do quality, enforcement, and compliance reduce organizational fraud?

Researcher's Contact Information: Name, Telephone, and Email. Dennis Brown, 678-557-9844. DBrown3@kennesaw.edu.

Introduction: You are being invited to take part in a research study conducted by Dennis Brown of Kennesaw State University. Before you decide to participate in this study, you should read this form and ask questions about anything that you do not understand. This is an academic study for purposes of partial fulfillment of requirements for the Doctorate of Business Administration (DBA) at Kennesaw State University.

Description of Project

The purpose of the study is to gain insight into potential effect(s) of information

security policy quality and enforcement on policy compliance. Ultimately, we hope to determine potential impacts of policy compliance on organizational fraud.

Explanation of Procedures

You will be asked to complete online a series of questions relating to your job position. Please answer each question honestly and to the best of your ability. It is important to answer all questions, but you may stop answering at any time.

Time Required

The entire questionnaire should take no longer than 20 minutes to complete.

Risks or Discomforts: There are no known risks or anticipated discomforts in this study.

Benefits: Although there are no direct benefits to you for answering the survey questions, you may learn more about yourself and about the topic of fraud and information security policies. Your responses will also help further research in this important and emerging field.

Compensation: Compensation will be offered via your panel membership.

Confidentiality: The results of this participation will be anonymous. Data will not be linked to any individual initially or at any stage of the survey. All data will be aggregated and statistically tested for overall results. IP addresses will not be collected at any time.

Inclusion Criteria for Participation: You must be 18 years of age or older to participate in this study.

Use of Online Survey: IP addresses will NOT be collected. Since there is no need to correlate individual responses with aggregate data, participant responses will be anonymous and not linked to any individual. Research at Kennesaw State University that involves human participants is carried out under the oversight of an Institutional Review Board. Questions or problems regarding these activities should be addressed to the Institutional Review Board, Kennesaw State University, 585 Cobb Avenue, KH3403, Kennesaw, GA 30144-5591, (470) 578-2268 or via e-mail at IRB@kennesaw.edu. PLEASE PRINT A COPY OF THIS CONSENT DOCUMENT

FOR YOUR RECORDS, OR IF YOU DO NOT HAVE PRINT CAPABILITIES, YOU MAY CONTACT THE RESEARCHER TO OBTAIN A COPY

I agree and give my consent to participate in this research project. I understand that participation is voluntary and that I may withdraw my consent at any time without penalty.

I do not agree to participate and will be excluded from the remainder of the questions.

Considering your current position, please rate the extent that you agree or disagree with the following statements below?

Policy Quality (PQ)

*PQ1 My company provides all employees mandatory policies regarding computer usage and proprietary data usage.

*PQ2 My company's written security policy clearly states that employees should only use computer resources (and access data) for job-specific duties.

*PQ3 My company's written policies clearly state what computer resources employees should have access to complete their job duties.

PQ4 My company's written policies specifically forbid employees from accessing computer resources and data that they are not authorized to use in their job responsibilities.

PQ5 My company has a clearly written information security policy that is easy to understand and comply with.

PQ6 My company's Information security policy probably meets internationally recognized technical benchmarks.

PQ7 My company's information security policy informs employees that all use of computer resources will be logged and potentially monitored.

PQ8 My company's information security policy includes a clear and consistent definition of boundaries regarding proper (and improper) employee use of computing assets.

PQ9 My company's information security policy ensures protection and security of sensitive company information.

PQ10 My company's information security policy clearly sets forth disciplinary action and sanctions for policy violations and disclosure.

PQ11 My company's information security policy is comprehensive (covers all important topics of computer and data risk).

PQ12 My company's information security policy is tailored to the different functional areas specific to each business unit.

Enforcement (ENF)

*E1 If an employee were caught violating organizational information security policies, they would be severely punished.

*E2 My company's whistleblower" program is reliable and actively monitored.

*E3 My company actively disciplines employees who break information security policies and rules.

*E4 My company quickly investigates suspected information security policy infractions and always holds employees accountable for violations.

*E5 My supervisor and management are focused on making sure that everyone follows established information security policies and procedures.

*E6 The supervisors and leaders in my organization lead by example in information security policy enforcement.

*E7 My fellow employees are active in information security policy enforcement activities.

Compliance (COMP)

*C1 My company encourages all employees to lead by example to encourage compliance with computer/data use and Information security policies.

*C2 All employees of my company intend to actively protect data and technology resources. (according to the policies)

*C3 I perceive that all employees carry out prescribed information security policies of my company.

