Computers in Human Behavior 49 (2015) 567–575

Contents lists available at ScienceDirect

Computers in Human Behavior

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

Design and validation of information security culture framework

Areej AlHogail

Department of Information Systems, College of Computing and Information Sciences, King Saud University, P.O. BOX 50333, Riyadh 11523, Saudi Arabia

ARTICLE INFO

Article history:

Keywords:
Information security culture
Information security management
Change management
Human factor
Human behavior

ABSTRACT

Establishing information security culture in organizations impacts employees' perceptions and security behavior in a way that can guard against many information security threats posed by insiders. This paper is concerned with the development of a comprehensive information security culture framework for organizations. The structured STOPE (Strategy; Technology; Organization; People; and Environment) scope has been used as a base for the framework so that the various issues of information security can be integrated. The resulted framework incorporates the four main domains of the human factor diamond: preparedness, responsibility, management, and society and regulations. The framework also incorporates change management principles that guide the cultivation of the information security culture. The framework is validated by surveying experts to provide their views and feedback on the correctness and comprehensiveness of the framework structure and its associated tasks. The framework can assist organizations to develop an effective information security culture that protects their information assets.

1. Introduction

This introductory section has three main parts. The first presents the subject of this paper and emphasizes its importance. The second provides a review of the main available literature associated with the topic considered. The third introduces the work described by this paper.

1.1. Information security culture

The rapid changes in computers and information technology (ICT) continually initiate new risks to the security of information assets. In addition, the use of ICT could make the violation of information security easier, and in some cases, undetectable. Organizations need to enhance their information security capabilities to respond creatively to new challenges and risks to ensure survival in this highly competitive environment. Many technical approaches to security, controls, countermeasures, and safeguards have been introduced, developed, practiced, and learned within organizations; however, this is not enough in the battle to achieve security, as many researchers and experts believe that security is both a "people issue" and "technical issue"(Schultz, 2005).

Information security culture provides a guide and structure to human behavior when interacting with ICT to avoid actions that may cause risks to the security of information assets. The culture that promotes good security-related human behavior through knowledge, artifacts, values, and assumptions is far more effective than regulations that simply mandate employees' behavior. It is apparent that security can only be effective if employees know, understand, and accept the necessary precautions.

Information security culture includes all socio-cultural measures that support technical security methods in order to make information security a natural aspect of employees' daily activities (Schlienger & Teufel, 2003). It involves identifying the security-related ideas, beliefs, and values of the group, which shape and guide security-related behaviors (Ramachandran, Rao, & Goles, 2008). Malcolmson (2009) argued that "Security culture could potentially impact on the security of that organization"; it could affect how employees interact with the organization's systems and procedures at any point in time and results in acceptable or unacceptable behavior.

Information security culture can be defined as follows: "The collection of perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction with information assets in [an] organization with the aim of influencing employees' security behavior to preserve information security" (Alhogail & Mirza, 2014b).

1.2. Literature review

Many studies suggest that implementing information security culture inside organizations would manage and reduce security risks to information assets (Bess, 2009; Da Veiga & Eloff, 2010; Furnell & Thomson, 2009; Knapp, Marshall, Rainer, & Ford, 2006;

E-mail address: alhogail@ccis.imamu.edu.sa

http://dx.doi.org/10.1016/j.chb.2015.03.054
0747-5632/

Ruighaver, Maynard, & Chang, 2007; Zakaria, 2006) and many others. They suggest that organizations need to take formative steps in order to create an environment where security is "everyone's responsibility" and where doing the right thing is the norm (Alfawaz, Nelson, & Mohannak, 2010). Consequently, organizations need a comprehensive framework and guidelines to build a security-aware culture.

While among the literature reviewed, 62 papers that were published in the period of 2003–2013 were focused on information security culture in organizations (Alhogail & Mirza, 2014b). Only 14 papers (22% of the total number of papers) presented a framework. The frameworks discussed different specific issues, and some touched on human components such as awareness and training; however, they did not focus on directing employee behavior. In addition, most of the available frameworks lacked a comprehensive view that integrated humans, organizations, and technology to provide organizations with an all-inclusive framework to aid organizations' information security practitioner in the implementation of an information security culture (Alhogail & Mirza, 2014b).

