Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture

Waldo Rocha Flores*, Egil Antonsen, Mathias Ekstedt

Industrial Information and Control Systems, Royal Institute of Technology, 10044 Stockholm, Sweden

ARTICLE INFO

Article history:
Received 28 October 2013
Received in revised form
5 March 2014
Accepted 7 March 2014

Keywords:
Information security
Knowledge sharing
Cultural differences
Mixed methods research
Partial least squares structural equation modeling
Multigroup analysis

ABSTRACT

This paper presents an empirical investigation on what behavioral information security governance factors drives the establishment of information security knowledge sharing in organizations. Data was collected from organizations located in different geographic regions of the world, and the amount of data collected from two countries – namely, USA and Sweden – allowed us to investigate if the effect of behavioral information security governance factors on the establishment of security knowledge sharing differs based on national culture.

The study followed a mixed methods research design, wherein qualitative data was collected to both establish the study's research model and develop a survey instrument that was distributed to 578 information security executives. The results suggest that processes to coordinate implemented security knowledge sharing mechanisms have a major direct influence on the establishment of security knowledge sharing in organizations; the effect of organizational structure (e.g., centralized security function to develop and deploy uniform firm-wide policies, and use of steering committees to facilitate information security planning) is slightly weaker, while business-based information security management has no significant direct effect on security knowledge sharing. A mediation analysis revealed that the reason for the nonsignificant direct relation between business-based information security management and security knowledge sharing is the fully mediating effect of coordinating information security processes. Thus, the results disentangles the interrelated influences of behavioral information security governance factors on security knowledge sharing by showing that information security governance sets the platform to establish security knowledge sharing, and coordinating processes realize the effect of both the structure of the information security function and the alignment of information security management with business needs.

A multigroup analysis identified that national culture had a significant moderating effect on the association between four of the six proposed relations. In Sweden – which is seen as a less individualist, feminine country – managers tend to focus their efforts on implementing controls that are aligned with business activities and employees' need; monitoring the effectiveness of the implemented controls, and assuring that the controls are not too obtrusive to the end-user. On the contrary, US organizations establish security knowledge sharing in their organization through formal arrangements and structures.

* Corresponding author. Tel.: +46 8 790 68 38; fax: +46 8 790 68 39.
E-mail addresses: waldorf@kth.se (W. Rocha Flores), egila@kth.se (E. Antonsen), mathias.ekstedt@ics.kth.se (M. Ekstedt).

http://dx.doi.org/10.1016/j.cose.2014.03.004

These results imply that Swedish managers perceive it to be important to involve, or at least know how their employees cope with the decisions that have been made, thus favoring local participation in information security management, while US managers may feel the need to have more central control when running their information security function.

The findings suggest that national culture should be taken into consideration in future studies – in particular when investigating organizations operating in a global environment – and understand how it affects behaviors and decision-making.

Introduction

As the technological solutions with the purpose to prevent information system from being compromised have increased in effectiveness and robustness, attackers have been forced to find new means to attain their objectives. Many attackers have started to include social means in their malicious efforts and target employees accessing and using IT products and services (Applegate, 2009). The presence of new ways to compromise information security has moved the attention to a more holistic approach to information security management comprising technological, organizational and social components (Kayworth and Whitten, 2010). A holistic information security management approach emphasizes the importance of taking account of the “human” element when ensuring information security throughout the organization. That is, attitudes, beliefs, norms, behavioral patterns, leadership, culture, employee awareness etc. (e.g., Albrechtsen, 2007; Dhillon and Backhouse, 2001; Siponen, 2005). Several approaches focusing on the “human” side of holistic information security management have, therefore, been proposed by researchers. These approaches can roughly be divided in two categories: (1) information security approaches focusing on the ‘individual’ level of information security to understand why end-users engage in risky behavior; (2) information security approaches focusing on the managerial level to understand which organizational factors determine effective holistic information security management. Puhakainen and Siponen (2010), however, criticized information security approaches as lacking not only theoretically grounded methods, but also empirical evidence on their effectiveness. As a possible consequence of this critique, the recent years have witnessed an increase in investigations that meet these criteria, and have based their analyses on a variety of theories including theory of planned behavior (Bulgurcu et al., 2010), neutralization theory (Siponen and Vance, 2010), learning theory (Warkentin et al., 2011), organizational narcissism (Cox, 2012), and protection motivation theory (Ifinedo, 2012). A dominant part of the studies have focused on the first category (Warkentin and Willison, 2009) – that is, the ‘individual’ level of information security by either testing theories that explain an individual’s compliance/non-compliance to information security policies (e.g., Ifinedo, 2012) or how perceptions of different information security countermeasures such as education and awareness training might lead to a decrease in information system abuse or misuse (e.g., D’Arcy et al., 2008). While these studies have increased the understanding of information system misuse on an end-user level, they do not investigate the effect of factors on a managerial level of information security; e.g., the establishment of organizational structures and governance procedures to ensure that proper interventions are in place to support employees to not engage in risky behavior. Research focusing on behaviors of individuals related to the protection of information and information system assets goes under the name of behavioral information security research (Fagnot, 2008; Crossler et al., 2013). Consequently, the governance of information security behavior is referred to as behavioral information security governance and in line with the terminology used by Mishra and Dhillon (2006).

Existing work related behavioral information security governance have proposed different approaches to help firms organize and structure their information security initiatives. First, conceptual and practical principles that neither are theoretical grounded nor offer empirical evidence have been proposed (e.g., Veiga and Eloff, 2007; Brotby, 2009; Sobh and Elleithy, 2013). Other works have based their empirical studies on best practice frameworks such as ISO/IEC 27002 (e.g., Chang and Ho, 2006; Dzazali and Zolait, 2012), and the use of best practice frameworks have been criticized by Siponen and Willison (2009) for being generic or universal in scope and thus not pay enough attention to the differences between organizations and their information security requirements. Finally, qualitative conclusions have been drawn based on case studies or semi-structured interviews. Warkentin and Johnston (2007) conducted a comparative case study in which information security controls were considered within both a centralized and decentralized governance environment. The study identified, for instance, that users in the later environment are responsible for their own awareness training, while the development and implementation of formal training programs in the centralized environment are only carried out by IT personnel. Werlinger et al. (2009) built an integrated framework of information security challenges based on a total of 18 human, organizational, and technological challenges identified by conducting 36 semi-structured interviews with information security practitioners. Kayworth and Whitten (2010) developed a framework to support the attainment of information security strategy objectives. The components of the framework included nine organizational integration mechanisms (e.g., formal security