


Chapter 17

Exploring the Impact of Security Policy on Compliance

Winfred Yaokumah

 <https://orcid.org/0000-0001-7756-1832>

Pentecost University College, Ghana

Peace Kumah

Ghana Education Service, Ghana

ABSTRACT

Extant studies on compliance with security policies have largely ignored the impact of monitoring, security operations, and roles and responsibilities on employees' compliance. This chapter proposes a theoretical model that integrates security policy, monitoring, security operations, and security roles to examine employees' security compliance. Data were collected from 233 IT security and management professionals. Using partial least square structural equation modelling and testing hypotheses, the study finds that information security policy has significant indirect influence on information security compliance. The effect of security policy is fully mediated by security roles, operations security activities, and security monitoring activities. Security policy strongly influences operations security activities and has the greatest effect on security roles and responsibilities. Among the three mediating variables, monitoring has the most significant influence on security compliance. Conversely, the direct impact of security policy on compliance is not significant.

INTRODUCTION

The failure of employee to comply with information systems security policies is a key concern for organizations (Puhakainen & Siponen, 2010). Information security breaches often result from employees' non-compliance with the security policy. A global survey profiles the nature of data breaches in 19 organizations from 27 countries. The study covers more than 47,000 reported security incidents and 621 confirmed data breaches. The findings reveal that over 50% of the insiders who committed sabotage were formal employees, 70% of Internet Protocol address (IP) theft cases were committed by internal

DOI: 10.4018/978-1-7998-7705-9.ch017

people intended to resign their job, and 75% of attacks were opportunists with financial motives targeting no specific individual or organization (Data Breach Investigations Report [DBIR], 2013). This report heightens the need for organizations to ensure that essential security controls are put in place and security policies are complied with. A recent study found that insiders (current and former employees, third parties) with trusted network access represent a major threat to information security, yet many organisations fail to implement processes and technologies to address internal incidents (PWC Report, 2015). Sometimes, even the organisational efforts to protect information assets from employee security threats may rather encourage the behaviors organizations are attempting to thwart (Lowry et al., 2015).

Compliance with information security policy remains a challenging task (D'Arcy & Greene, 2014). To ensure compliance with security objectives, legal, and regulatory requirements, organizations have established security policies to guide employees' behaviour. The information security policy contains intentions, principles, rules, and guidelines which the management wants the employees to adhere to (Sommestad et al., 2014). It provides management direction and support for information security (ISO/IEC, 2009). It generally describes the acceptable use of computer resources, information security roles and responsibilities, the type of training that employees should have, and the consequences of security policy violation (Sommestad et al., 2015). Providing adequate security to information security requires that technical information systems security and management personnel comply with security measures. For instance, critical data may be put at risk when the technical personnel fail to follow operational procedures, perform vulnerability assessment, check security in the third party products and services, perform regular backups, properly manage user accounts, secure mobile devices that are attached to the organization's productive networks, effectively control malware activities, protect data transfer and network services, monitor, log, and audit information systems regularly. Accordingly, Qing et al. (2011) suggest the development and deployment of more advanced protective technologies and enforcement of effective security policies and procedures.

Although organizations have instituted information security policy and compliance programs (D'Arcy & Herath, 2011; Sommestad et al., 2014), concise models to fulfil the organization's information security policy and compliance efforts are sparse. A major problem with security models is that there are just too many to follow. In just the ISO/IEC 27002:2013 framework, there are 14 major controls, which in itself a challenge for employees to comply with. Information security policy-compliance model for incorporating critical inter-related security measures is necessary for knowledge support in the management of information security in organizations where confidentiality, integrity, and availability are paramount. Therefore, the purpose of this study is to model the impact of information security policy on compliance, focusing on information systems security and management personnel, to understand how the activities of these personnel can influence security compliance. A recent study found that malicious database administrators can bypass the security mechanisms and make hidden modifications to databases, which may be untraceable (Kieseberg et al., 2013). Previous literature on security policy compliance focused on end-users (non-technical users). For instance, D'Arcy and Herath (2011) and Ifinedo (2016) applied deterrence theory; Hedström et al. (2013) applied social action theory (SAT) for management of information security; Sommestad et al. (2014) identified attitudes, intentions or actual behaviour having influence on compliance with information security policy. Also, Sommestad et al. (2015) found that anticipated regret and threat appraisal predict information security policy compliance. Also, organizational justice influences Internet use policy compliance (Li et al., 2014).

However, the actual technical and operations security activities are performed by the security and operations management personnel. This, therefore, suggests that there should be increasing focus on

17 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/exploring-the-impact-of-security-policy-on-compliance/270606

Related Content

A New Approach for Building a Scalable and Adaptive Vertical Search Engine

H. Arafat Ali, Ali I. El Desouky and Ahmed I. Saleh (2008). *International Journal of Intelligent Information Technologies* (pp. 52-79).

www.irma-international.org/article/new-approach-building-scalable-adaptive/2430

A Fuzzy Relational Classifier Based Image Quality Assessment Method

Indrajit De (2017). *Intelligent Analysis of Multimedia Information* (pp. 247-265).

www.irma-international.org/chapter/a-fuzzy-relational-classifier-based-image-quality-assessment-method/159439

Cognitive Parameter Based Agent Selection and Negotiation Process for B2C E-Commerce

Bireshwar Dass Mazumdar and R. B. Mishra (2011). *Intelligent, Adaptive and Reasoning Technologies: New Developments and Applications* (pp. 181-203).

www.irma-international.org/chapter/cognitive-parameter-based-agent-selection/54431

Continuous ACO in a SVR Traffic Forecasting Model

Wei-Chiang Samuelson Hong (2009). *Encyclopedia of Artificial Intelligence* (pp. 410-417).

www.irma-international.org/chapter/continuous-aco-svr-traffic-forecasting/10280

An Analysis of Device-Free and Device-Based WiFi-Localization Systems

Heba Aly and Moustafa Youssef (2014). *International Journal of Ambient Computing and Intelligence* (pp. 1-19).

www.irma-international.org/article/an-analysis-of-device-free-and-device-based-wifi-localization-systems/109625