Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance

Chul Woo Yoo[a,*], G. Lawrence Sanders[b], Robert P. Cerveny[a]

[a] Department of Information Technology and Operations Management, College of Business, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431, United States

[b] Department of Management Science and Systems, School of Management, University at Buffalo, Jacobs Management Center Buffalo, NY 14260, United States

ARTICLE INFO

Keywords:
Security compliance
Flow
Self-efficacy
Psychological ownership
Security training
Education and awareness effectiveness

ABSTRACT

The purpose of this study is to investigate the impact of flow and psychological ownership on security education, training, and awareness (SETA) effectiveness, self-efficacy, and security compliance intention. The important role of experiencing flow in SETA is presented as focal antecedents of psychological ownership, self-efficacy, SETA effectiveness, and security compliance intention. To achieve these goals, we propose a theoretical framework and analyze survey data to test the hypotheses. Flow components in SETA are extended to include challenge, feedback, autonomy, immersion, and social interaction. The results illustrate that experiencing flow in SETA shows significant relationships with SETA effectiveness and psychological ownership, which in turn positively influence security compliance intention. Appropriate theoretical contributions and managerial implications are also discussed.

1. Introduction

Numerous surveys and research illustrate information security as a very important managerial concern [1–3]. In response, organizations have consistently increased their budgets for information security without satisfactorily addressing the issue [4,5]. Many information security studies describe employee noncompliance with information security policies, insecure user practices and security threat unawareness as main barriers to organizational information assurance [6]. In an attempt to offset such breaches, organizations invest in and conduct employee security education training and awareness (SETA) programs [7,8]. SETA is regarded as one of the most important explicit methodologies that guide employees to achieve the security goals in the workplace [9]. SETA can be defined as an educational program that is designed to reduce security breaches that occur through a lack of employee security awareness.

In information security literature, diverse theoretical approaches, such as deterrence theory [6,10], control theory [11], protection motivation theory [12,13], theory of planned behavior [14], institutional theory [15,16], health belief theory [17], criminology theories [5,18], etc., have been deployed to examine the antecedents of employees' compliance or deviant behaviors. However, only a handful of studies have examined the role of SETA in line with security compliance. For example, D'Arcy et al. [7] investigated the relationship between SETA and IS misuse through the lens of deterrence. Puhakainen and Siponen [8] demonstrated that SETA should use contents and methods that motivate the learners to the systematic cognitive processing of information. Posey et al. [19] examined the influence of SETA frequency on protective motivation factors. These studies provide valid contributions to the literature on information security by showing that SETA increases employees' awareness regarding penalties for noncompliance, security threats, security efficacy, etc. However, these studies did not consider how employees' experience during the SETA participation influences SETA effectiveness and eventually nurtures employees' security behaviors. Considering the effort, time and cost organizations spend on the SETA, examining the antecedents of SETA effectiveness and security behaviors have significant implications for maintaining business continuity.

Numerous studies have reported that security behaviors, including SETA participation and security compliance, are often regarded as an impediment to regular work activities by employees [14,20]. Neglecting this conflict can lead to employees' unwilling and unenthusiastic security behavior, and is not an appropriate strategy for maximizing effectiveness. Instead, recent security environments require employees to be more engaged in SETA and to display ownership over information security in the workplace [21], beyond simply checking in periodically with a few mouse clicks to increase the SETA attendance rate. However, users and managers are unsure as to what types of

[*] Corresponding author.
E-mail addresses: yooc@fau.edu (C.W. Yoo), mgtsand@buffalo.edu (G.L. Sanders), cerveny@fau.edu (R.P. Cerveny).

https://doi.org/10.1016/j.dss.2018.02.009
Received 14 July 2017; Received in revised form 26 February 2018; Accepted 28 February 2018

psychological experience/state influence the effectiveness of SETA and employees' intention to comply with organizational security policies. Therefore, a key question becomes what factor allows SETA to be effective and motivate employees to be more willing to comply with security policies? For this research question, we put SETA effectiveness in the center of our research agenda, and examine the key SETA experiences, and their effect on the employees' psychological state and employees' intentions toward security compliance. To our best knowledge, this question has not been answered in the previous literature of information security.

To explore the focal research question, we approached the issue by focusing on the role of *flow* (here defined as a psychological state of being fully immersed in an activity [22]) and *psychological ownership* (here defined as the internalization of ownership of the object [23]). These two theories are strongly related to the discussion above, but have not been well explored in the domain of information security [24]. We consider that using these two theories is appropriate to the context of this study because both help explain employees' immersive engagement and address the outcomes of that engagement. And the body of these two theory streams provides relevant insights for examining our focal research question. The present study proposes a conceptual framework derived from previous literature that discusses the theoretical underpinnings of both flow and psychological ownership. Since this study views the role of SETA effectiveness as a central premise, we do not attempt to revisit the exhaustive list of the variables (e.g., deterrence, normative influence, threats, etc.) often used to anticipate security compliance in the previous studies, in formulating the focal hypotheses. In order to empirically investigate employees' flow in SETA and psychological ownership, a survey instrument was designed and used to collect data from organizations that adopted flow elements in the SETA.

