COMPUTERS & SECURITY 48 (2015) 267–280

Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

# Measuring user satisfaction with information security practices

*Gustavo Percio Zimmermann Montesdioca* [*], *Antônio Carlos Gastaud Maçada* [1]

*Universidade Federal do Rio Grande do Sul (UFRGS-Brazil), Rua Washington Luiz, 855, Porto Alegre, RS 90010-460, Brazil*

ARTICLE INFO

*Article history:*
Received 27 July 2013
Received in revised form
2 October 2014
Accepted 23 October 2014
Available online 4 November 2014

*Keywords:*
User satisfaction
Security practices
Information security
Measurement
Expectation disconfirmation theory
Needs theory
Equity theory

ABSTRACT

Information security is a major concern of organizational management. Security solutions based on technical aspects alone are insufficient to protect corporate data. Successful information security depends on appropriate user behavior while using information systems. User satisfaction is widely used to measure the success of information systems. The objective of this research is to develop a model to measure user satisfaction with information security practices. An instrument was developed based on this model. A survey was conducted, and 173 valid responses were obtained. Structural equation modeling was used for the data analysis. The results indicated that users understand the benefits of information security practices, but the use of information systems with security controls is considered a complex matter, which reduces information systems productivity. The measurement of the user satisfaction with information security practices is a starting point to diagnose the behavior of users in relation to information security, providing metrics to management evaluate the investment in information security training and awareness program.



## 1. Introduction

Information security is a major concern of organizational management. Security solutions based on technical aspects alone are insufficient to protect corporate data. Studies indicate that successful information security can be achieved through a combination of technical and socio-organizational investments that consider the user as an active agent (Bulgurcu et al., 2010; Dhillon, 1999; Spears and Bakri, 2010; Stanton et al., 2004). One of the most relevant variables used to assess the success of information systems is user satisfaction (Delone and Mclean, 1992). Studies using this variable are important because they suggest that user satisfaction results in the use of the information system itself and simultaneously provides data for the investment decision-making process (Doll and Torkzadeh, 1988; Delone and Mclean, 1992).

Information systems produce significant benefits to organizations when the users learn and use all of the system capabilities. However, one risk of corporate system and data protection is the difficulty users may experience in understanding and executing the information security practices that are regulated by corporate security policies (Goel and

* *Corresponding author*. Tel.: +55 51 9328 4131.
E-mail addresses: gustavo.percio@ufrgs.br (G.P.Z. Montesdioca), acgmacada@ea.ufrgs.br (A.C.G. Maçada).
[1] Tel.: +55 51 9996 7657.
http://dx.doi.org/10.1016/j.cose.2014.10.015
0167-4048/

Chengalur-Smith, 2010). Users face pressures to increase productivity at work. Security practices may limit daily activities, forcing users to a choice between system functionality and information security practices (Besnard and Arief, 2004). Understanding the factors that measure user satisfaction with information security practices can help organizations improve information systems functionality, while keeping them safe.

The success of information security depends on appropriate user behavior while interacting with information systems. Investigating the cognitive factors that influence such behavior is important in designing an effective information security policy (Rhee et al., 2009). User satisfaction is widely used to evaluate the cognitive aspects behind the user's utilization of information systems (Au et al., 2008). User satisfaction can provide the data required to align information security policies with user information system needs.

The purpose of this paper is to develop a model to address this gap and measure user satisfaction with information security procedures while using information systems. This study can help security professionals and management with the design of information security policies that leverage the user experience with the information systems and provide data to aid decision making about information security investments. The measurement of the user satisfaction with information security practices is a starting point to diagnose the behavior of users in relation to information security, providing metrics to management evaluate the investment in information security training and awareness program.

This research began with a review of the literature on information security and user satisfaction. The information security review identified the information security management concepts, practices and behavioral factors used to integrate information security and user satisfaction. The user satisfaction review generated three theories of motivation that use satisfaction as an exogenous variable (expectancy disconfirmation theory, needs theory, and equity theory) and as user satisfaction constructs and measurement items. The research model, hypotheses, and instrument[2] were validated with data gathered from academics, information security specialists, researchers, and information systems corporate users. An instrument was developed based on this model. A survey was conducted, and 173 valid responses were obtained. Structural equation modeling was used for the data analysis. The results indicated that users understand the benefits of information security practices, but the use of information systems with security controls is considered a complex matter, which reduces information systems productivity.

Section 2 of this paper presents the conceptual background of user satisfaction and information security. Section 3 presents the research model and hypotheses. The research methods are presented in Section 4. Section 5 presents the results of the structural equation modeling. In Section 6, discussion, implications, and future work are presented. Section 7 presents the conclusion for the paper.

## 2. Background

### 2.1. *Information security*

Solutions based only on technology are not sufficient to guarantee the protection of organizational assets. Information security involves human beings that do not always act as they are supposed to while interacting with information systems (Aytes and Connolly, 2004). Therefore, understanding which factors motivate users to adopt security practices is fundamental to solving information security problems (Bulgurcu et al., 2010). Social rules and interactions in the workplace influence an individual's understanding of information security (Albrechtsen, 2007).

Successful implementation of information security practices requires support and leadership from management. Managers have the responsibility to formulate the strategy for protecting information assets, defining a budget that optimizes corporate information security, and minimizing damage caused by possible attacks (Anderson and Choobineh, 2008). Management uses information security policy to guide and control users' behavior, expressing the values and sets of instructions users must follow (Hedström et al., 2011). Information security management involves implementing policies, processes, and procedures to secure the organization, including the development of the soft skills necessary to manage the personal and social identities of users to meet business objective (Ashenden, 2008). Management efforts aim to teach users the importance of adopting information security practices that are aligned with information security policies (Thomson and Solms, 2005).

One dimension of information security practices is related to user behavior while utilizing information systems and, consequently, corporate data. Such practices involve conscious security behavior while using the information systems (Rhee et al., 2009). User attention to information security is associated with a combination of personal and organizational factors, such as satisfaction with support services, satisfaction with salary, satisfaction with colleagues, organizational commitment, technical knowledge, and emotional events (Stanton et al., 2004). Security practices do not always require technology; preventive behavior can protect information systems, such as choosing safe passwords, backing-up data regularly, and carefully handling files (Ng et al., 2009).

Aytes and Connolly (2004) considered the intention for adopting a secure behavior as a rational choice based on individual perceptions of the usability of security practices and the consequences for not using such practices. Users develop attitudes about information security through interlocking organizational, technological, and individual factors. These factors influence user behavior, affect motivations about work with information security practices, create conflict of interests between information system functionality and information security practices, and influence the effect of documentation and awareness campaigns on security behavior (Albrechtsen, 2007). User behavior is also explained through the concept of

[2] Research instruments are measurement tools designed to produce quantitative descriptions of some aspects of the study population by asking people structured and predefined questions. The measurement tool is a form of survey conducted to advance scientific knowledge (Pinsonneault and Kraemer, 1993).