Chapter 14
A Conceptual Model for the Organizational Adoption of Information System Security Innovations

Mumtaz Abdul Hameed
Technovation Consulting and Training (Private) Limited, Maldives

Nalin Asanka Gamagedara Arachchilage
University of New South Wales, Australia

ABSTRACT

Information system (IS) security threats are still a major concern for many organizations. However, most organizations fall short in achieving a successful adoption and implementation of IS security measures. In this chapter, the authors developed a theoretical model for the adoption process of IS security innovations in organizations. The model was derived by combining four theoretical models of innovation adoption, namely diffusion of innovation theory (DOI), the technology acceptance model (TAM), the theory of planned behavior (TPB), and the technology-organisation-environment (TOE) framework. The model depicts IS security innovation adoption in organizations, as two decision proceedings. The adoption process from the initiation stage until the acquisition of innovation is considered as a decision made by organisation while the process of innovation assimilation is assumed as a result of the user acceptance of innovation within the organization.

INTRODUCTION

Information and computer resources (hardware, software, database, networks, etc.) collectively be referred as Information System (IS) assets (Alshboul, 2010) that need to be protected against malicious attacks such as unauthorised access and improper use. Thus, safeguards of IS assets is a widespread concern for individuals and organisations (Stergioua et al., 2016; Zhang et al., 2016). Research on the preservation of IS assets falls under the theme of IS Security. There are numerous technical measures

DOI: 10.4018/978-1-5225-9742-1.ch014

(software and hardware tools) and non-technical safeguards (physical defences and security procedure) available that provides protection for IS assets. Nevertheless, organisations are still struggling to keep up with threats to their IS assets and security breach incidents that have cost them tens of thousands of dollars in loss (Kaspersky lab, 2015). Previous scholarly contributions have constantly argued that the weakest link in any security plan is the computer users themselves (Almomani et al. 2013a; Almomani et al. 2013b; Arachchilage, 2016; Arachchilage et al., 2016; Gross and Mary, 2007; Wynn et al., 2012). As a matter of fact, computer security education needs to be considered as a means to combat against IS threats (Arachchilage, 2016; Arachchilage and Love, 2013; Arachchilage & Love, 2014; Arachchilage et al., 2016; Ben-Asher & Gonzalez, 2015, Gupta et al., 2016; Gupta et al., 2018; Tewari & Gupta, 2017).

The main focus of IS security is to deploy strategies to protect and safeguard IS assets from vulnerabilities (Alshboul, 2010). However, adoption and implementation of IS security measures in an organisation are a complex process (Hameed & Arachchilage, 2016). Besides, adoption of IS security measures by the individuals and organisations is exceptionally low, considering the efforts put in for developing and implementing such systems (Lee & Kozar, 2008; Tuncalp, 2014). Hence, it is critically important to understand what causes the users accept or reject the organisations IS security measures (Jones et al., 2010). As far as we can tell from the IS security literature that there is no model that fully explains the IS security adoption in organisations. Nonetheless, research on IS innovation has introduced models, theories and frameworks related to the adoption and implementation of IS innovations in organisations (Hameed et al., 2012a). IS scholars define innovation as an idea, a method, a product, a program or a technology that is new to the adopting unit (Damanpour, 1991; Hameed et al., 2012a). Hence, the measures of IS security, undoubtedly, be considered as an IS innovation and the theories based on innovation adoption may obviously be applied in an empirical study on IS security adoption process.

In this research, we aimed to theoretically construct a model for IS security innovation adoption process in organisations, which includes organisational adoption process and the user acceptance of innovation. To this end, we explore the past literature on the stages of innovation adoption, theories of innovation adoption, models of technology acceptance and popular frameworks developed by researchers for organisational adoption, with factors considered to influence IS innovation adoption. This study, then utilised the most suitable concepts and relationships of prominent IS innovation adoption theories and user acceptance models, to explain the process of adoption of IS security innovations in organisations. In addition, this study suggests a number of factors from different context that would either assist or inhibit the process of IS security innovation adoption.

The current study focuses on IS security adoption in organisations. The research makes several contributions to the theory and practice of IS security and innovation adoption research. First, it draws upon and synthesizes the rich literature in IS innovation adoption theories and applied it in the context of IS security innovations. The IS security innovation adoption model proposed is based on the theoretical perspective of four innovation adoption theories. The integrated illustration of these models could methodically be used to examine the adoption process and user acceptance of IS security innovations in organisations. Secondly, the proposed IS security adoption model encompasses both the organisational adoption process and user acceptance of innovation. It is evident from the literature that previous scholarly IS security adoption contributions have on no account addressed organisational adoption process and user acceptance of innovation in a single investigation. Past studies on IS security adoption either examine the processes of adoption of IS security innovation until the acquisition of innovation with no assessment on whether the innovation grows to be part of their regular practice (Lee & Kozar, 2005; Safa et al., 2015). On the other hand, studies on user acceptance have only examined the behaviour and