


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

Dennis T. Brown

Kennesaw State University, dbrown3@kennesaw.edu

Follow this and additional works at: <https://digitalcommons.kennesaw.edu/ccerp>

 Part of the [Accounting Commons](#), [Information Security Commons](#), [Management Information Systems Commons](#), and the [Technology and Innovation Commons](#)

Brown, Dennis T., "Investigating Information Security Policy Characteristics: Do Quality, Enforcement and Compliance Reduce Organizational Fraud?" (2016). *KSU Proceedings on Cybersecurity Education, Research and Practice*. 12.
<https://digitalcommons.kennesaw.edu/ccerp/2016/Student/12>

This Event is brought to you for free and open access by the Conferences, Workshops, and Lectures at DigitalCommons@Kennesaw State University. It has been accepted for inclusion in KSU Proceedings on Cybersecurity Education, Research and Practice by an authorized administrator of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

Abstract

Occupational fraud, the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets, is a growing concern for all organizations. While the typical organization loses at least 5% of annual revenues to fraud, current methods of detection and prevention are not fully adequate to reduce increasing occurrences. Although information systems are making life easier, they are increasingly being used to perpetrate fraudulent activities, and internal employee security threat is responsible for more information compromise than external threats.

The purpose of this research is to examine how information security policy quality and enforcement impacts compliance and mediates organizational fraud levels in a sampling of small to medium-size firms. We will examine if (1) organizations with low (high) quality information security policy experience lower (higher) information security policy compliance; (2) organizations with strong (weak) enforcement of the existing policy experience lower (higher) levels of information security policy compliance; (3) if there is any significant interaction effect between information security policy quality and enforcement and (4) if perceived information security policy compliance is inversely related to reported organizational fraud.

Completion of this research will approach the fraud problem from a perspective that has not been studied previously and will inform current findings regarding the potential direct and indirect effects of information security noncompliance on organizational fraud by giving insights into the motivation leading to compliance versus noncompliance decisions encountered by employees in various organizational settings.

Disciplines

Accounting | Information Security | Management Information Systems | Technology and Innovation

SUMMARY

Fraud reduces every organization's ability to reach its full potential. It is a major risk businesses face, and is increasingly difficult to detect and prevent. Fraud is a latent crime, with a true, complete impact is difficult to comprehensively measure. Global business costs resulting from fraud exceeded USD\$2.9 trillion or five percent annually as of 2010. Fraud impacts society to such a degree that it has effectively reduced overall consumer and investor confidence in core business processes.

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) and the Theory of Planned Behavior (TPB). Past research has linked information security policy quality and enforcement to information security policy compliance; 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.

Multiple methods of fraud detection and prevention have been explored to address increasing trends of organizational fraud. 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. Current approaches and potential solutions have not fully met expectations and require significant improvement to stem rising losses.

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. It will also give organizations increased insight into prevention and mitigation strategies for this increasingly common and damaging threat.