


Chapter 9

Evaluating the Effectiveness of Deterrence Theory in Information Security Compliance: New Insights From a Developing Country.


Felix Nti Koranteng

*University of Education, Winneba, Kumasi
Campus, Ghana*


Richard Apau

 <https://orcid.org/0000-0002-5621-1435>
*Kwame Nkrumah University of Science and
Technology, Ghana*

Jones Opoku-Ware

 <https://orcid.org/0000-0002-7828-1725>
*Kwame Nkrumah University of Science and
Technology, Ghana*

Akon Obu Ekpezu

 <https://orcid.org/0000-0002-9502-1052>
*Cross River University of Technology, Cross
River, Nigeria*

ABSTRACT

There is a long-held belief that deterrence mechanisms are more useful in developing countries. Evidence on this belief is anecdotal rather than empirical. In this chapter, individual compliance to information system security policy (ISSP) is examined through the lenses of deterrence theory. The effects of certainty of detection and severity of punishment on attitude towards compliance and also ISSP compliance behaviour are investigated. A survey questionnaire was distributed to gather responses from 432 individuals who are staff of a public university in Ghana. The data was analysed using partial least square structural equation modelling (PLS-SEM). The results indicate that severity of punishment has a positive effect on attitude towards compliance and ISSP compliance behaviour. However, certainty of detection neither affected attitude towards compliance nor ISSP compliance behaviour. It is recommended that organizations enhance the severity of sanctions imposed on those who violate ISSPs. Future studies should explore how users apply neutralization techniques to evade sanctions.

DOI: 10.4018/978-1-7998-3149-5.ch009

INTRODUCTION

Globally, businesses rely heavily on Information Systems (IS) to function efficiently. Therefore, the security of these systems remains crucial (Chen, Wu, Chen, & Teng, 2018). Despite increasing investments in intrusion detection and prevention tools, incidences of Information System (IS) breaches continue to rise. This is because intrusion sources and vulnerabilities often originate from individual's activities within the organization. Thus, unacceptable end-user behavior accounts for many security issues in organizations (Safa et al., 2019). Consequently, many organizations employ guidelines and requirements laid out in their IS Security Policy (ISSP) to influence end-user behavior. Nonetheless, users rarely comply with these rules (Willison & Warkentin, 2013). This makes the individual users in organizations the weakest link in information security assurance (Tsohou & Holtkamp, 2018; Yoo, Sanders, & Cerveny, 2018).

Several studies have investigated information security compliance. Whilst some studies acknowledge deterrence mechanisms as effective means of ISSP compliance in organizations (Herath & Rao, 2009a; Safa et al., 2019), other studies contradict this assertion (Chen et al., 2018; Siponen & Vance, 2010; Rajab & Eydgahi, 2019). Therefore, there is dissonance on the effectiveness of deterrence mechanisms in ensuring ISSP compliance. In most instances, the disagreement has been attributed to the differences in geographical boundaries within which prior studies were conducted (D'arcy & Herath, 2011). To explain further, deterrence mechanisms seem to have been less effective in individualist societies than in collectivist (Hofstede, 1983). Therefore, it is anticipated that deterrence mechanisms for encouraging ISSP compliance will likely be more effective in collectivist societies than in individualist ones. Collectivist societies emphasize on cohesiveness among individuals and thus seek to prioritize the interest of the society over the individual good or welfare (Tan, Nainee, & Tan, 2016). On the other hand, individualistic societies tend to produce individuals with self-concepts who are focused on independence rather than interdependence. Therefore, people in individualist societies tend to prioritize the individual good over that of the group or society (Lapidot-Lefler & Hosri, 2016). Afukaar (2003), for instance, has indicated that deterrence mechanisms are effective in influencing ISSP compliance in developing countries since many of these countries are collectivist. This assertion is based on purely anecdotal evidences rather than empirical.

In this regard, this chapter examines ISSP compliance in a developing country through the lens of the classical Deterrence Theory (Higgins, Wilson, & Fell, 2005). It investigates the direct effects of Severity of Punishments and Certainty of Detection on ISSP Compliance Intention and also how Attitude Toward Compliance mediate these relationships. As a first step, relevant literature and theoretical frameworks are presented in the following section. This is followed by an analysis and discussion of the findings based on which conclusions and recommendations are drawn.

LITERATURE REVIEW

In recent years, approaches for ensuring information security have shifted focus from technology to the human perspective. Literature suggests that insiders through their ignorance, negligence or deliberate acts subject organizations' IS to various threats (Safa et al., 2019). Indeed, many security issues are as a result of the actions or inactions of end-users (Cheng, Li, Li, Holm, & Zhai, 2013). Despite the provision of ISSPs which stipulates desired security behavior, end-users mostly choose to engage in abusive behavior. Therefore, many scholars recommend deterrent and preventive approaches (e.g. sanctions) to

10 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/evaluating-the-effectiveness-of-deterrence-theory-in-information-security-compliance/253667

Related Content

Towards a Theory for Explaining Socially-Engineered Cyber Deception and Theft

Paul Danquah, Olumide Babatope Longe, Jojo Desmond Lartey and Peter Ebo Tobbin (2020). *Modern Theories and Practices for Cyber Ethics and Security Compliance* (pp. 44-58).

www.irma-international.org/chapter/towards-a-theory-for-explaining-socially-engineered-cyber-deception-and-theft/253661

The Effect of Privacy Concerns on the Purchasing Behavior Among Malaysian Smartphone Users

Zakariya Belkhamza, Mohd Adzwin Faris Niasin and Sidah Idris (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 1230-1246).

www.irma-international.org/chapter/the-effect-of-privacy-concerns-on-the-purchasing-behavior-among-malaysian-smartphone-users/228780

Futurologist Predictions on Global World Order of Cyborgs and Robots

(2022). *Philosophical Issues of Human Cyborgization and the Necessity of Prolegomena on Cyborg Ethics* (pp. 265-286).

www.irma-international.org/chapter/futurologist-predictions-on-global-world-order-of-cyborgs-and-robots/291953

Introduction to Ransomware

Qasem Abu Al-Haija and Noor A. Jebril (2023). *Perspectives on Ethical Hacking and Penetration Testing* (pp. 139-170).

www.irma-international.org/chapter/introduction-to-ransomware/330263

Cloud Computing and Cybersecurity Issues Facing Local Enterprises

Emre Erturk (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 1777-1799).

www.irma-international.org/chapter/cloud-computing-and-cybersecurity-issues-facing-local-enterprises/228809