



Full length article

An information security knowledge sharing model in organizations

Nader Sohrabi Safa^{*}, Rossouw Von Solms

Centre for Research in Information and Cyber Security, School of ICT, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa

ARTICLE INFO

Article history:

Received 20 August 2015

Received in revised form

12 November 2015

Accepted 16 December 2015

Available online 11 January 2016

Keywords:

Information security

Knowledge sharing

Motivation

Behavior

Organization

ABSTRACT

Knowledge sharing plays an important role in the domain of information security, due to its positive effect on employees' information security awareness. It is acknowledged that security awareness is the most important factor that mitigates the risk of information security breaches in organizations. In this research, a model has been presented that shows how information security knowledge sharing (ISKS) forms and decreases the risk of information security incidents. The Motivation Theory and Theory of Planned Behavior besides Triandis model were applied as the theoretical backbone of the conceptual framework. The results of the data analysis showed that earning a reputation, and gaining promotion as an extrinsic motivation and curiosity satisfaction as an intrinsic motivation have positive effects on employees' attitude toward ISKS. However, self-worth satisfaction does not influence ISKS attitude. In addition, the findings revealed that attitude, perceived behavioral control, and subjective norms have positive effects on ISKS intention and ISKS intention affects ISKS behavior. The outcomes also showed that organizational support influences ISKS behavior more than trust. The results of this research should be of interest to academics and practitioners in the domain of information security.

© 2015 Elsevier Ltd. All rights reserved.

1. Introduction

As the Internet has become an integral commodity in human life, organizational activities rely on the web-based technologies widely. However, information security is still a controversial issue for both users and organizations. Information security refers to defending information from unauthorized access, disclosure, use, modification, disruption, inspection, and perusal. In other words, confidentiality, integrity and reliability of information are important in information security (Von Solms and Van Niekerk, 2013). Information security awareness plays a vital role in mitigating the risk of information security breaches (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014). The Internet is a vast environment with a great potential of information security breaches. Hackers use new and ingenious methods to hack the others' computers or systems in line with their own benefits (Choo, 2011; Safa, Ghani, & Ismail, 2014). Recently, online attackers developed a bogus website and asked users to download free anti-virus software. Many of these people downloaded their fake anti-virus and they lost their private information. Different social engineering methods

and phishing are other examples of users' mistakes in the domain of information security behavior (Islam and Abawajy, 2013). In this dynamic environment, information security knowledge sharing not only increases the level of awareness as an effective approach, but also reduces the cost of information security in organizations. Information security knowledge sharing refers to collaboration with others by sharing our experiences, ideas and knowledge in order to safeguard information assets in organizations (Rocha Flores et al., 2014).

Experts face similar problems in this domain and they should provide proper solutions for them. Preventing the development of the same solutions for similar problems by way of sharing knowledge leads to the avoidance of time-wasting and extra costs (Feledi, Fenz, & Lechner, 2013). This time and funding could be better spent by improving the quality of solutions, instead of reinventing the security wheel. However, the previous study showed that the motivation for knowledge sharing among employees is the important challenge in this realm. Sharing previous relevant experiences in the domain of information security is a valuable resource in information security awareness (Rhee, Kim, & Ryu, 2009; Safa, Sookhak, et al., 2015; Safa, VonSolms, Furnell, 2015).

Tamjidyamcholo, Bin Baba, Shuib, and Rohani (2014) investigated the effect of information security knowledge sharing in the virtual community, and its effect on reducing the risks. They also mentioned the low level of willingness of members to share

^{*} Corresponding author.

E-mail addresses: n.sohrabisafa@gmail.com (N.S. Safa), Rossouw.VonSolms@nmmu.ac.za (R. Von Solms).

knowledge with each other as an important barrier in the information security knowledge sharing. Confidence in one's knowledge ownership, the danger of losing one's job, the perceived cost, unfamiliarity with the subject, one's individual attitude and distrust have been already mentioned as obstacles to knowledge sharing (Amayah, 2013).

In this research, a conceptual framework has been presented that shows how intrinsic and extrinsic motivations, attitude toward information security knowledge sharing, perceived behavioral control, and subjective norms influence information security knowledge sharing intention. In addition, organizational support and trust speed up information security knowledge sharing, as facilitating conditions based on the Triandis model.

The remainder of the paper is organized as follows: The theoretical background comprises Motivation Theory and the Theory of Planned Behavior besides the Triandis' model is described in section two. A research model and the various hypotheses are depicted in section three. The research methodology, data collection and the demography of the participants are discussed in section four. The results of the measurement model, the structural model, as well as statistical tests are presented in section five. Contributions to, and implementation of the research are explained in section six. The conclusion, limitations and future work are all described in section seven.