*C4 All employees understand the importance of following prescribed information security policy responsibilities at work, which creates a strong culture to meet established standards for computer resources and Information security.

* C5 All employees view meeting established information security policy and computer use as an integral part of their job.

*C6 Employees in my company visit prohibited, non-work related sites (ESPN, Facebook, etc.) even though this may increase the risk to company information system

*C7 Employees in my company play games using online social networks knowing this may compromise company data.

Fraud (FRAUD)

*F1 I am aware of employees of my company using computer resources for personal gain.

*F2 Stealing valuable assets from my employer using the company's computer system would be easy for a manager to accomplish.

*F3 Engaging in fraudulent behavior using my company's computer system would be something that most managers would consider.

*F4 Managers are more likely to engage in fraudulent behavior using my company's computer system if they feel their activities are anonymous.

*F5 Most managers would never engage in fraudulent behavior using our computer systems since they are loyal to the company and stakeholders.

APPENDIX 2

MEDIATION ASSESSMENT

Mediation Assessment

Baron and Kenny (2006) posit that certain tests must be met in order for mediation to be supported. Mediation tests the conditions that 1) the proposed mediator is statistically significant with the independent variables; 2) that the proposed mediator is statistically significant with the dependent variable; and that 3) when the dependent variable is regressed on the proposed mediator and the independent variables, the mediator must be statistically significant. All of these conditions must be present to support a full mediation model (Baron & Kenny, 1986; P. J.-H. Hu, Hu, & Fang, 2017; Zhao, Lynch Jr, & Chen, 2010). Here we test to see if policy compliance either fully or partially mediates between the independent variables, (policy quality and policy enforcement) and the dependent variable, fraud.

Predicted Fraud Incidence $Y = b_o + b_1v_1 + b_2v_2 + b_3v_3 + b_4v_{4+}e$

Where:

b_o = constant rate of fraud incidence independent of policy quality, enforcement, and compliance.
v_1 = change in fraud incidence associated with change in policy enforcement
v_2 = change in fraud incidence associated with change in policy quality
v_3 = change in fraud incidence associated with change in policy compliance
v_4 = change in fraud incidence associated with interaction of quality and enforcement
e = Prediction error (residual)

We calculated an initial multiple regression of quality and enforcement on compliance, B = 0.61 (enforcement) and 0.22 (quality), p = 0.05, (Table 15). A significant regression equation was found, F (1, 398) = 165.52, p = 0.05 with adjusted R^2 of 0.56. The model produces a statistically significant relationship between the independent variables (policy quality and enforcement) and the potential mediator (compliance). This satisfies the first condition to support a finding of mediation.

Table 15

Regression Results for Quality & Enforcement on Policy Compliance (COMP)

Variable	Coefficient	Std. Error	t-stat	p-value	Adj. R^2	F-Statistic
ENF	0.61	0.05	12.28	0.00	0.56	165.52
QUAL	0.22	0.06	4.41	0.00	0.56	165.52

Next, we calculated a regression of fraud on the potential mediator (compliance), B = -0.53, p = 0.05, (Table 16). A significant regression equation was found, F (1, 398) = 80.56, p = 0.05 with adjusted R^2 of 0.28. The model produces a meaningful adjusted R^2 and a statistically significant relationship between the dependent variable (fraud) and the potential mediator (compliance). This satisfies the second condition to support a finding of mediation.

Table 16

Regression Results for Fraud and Compliance (COMP)

Variable	Coefficient	Std. Error	t-stat	p-value	Adj. R^2	F-Statistic
COMP	-0.53	0.29	-8.97	0.00	0.28	80.56

Finally, we calculated a regression of fraud on the mediator (compliance), B = -0.60; quality, B = 0.07; and enforcement, B = 0.05, p = 0.05, (Table 17). A significant regression equation was found, F (3, 396) = 27.36, p = 0.05 with adjusted R^2 of 0.28. The model produces a meaningful adjusted R^2 and a statistically significant relationship between the dependent variable (fraud) and the potential mediator (compliance). Enforcement and quality are not significant. This satisfies the third and final condition to support a finding of mediation. Therefore, compliance fully mediates the relationship between the independent variables (quality and enforcement) and fraud.

Table 17

Regression Results for Quality, Enforcement & Compliance (COMP)- Fraud

Variable	Coefficient	Std. Error	t-stat	p-value	Adj. R^2	F-Statistic
ENF	0.05	0.57	0.56	0.58	0.28	27.36
QUAL	0.07	0.36	0.95	0.34	0.28	27.36
COMP	-0.60	0.44	-6.74	0.00	0.28	27.36