This study offers two main contributions to the information security literature. First, this study examines how SETA effectiveness and security compliance intention can be enhanced through the lens of flow. Five components that form users' flow were identified and investigated. The results indicate that flow significantly influences users to develop psychological ownership and enhances SETA effectiveness. Secondly, the role of psychological ownership in facilitating SETA effectiveness and security compliance intention is also investigated. By themselves, well-elaborated security policies do not automatically motivate employees to comply with organizational mandates. This study, however, demonstrates that psychological ownership significantly enhances SETA effectiveness and individual employees' willingness to participate in security compliance.

The rest of this paper is structured as follows: the next section reviews previous studies on psychological ownership theory and flow theory. This review provides the theoretical support for the hypotheses tested in this study. The measurement instrument used to test the hypotheses is then described, and the resulting data gathered by application of the instrument is used to test a structural equation model based on the theoretical framework. Finally, the paper ends with discussions on empirical results and accompanying conclusions.

2. Psychological ownership theory

In the management literature, psychological ownership has been examined as an important factor that leads to employees' positive behaviors, such as performance, commitment, and ethical behavior [25]. Psychological ownership is defined as the state in which individuals feel as though the target of ownership is theirs (i.e., “It is mine.”) [26]. A sense of ownership can be perceived with respect to nonphysical targets, such as thoughts or brands, and even to the informational assets of an organization. Researchers have identified a variety of constructs, including important motives, key experiences, and the consequences of psychological ownership [23,26,27]. These findings provide an important baseline to illustrate how flow increases psychological ownership, and how psychological ownership positively influences SETA effectiveness and security compliance.

Firstly, previous literature illustrates that having the experience of engaging in the target implies that an individual invests not only time and physical effort, but also mental energy toward the target object [25]. The engagement of an individual's self into objects causes the self to become one with the object and to develop feelings of ownership toward that object [23]. For example, Moon et al. [28] discussed that the immersive experience is one of the most critical precedents of psychological ownership toward game avatars in the context of massively multiplayer online role-playing games. Rudmin and Berry [29] also suggested that through the process of association, an individual integrates the objects into an artifact of possession. In the process, the individual becomes attached to and has feelings of belongingness with the object [30]. The engagement of the self, allows an individual to see their reflection in the target and feel their own effort in its existence.

Secondly, the previous literature indicates that employees with psychological ownership show positive job performance [31]. Van Dyne and Pierce [32] argued that when individuals have possessive feelings, they proactively put forth efforts to control, enhance, and protect the object of ownership. It has been illustrated that when employees have a sense of psychological ownership toward the organization, it triggers active participation from employees, and leads to high levels of job performance [33]. Psychological ownership literature also demonstrated that increasing job performance by having psychological ownership explains variance beyond that provided by commitment and satisfaction [32].

Lastly, previous literature on psychological ownership shows that having psychological ownership increases ethical and responsible behaviors [23]. For example, it has been demonstrated that employees with strong psychological ownership do not tend to display such behaviors as stealing/damaging the organization's property, intentional errors in work, or cyber loafing [34]. Van Dyne and Pierce [32] argued that when individuals feel ownership toward a social entity (e.g., family, group, organization, or nation), they are likely to engage in ethical behaviors toward that entity. In other words, when an individual's sense of oneness is closely linked to the target, it enhances the person's self-identity and increases the sense of responsibility and ethics [27]. In a similar vein, Anderson and Agarwal [24] showed that psychological ownership toward the Internet and home computers initiate protective security behaviors.

Based on the above discussion, psychological ownership theory has important implications which are relevant for this study. First, previous studies show that having strong engagement lead to psychological ownership. Flow, one of the core variables which will be discussed later, is achieved when individuals focus on certain actions. And the focal activity or task of SETA is learning about securing the organization and its informational assets. Therefore, the immersive experience of engaging in SETA can lead to employees acquiring psychological ownership toward the object. Second, studies indicate that having psychological ownership leads to good performance on a given job. Considering that effectively completing a SETA program is a job given to employees, employees with psychological ownership are expected to complete this job successfully. Third, the literature illustrates the role of psychological ownership in motivating ethical and responsible behaviors. Security compliance cannot be fully achieved by an employee's passive attention. Even under the mandatory context, employees' perception regarding security compliance as extra work or an impediment might result in negative ramifications [20]. Therefore, we consider that psychological ownership can explain security compliance intention beyond that provided by previous studies. Based on the discussion above, we consider psychological ownership as an appropriate conceptual framework for the overarching theory in the study.