2. The theoretical background

We have conceptualized information security knowledge sharing under two fundamental theories – the Theory of Motivation and Theory of Planned Behavior. On the other hand, Triandis' model has helped us to improve the model, by considering the facilitating conditions in organizations. Motivation encourages individuals to act in a certain way, and to develop a specific behavior. Knowledge sharing is more likely to occur when individuals are motivated (Chang and Chuang, 2011). The Theory of Planned Behavior explains how attitude, perceived behavioral control, and subjective norms affect individuals' intention toward particular behavior. In this regard, facilitating conditions play an important role in the formation of such behavior. More explanations about the theories and the Triandis model will be presented in the following parts.

2.1. The Theory of Planned Behavior

Individuals' thoughts, feelings, actions and behavior are all influenced by their interaction with other persons. The Theory of Planned Behavior was developed from the Theory of Reasoned Action (TRA); and it describes the changes in human behavior based on the perspective of social influence. In simple words, if people evaluate a behavior as positive (attitude), or they think that significant others want them to perform the behavior (subjective norms); then these should lead to higher intentions; and they would be more likely to do so (Fishbein and Ajzen, 1981). However, there were some arguments against the relationship between intention and actual behavior. Some studies showed that intention cannot be the exclusive determinant of behavior, where an individual's control over his/her behavior is incomplete. Ajzen (1991) developed the Theory of Planned Behavior by considering perceived behavioral control. In this way, the Theory of Planned Behavior can cover non-volitional behavior for predicting behavioral intention and actual behavior.

The Theory of Planned Behavior has been widely applied in the domain of the information system and security in recent years. Several studies have discussed how complying with information security organizational policies forms in organizations based on the

Theory of Planned Behavior (Cox, 2012; Ifinedo, 2014). In other studies, the Theory of Planned Behavior was used to explain knowledge sharing behavior based on attitude, subjective norms and perceived behavioral control (Suhwan Jeon, Kim, & Koh, 2011; Pi, Chou, & Liao, 2013). In this research, the Theory of Planned Behavior has been used to describe how employees engage in information security knowledge sharing in order to mitigate the risk of information security breaches in organizations.

2.2. The Motivation Theory

Previous studies have revealed that the motivations associated with individuals' needs and expectations can encourage people to engage in a specific behavior (Ryan, Lynch, Vansteenkiste, & Deci, 2010). Motivation represents the reasons for people's actions, needs, and desires. Motivation defines the direction and the reasons for a particular behavioral pattern. A motive prompts one to behave in a specific manner. The lack of motivation has been mentioned as an important obstacle for knowledge sharing behavior, regardless of the type of knowledge to be shared (Hung, Durcikova, Lai, & Lin, 2011).

Intrinsic and extrinsic motivations play important roles in the domain of knowledge sharing in organizations (Cabrera, Collins, & Salgado, 2006; Hau, Kim, Lee, & Kim, 2013). In this research, intrinsic and extrinsic motivations have been considered as important factors that affect employees' attitude towards information security knowledge sharing in organizations.

2.3. Triandis' model

Triandis (1980) asserted that facilitating conditions are effective factors which besides the other factors drive a particular behavior. Despite strong intentions, a behavior cannot materialize when there is an obstacle against such a behavior (Su-Hwan Jeon Kim, & Koh, 2011). Facilitating conditions are factors that make an act easy to do. In the context of this research, the facilitating conditions include organizational support and trust among the employees in order to share their knowledge in the domain of information security. Fig. 1 depicts the integrated theoretical background of the research model in a concise format.

3. Research model and hypotheses

The presented study investigates the relationships between intrinsic and extrinsic motivations with attitude on the one hand, and information security knowledge sharing attitudes, perceived behavioral control, and subjective norms with information security knowledge sharing intention, on the other hand. In addition, the research model shows the relationships between information security knowledge sharing intention and facilitating conditions with actual information security knowledge sharing behavior. The structure of the conceptual framework is based on the Motivation Theory, the Theory of Planned Behavior and Triandis' model.

The first four hypotheses correspond with the motivational variables that influence employees' attitude. Extrinsic and intrinsic motivations are two main elements of the Motivation Theory. The next three hypotheses are based on the Theory of Planned Behavior that shows the effect of attitude, subjective norms and perceived behavioral control on information security knowledge sharing intention. Finally, the last three hypotheses depict the effects of ISKS intention on ISKS behavior, trust among employees and organizational support as facilitating conditions in ISKS behavior.

Download English Version:

<https://daneshyari.com/en/article/350252>

Download Persian Version:

<https://daneshyari.com/article/350252>

[Daneshyari.com](https://daneshyari.com)