Journal of Strategic Information Systems 26 (2017) 39–57

Contents lists available at ScienceDirect

Journal of Strategic Information Systems

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

Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method

Ella Kolkowska, Fredrik Karlsson *, Karin Hedström

School of Business, Örebro University, Fakultetsgatan 1, SE-701 82 Örebro, Sweden

ARTICLE INFO

Article history:
Received 1 September 2014
Received in revised form 16 August 2016
Accepted 29 August 2016
Available online 3 September 2016

Keywords:
Information systems security
Compliance
Goals
Value
Rationale
Method
Security policy

ABSTRACT

Employees' poor compliance with information security policies is a perennial problem. Current information security analysis methods do not allow information security managers to capture the rationalities behind employees' compliance and non-compliance. To address this shortcoming, this design science research paper suggests: (a) a Value-Based Compliance analysis method and (b) a set of design principles for methods that analyse different rationalities for information security. Our empirical demonstration shows that the method supports a systematic analysis of why employees comply/do not comply with policies. Thus we provide managers with a tool to make them more knowledgeable about employees' information security behaviours.

1. Introduction

An organisation's information is often one of its most important assets, yet the number of information security incidents, as well as the financial losses relating to such incidents is increasing (Cisco, 2014; ENISA, 2014; European Commission, 2013; Intel Security, 2014; PwC, 2013). For instance, the Global State of Information Security Survey 2014 (PwC, 2013) reported a 25% increase in security incidents compared with 2012. Furthermore, average financial losses relating to security incidents had increased by 18%. Thus, it is not surprising that information security management, aimed at safeguarding an organisation's information assets, has become a key strategic issue for many organisations (Van Niekerk and Von Solms, 2010). Indeed, it is widely argued that information security, which can be defined as "the protection of information" that minimises "the risk of exposing information to unauthorised parties" (Venter and Eloff, 2003), should be an integrated part of organisational governance (McFadzean et al., 2006; von Solms, 2006).

Because of its military and technical origin, information security is sometimes reduced to "the techniques employed to maintain security within a computer system" (Gollmann, 1999). However, information security in the context of organisational governance is much broader. Today, information security includes both technical and non-technical information-handling activities (Dhillon, 2007). Management of information security therefore embraces various technical, operational, and managerial controls (NIST, 2012) for safeguarding information and preventing the misuse of information systems (Baker and Wallace, 2007). One type of management control is the implementation of policies, rules and guidelines for regulating

* Corresponding author.
E-mail addresses: ella.kolkowska@oru.se (E. Kolkowska), fredrik.karlsson@oru.se (F. Karlsson), karin.hedstrom@oru.se (K. Hedström).

http://dx.doi.org/10.1016/j.jsis.2016.08.005
0963-8687/

employees' information security behaviours (Siponen and Vance, 2010). Despite this, the majority of information security breaches are caused by employees who violate information security policies (Herath and Rao, 2009b; Nash and Greenwood, 2008; Siponen et al., 2014; Stanton et al., 2005). Non-compliance, where employees fail to act according to information security policies, is therefore seen as a serious security problem, particularly in practice (ENISA, 2014; PwC, 2014a; Symantec Corporation, 2014). For instance, the Global State of Information Security Survey 2015 (PwC, 2014b) stated that current employees account for 35% of all security breaches within organisations. Furthermore, ENISA's (2014) incident report showed that, in some sectors, incidents caused by employees who, intentionally or unintentionally, violate information security regulations are among the top five causes of large disruptions in organisations.

The seriousness of this problem also means that employees' non-compliance has received significant attention from researchers (e.g. Crossler et al., 2013; Karjalainen, 2011; Siponen and Vance, 2013). Son (2011) has shown that intrinsic motivation, such as value congruence, explains employees' compliance more effectively than security measures that are rooted in extrinsic motivations such as sanctions. Thus, in terms of information security, it is necessary to recognise different goals and values (i.e., rationalities) as important factors when analysing the reasons for non-compliance (Albrechtsen, 2007; Kolkowska, 2009; Son, 2011; Vaast, 2007; Besnard and Arief, 2004). According to these scholars, tensions exist between the values prescribed in information security policies and those that are actually in use.

Kirlappos et al. (2013) and Hedström et al. (2011) have argued for an alternative to the prevailing centralised and uncontextualised "command-and-control" approach to managing employees' information security behaviour. According to them there is a need for an approach that balances organisational goals (e.g., productivity goals) with those of information security management. Currently, the prioritization of different rationalities is left to individual employees (Kirlappos et al., 2013), thus risking security breaches. To improve compliance, information security management needs to understand the different rationalities that come into play in relation to information security (Besnard and Arief, 2004; Mishra and Dhillon, 2006; Renaud and Goucher, 2012; Vaast, 2007). Consequently, information security managers need methodological support to analyse and understand the different rationalities that exist in their organisations. Such support would help them to improve the alignment of information security policies with the organisation's work practices (Hedström et al., 2011).

Many studies have used existing approaches to analyse employees' compliance (e.g. Myyry et al., 2009; Siponen and Vance, 2010; Son, 2011) by examining rationalities related to employees' information security behaviours. However, only a few studies have sought to address the rationality behind the information security policies (e.g. Albrechtsen and Hovden, 2009; Thomson, 2009). Thus, although most compliance studies describe the research method used, few can claim to offer an explicit method that can be used to guide information security managers' efforts to analyse and understand the rationalities behind employees' non-compliance in relation to information security regulations. In order to be a useful tool, an explicit method needs to include not only a clear description of the steps to be taken, but also a set of concepts to create an analytical focus, and a specific form of notation to document the results (Brinkkemper, 1996).

As argued by Kirlappos et al. (2013) and Hedström et al. (2011), few *comprehensive* information security analysis methods (ISAMs) exist which are aimed at supporting information security managers when carrying out a *systematic analysis* of different rationalities in relation to information security within an organisation. Information security managers are therefore not as well informed as they could be when making decisions about resource allocation to counteract security breaches caused by employee non-compliance. The purpose of an ISAM is therefore to provide management with a tool to analyse the current level of security, as well as provide support for prioritising future information security investments (Siponen et al., 2006). For instance, investment decisions are highly dependent on an ISAM's ability to highlight the relevant information security issues.

Against this backdrop, we elaborate on the design of an ISAM, the Value-Based Compliance (VBC) method for analysing different rationalities in relation to information security compliance. This method provides information security managers with a powerful analytical tool to understand why rationality conflicts exist and the impact they have on employees' compliance. We hope that this tool offers an improved basis for strategic decision making on investment in information security by pointing towards more efficient security solutions that are better aligned with organisational goals and practices. Such solutions can change bad practices by creating better information security policies and work procedures. Ultimately, the VBC method can act as a tool that changes the management of employees' information security behaviour.

This paper is organised as follows. The next section presents an overview of related research. This is followed by a section on our design science research approach. The next two sections are devoted to the VBC method. The first of these covers the method itself, whilst the second reports on the lessons learned from using the VBC method in two hospital cases. This is followed by a discussion section in which we address the implications for practice and research. Finally, we present a short conclusion.

2. Related research

The proposed ISAM needs to be based on a theory that acknowledges the existence of several competing rationalities in an organisation. The Value-Based Compliance theory (Hedström et al., 2011; Karlsson and Hedström, 2008) takes a pluralistic perspective on rationalities in organisations. Thus, employees do not simply serve as the instruments of a particular rationality promoted by one category of managers, such as information security managers. Instead, the VBC theory assumes that employees base their actions on different types of rationalities when complying or not complying with information