

Chapter 9

SETA and Security Behavior: Mediating Role of Employee Relations, Monitoring, and Accountability

Winfred Yaokumah

Pentecost University College, Accra, Ghana

Daniel Okyere Walker

Pentecost University College, Accra, Ghana

Peace Kumah

Ghana Education Service, Accra, Ghana

ABSTRACT

This article contends that information security education, training and awareness programs can improve employee security behavior. Empirical studies have analyzed the direct effects of employee security training on security behavior without taking into account the mediating role of employee relations, monitoring, and accountability. Based on employee relations and accountability theories, this study proposes and tests a causal model that estimates the direct effect of employee security training on security behavior as well as its indirect effects as mediated by employee relations, monitoring, and accountability. The empirical analysis relies on a survey data from a cross section of employees from five major industry sectors and a structural equation modeling approach via SmartPLS 3.0. The results show that employee security training has indirect and significant effects on security behavior through its influence on employee relations, monitoring, and accountability. However, the result does not indicate direct and significant effect of security training on employee security behavior.

INTRODUCTION

Organizations rely on information systems to enhance productivity and performance, thereby gaining competitive advantage and achieving strategic goals. Users of information systems are, however, prone to intentional and unintentional security risks. Users tend to be the major contributing factor in many information security breaches (Abawajy, 2014). As such, an increasing amount of attention is being paid to the human side of information security (Marett, 2015). According to Ponemon Institute (2012), employees are the main causes of many data breaches in organizations. Information security breaches often occur in organizations due to employees' ignorance or careless behaviors (Abawajy, 2014). For instance, employee negligence or maliciousness account for 78% of data breaches in organizations (Ponemon Institute, 2012). As a result, organizational leaders are seeking behavioral solutions to effect a positive change in employee behavior toward the security of information resources (Pattinson et al., 2016).

An important aspect of managing employee security behavior in organizations is through security education, training, and awareness. Information security education is the organizational effort at making employees aware of the security environment, policies, and security manuals of the organization (D'Arcy et al., 2009). A growing body of evidence suggests that information security training can be used to improve employee information security behavior (Chen, Ramamurthy & Wen, 2015; Helkala & Bakås, 2014; Tsohou et al., 2015). The main reason organizations provide security education, training, and awareness programs is to change employees' behavior and to reduce employees' undesirable security behavior toward organizational information resources (Abawajy, 2014). Through the use of effective training techniques, employees can be educated on how to make safe information security decisions (Kennedy, 2016).

Employee information security education, training and awareness programs and security behavior continue to be strong themes in the human aspects of information security literature (Boss et al., 2015; Chu & Chau, 2014; Pattinson & Anderson, 2007). However, little attention is being paid to human factors that can influence employee security behavior. Many organizations have established SETA and security monitoring programs to safeguard information resources (Chen, Ramamurthy & Wen, 2015). But the current methods of training employees about information security are apparently failing as the number of employee-related breaches is increasing each year (Kennedy, 2016). Lacey (2010) believes that lack of proper training and supervision are the contributing factors behind many information security breaches. However, Slusky and Partow-Navid (2012) argue that failure of employees to comply with security measures is not due to lack of security training and awareness. Even individuals with security knowledge are unable to draw the necessary conclusions about digital risks when browsing the web (Bennett & Bertenthal, 2016). Thus, there is a significant gap between employee information security training and security behavior (Stanciu & Tinca, 2016). Parsons et al. (2014) suggest that organizations should assess the impact of information security training programs on addressing organizational information security challenges.

According to Meso, Ding and Xu (2013), there is the need for a broader and better training of employees to be able to effectively deal with information security risks. Organizations need to incorporate into security education, training and awareness programs three key interventions (mediators), including establishing closer employee relations, monitoring employees' security behavior, and making employees accountable for security. Employee relations, monitoring, and accountability are core human resource (HR) management activities that can improve employee behavior. Human resource management plays an important role by coordinating the activities (policies and procedures) of the organization, which are

20 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/seta-and-security-behavior/288679

Related Content

Seamlessly Securing Web Services by a Signing Proxy

Mario Jeckle and Ingo Melzer (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications* (pp. 2103-2113).

www.irma-international.org/chapter/seamlessly-securing-web-services-signing/23211

Face Recognition Technology: A Biometric Solution to Security Problems

Sanjay K. Singh, Mayank Vatsa, Richa Singh and K. K. Shukla (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications* (pp. 3968-3999).

www.irma-international.org/chapter/face-recognition-technology/23339

The Influence of Trust in the UTAUT Model

Eduardo Esteva-Armida and Alberto Rubio-Sanchez (2014). *Analyzing Security, Trust, and Crime in the Digital World* (pp. 162-186).

www.irma-international.org/chapter/the-influence-of-trust-in-the-utaut-model/103815

A Critical Review of the Big-Data Paradigm

Ruben Xing, Jinluan Ren, Jianghua Sun and Lihua Liu (2016). *International Journal of Risk and Contingency Management* (pp. 46-59).

www.irma-international.org/article/a-critical-review-of-the-big-data-paradigm/158021

Subjective Attack Trees: Security Risk Modeling Under Second-Order Uncertainty

Nasser Al-Hadhrami (2023). *International Journal of Blockchain Applications and Secure Computing* (pp. 1-27).

www.irma-international.org/article/subjective-attack-trees/320498