Introduction

Fraud reduces every organization’s ability to reach its full potential. It is a major risk facing business and is increasingly difficult to detect and prevent (Abbasi et al. 2012). Fraud is a latent crime, and its true, complete impact has proved difficult to measure (Davis and Pesch 2013). Fraud impacts society to such a degree that it has effectively reduced overall consumer and investor confidence in core business processes (Albrecht et al. 2008).

The purpose of this research is to examine the impact of information security policy quality and enforcement on information security policy compliance and ultimately on organizational fraud using General Deterrence Theory (GDT). Past research has linked information security policy quality and enforcement to information security policy compliance (Goo et al. 2014); however, any potential relationship between information security policy compliance and fraud has not been studied, although many of the accounting and behavioral “Red Flags” associated with fraud are linked to information security and policy compliance (Dorminey et al. 2012). There has been little research regarding the potential direct and indirect effects of information security noncompliance on organizational fraud. With this study we aim to add key insights into providing deeper understanding of the reasons for information security policy noncompliance and more effective tools to reduce fraud.

Recognizing the tremendous bottom-line impact that organizational fraud continues to have on the profitability of virtually all organizations, researchers and industry field practitioners are working to identify clearer insights into fraud motivation, detection and prevention. Stakeholders are seeking to find deeper actionable solutions beyond the traditional external audits and internal control measures which have failed to stem mounting losses (Abbasi et al. 2012). Therefore, we propose following research question (RQ): How is organizational fraud influenced by information security policy characteristics? This paper is organized beginning with a review of the extant literature. We then propose a research model and hypotheses. We then discuss data collection and propose a potential method to test the hypotheses. Finally, we discuss research limitations and future research.

Literature Review

Multiple methods of fraud detection and prevention have been explored to address increasing trends of organizational fraud (Trompeter et al. 2014). These methods include expanded traditional audits (including more appropriate analytical procedures), automated approaches, data analytics, meta-learning frameworks, and the Analytic Hierarchy Process (Abbasi et al. 2012). Current approaches and potential solutions have not met expectations and require significant improvement to stem rising losses (Abbasi et al. 2012).

General deterrence theory has been used to explain and in some cases predict individual choice of compliance or non-compliance with established rules and law. Significant research has been conducted to determine the effect that a threat of punishment or sanctions has on the intended future behavior of individuals in various social environments and context, including organizational and business (Boss et al. 2009). General deterrence suggests that individuals make an assessment of the potential positive or
negative outcomes of their actions when deciding whether or not to violate a given policy, procedure or rule. Deterrence has predictive ability for specific behaviors of criminal activity, has been successfully extended to the field of information systems (Chen et al. 2012), serves as a potent deterrent to potential information security policy violators, and leads to a significant decrease in violations (Straub & Nance, 1990).

Information security policy is defined as “a statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations” (Bulgurcu et al., 2010, p.527). Information security policy violations may be linked to fraudulent activity of various types (Lynch and Gomaa 2003). Policy compliance is a recognized weakness in most organizations but is increasingly becoming a management and leadership priority. According to Whitman (2003), human failures and insufficient security policies ranked number three and four among information security threats in order of severity, respectively. However, these policy violations and their possible links to organizational fraud have not been studied to a significant degree and require further research.

Research Model and Hypotheses

Our research model at Figure 1 suggests that information security policy compliance mediates the degree of organizational fraud between many antecedents, including policy quality and policy enforcement. Employees and employee behavior, known as the human factor, are well known and established as the weakest links in efforts to achieve higher levels of information security in organizations (Johnston et al. 2015). Multiple environmental and technical controls including leadership, password policies, firewalls, system monitoring, and other non-human factor related controls can only limit data loss to a certain degree.

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). 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., 2010).

Higher information systems security policy quality positively affects end-user compliance (Bulgurcu et al., 2010; 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., 2010). 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). 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).

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.**

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). 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).

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. 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.

Future Research and Limitations

Completion of this research will accomplish several key objectives. First, this study will approach the increasing fraud problem from a totally different perspective that has not been studied previously. It will also expand the body of organizational fraud knowledge by giving insights into the motivation leading to compliance versus noncompliance decisions encountered by employees in various organizational settings. Our research also has limitations. Empirical data regarding actual fraud outcomes is difficult to obtain, so we will rely on perceptions of fraud in the workplace.

REFERENCES


Tabuena, Jose. 2013. Controls for Protecting Against the Enemy Within. *Compliance Week, 10*(117), 42-43.