Alfawaz et al. (2010) studied a user's security behavior and suggested that by strengthening the security culture of an organization's members, significant security gains could be achieved. The effective implementation of an information security culture can lead an employee to act as a "human firewall" that can safeguard organizational information assets (Zakaria, Gani, Nor, & Anuar, 2007). Dojkovski, Lichtenstein, and Warren (2010) suggested that a strong information security culture in organizations might deal with many of the behavioral issues that cause information security breaches in such organizations.

Moreover, organizations should focus on employee behavior, as the organizations' success or failure effectively depends on the things that its employees do or fail to do Da Veiga and Eloff (2010). Although researchers have addressed the role of human behavior in information security, little evidence is available with regard to the application of this knowledge; hence, the topic requires more attention.

Unmanaged change can lead to chaos that exposes critical information assets to security risks. The main objectives of change management are to reduce the risks posed to the information assets by changes in practice and improve the stability and reliability of the working environment as changes are made. Changing employees' behavior to be consistent with information security principles and requirements in a way that information security becomes a natural aspect of daily activities is not easy; it requires a great deal of effort to change attitudes, perceptions, routines, and assumptions in addition to developing new skills and learning. Moreover, it requires interrupting what employees are used to doing do Bennett (2012), Ngo, Zhou, and Warren (2005), Okere, van Niekerk, and Carroll (2012).

The changeover needs to be managed carefully and appropriately to achieve the required strategic goals of creating an information asset-secure environment. However, the literature is lacking in research that is focused on using change management tactics in information security culture implementation. In this study domain, change management principles will be used to guide the changes that are associated with the development of an information security-aware culture inside the organization and to enhance acceptance of and compliance with information security policies and procedures.

1.3. The presented work

Dojkovski, Lichtenstein, and Warren (2006) argued that existing information security culture frameworks are fragmented and usually take a limited view of the involved issues. A deep review of the literature published in the last ten years on the topic supports this claim (Alhogail & Mirza, 2014b). Conceptual frameworks seek to identify and link the complexities of cultural change and the modification of behavior. Based on that, this research aims to present a comprehensive framework that guides organizations and professionals in creating an effective information security culture. The framework consists of five dimensions: strategy, technology, organization, people, and environment (STOPE). Each dimension is composed of a number of related tasks that cover four domains of human behavior factors: preparedness, responsibility, management, and society and regulations. These interact with each other to create an effective information security culture to minimize security threats posed by organizations' insider behavior. Change management should ensure smooth implementation of the information security culture and minimum resistance and change chaos.

This framework shall fill a gap in the knowledge and contribute to the field of information security management. A survey of experts validates the framework by collecting their views on the correctness and comprehensiveness of the framework structure and its associated elements. The following section will introduce the framework.

2. Information security culture framework

Having a secure environment requires a combination of technical controls and human controls in addition to other factors. Most available frameworks have focused on one issue, like the relationship between information security culture and environment, organization, policy, and strategy (see Table 1); therefore, this paper proposes a framework that tries to combine as many issues as possible in one comprehensive framework from a structured point of view; namely, STOPE (Bakry, 2003). It aims to understand the interrelationship and linkage between different factors and issues associated with the information security culture to guide management and professionals in the implementation process. Elements of the STOPE dimensions will be inspired by existing frameworks in addition to new required elements to achieve full coverage of the related issues. Table 1 shows the relationship between the proposed framework and existing frameworks.

2.1. Development principles

This framework is developed based on the STOPE profile and guided by the human factor diamond framework. The change management principles are used as the information security culture development tool. The following sections introduce these development principles to the reader.

2.1.1. STOPE development profile

The STOPE view was created by (Bakry, 2003) as a development profile that has been used in different information systems domains to support the development, transition, integration, or evaluation of different IT problems in fields such as e-government, e-learning, e-readiness assessment, grid computing, ERP, and

Table 1
The relationship of the framework dimensions to existing frameworks.

Dimension	Existing frameworks
Strategy	Martins and Eloff (2002), Von Solms and von Solms (2004), Da Veiga and Eloff (2010) and ISO/IEC 27001:2005
Organization	Van Niekerk and Von Solms (2010)
People	Human Factor Diamond
Environment	Dojkovski et al. (2010), Alfawaz et al. (2010), Alnatheer and Nelson (2009)