Journal of Strategic Information Systems 20 (2011) 373–384

Contents lists available at ScienceDirect

Journal of Strategic Information Systems

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

Value conflicts for information security management

Karin Hedström [a,*], Ella Kolkowska [a,1], Fredrik Karlsson [a,b,1], J.P. Allen [c]

[a] Swedish Business School, Örebro University, 701 82 Örebro, Sweden
[b] University of Skövde, 541 28 Skövde, Sweden
[c] School of Business and Professional Studies, University of San Francisco, 2130 Fulton Street, MH 222, San Francisco, CA 94117-1045, USA

ARTICLE INFO

Article history:
Received 18 October 2010
Received in revised form 27 June 2011
Accepted 28 June 2011
Available online 30 July 2011

Keywords:
Information systems security
Information security
Health care information systems
Values
Value conflicts
Management of information security

ABSTRACT

A business's information is one of its most important assets, making the protection of information a strategic issue. In this paper, we investigate the tension between information security policies and information security practice through longitudinal case studies at two health care facilities. The management of information security is traditionally informed by a control-based compliance model, which assumes that human behavior needs to be controlled and regulated. We propose a different theoretical model: the value-based compliance model, assuming that multiple forms of rationality are employed in organizational actions at one time, causing potential value conflicts. This has strong strategic implications for the management of information security. We believe health care situations can be better managed using the assumptions of a value-based compliance model.

1. Introduction

A business's information is one of its most important assets. Extensive research has therefore emphasized the strategic value of information and information systems (Glazer, 1993; McFadzean et al., 2006; Nadiminti et al., 1996; VanWegen and deHoog, 1996). This together with the advance and complexity of networking technologies, which create opportunities for attacks and security breaches causing great financial losses, make information security an important strategic issue (Hu et al., 2007; Posthumus and von Solms, 2004; van Niekerk and von Solms, 2010). Indeed, the Journal of Strategic Information Systems had a special issue on security and privacy pointing at the strategic importance of information security (Dhillon et al., 2007).

While the technical parts of information security often are integrated in corporate governance, little efforts has been made to address the non-technical issues as a strategic concern (Dhillon, 2007). At the same time, previous research shows that the majority of information security breaches are caused by incidents originating inside the organization (Nash and Greenwood, 2008; Stanton et al., 2005), where internal staff are identified as the most significant threat to information security (Gaunt, 2000; Williams, 2008). The behavioral and social aspects of information security are thus seen as critical for creating secure information systems in practice (e.g., Hu et al., 2007; Siponen et al., 2008; Stanton et al., 2005).

Security policies and codes of conducts are frequently the main, or only, tool used by managers to guide and control employees' security behaviors. The security policies and procedures of an organization embed underlying assumptions and beliefs about how to manage information security (von Solms and von Solms, 2004). In other words, security policies and regulations are expressions of values, as well as sets of instructions. Employees' security behaviors are also expression

* Corresponding author. Tel.: +46 19 30 12 41; fax: +46 19 33 25 46.
E-mail addresses: karin.hedstrom@oru.se (K. Hedström), ella.kolkowska@oru.se (E. Kolkowska), Fredrik.karlsson@oru.se (F. Karlsson), jpallen@usfca.edu (J.P. Allen).
[1] Tel.: +46 19 30 12 41; fax: +46 19 33 25 46.

0963-8687/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.jsis.2011.06.001

of values—values related to their profession. The security behavior of users is integrated in, and enacted through, the daily activities of their practice. User behavior with respect to security policies, i.e., compliance, has been recognized as an important and under-studied area for information security research (Herath and Rao, 2009; von Solms and von Solms, 2004). This research responds to this call for information security research to investigate user compliance and security practices as part of people's everyday activities (de Paula et al., 2005). We also want to argue, based on the strategic importance of securing information assets, that the management of information security should be integrated as part of corporate governance as it is closely related to the regulatory and legal development of an organization (von Solms, 2006).

The purpose of this paper is to create new conceptual and practical tools for managing the tension between information security policies as put forward by organizations, and the daily practice of information use by its employees. Our main theoretical contribution is to offer a new value-based compliance model for information security management. We argue that the state-of-the-art in information security management is based on what we define as a control-based compliance model. The control-based compliance model relies on the enforcement of bureaucratic rules to ensure proper information security, where security is seen as the most important value enacted by users in their daily work. This control-based model views humans, and human behavior, as something to be controlled and regulated (see e.g., Bakker, 1998; Luethi and Knolmayer, 2009).

Drawing upon the value-based compliance model, we propose a new technique for mapping complex security situations in an organization. The technique maps areas of agreement or conflict between espoused theories of information security, and the theories-in-use that guide actual user behavior. Following the call for more empirical research on the implementation and use of information security policies within healthcare (de Lusignana et al., 2007), we map areas of conflict related to the goals and values underlying security practice in a hospital setting. Using data from two longitudinal case studies of information security practice in a hospital, we map the security values underlying information security policies and regulations, the health care values held by practitioners, and the areas of conflict between the two.

By showing examples of where practitioners chose not to comply with policies and regulations, thus choosing health care values over information security values, we contribute toward a new view on the management of information security. This view is based on a value-based compliance model that acknowledges, and draws upon, the different values of the information security management and the users' work practice. The value-based compliance model, and its specific mapping techniques, can serve as the basis for professional reflection-on-action that can improve information security in ways that respect the deeply-held values of health care professionals.

1.1. Information security and values

Values, as prioritized concepts or beliefs about end states or behaviors that transcend specific situations, are a foundational concept for organizational research (e.g., Agle and Caldwell, 1999). Values have increasingly been used within information systems (IS) research (Friedman et al., 2006; Hedström, 2007) and information security research (Dhillon and Torkzadeh, 2006; Mishra and Dhillon, 2006) to understand behavior in complex situations where actors face multiple priorities and multiple choices for action. Value conflicts have also been found in studies of health information systems (HIS) use, for example in tensions between information availability and confidentiality (Mommens, 1999).

Although users are put forward as the most important aspect to address within information security, users are commonly viewed as a 'people problem' (Scheiner, 2000), and not as a resource to be drawn upon in the management of information security. Seeing users as a 'problem' makes it necessary to develop security measures based on a *control-based compliance model,* where the primary managerial concerns are user control and regulation in order to enforce policy. A control-based compliance model manages information security through the use of sanctions, controls and regulation of users (e.g., Boss et al., 2009; Herath and Rao, 2009; Straub, 1990). We argue that user violations of information security policies and regulations within health care organizations are not always best managed through a control-based compliance model. We offer an alternative model – *the value-based compliance model* – which assumes that groups within an organization, particularly users and managers, act based on their different values (see also Vaast, 2007). If the value-based compliance model identifies value conflicts as the fundamental driver of behavioral information security problems, this implies that creating a secure information security environment in health care will require reflecting on, and re-examining, values. This redefines the information security management problem as having a significant organizational change and development component, implying that changing peoples' daily practice is best addressed through an understanding of the values that guide their behaviors.

1.2. A value-based compliance model – information security as mediating different rationalities

Health care professionals need to have timely access to accurate patient information. At the same time, those responsible for information security have a duty to prevent unauthorized access to health care information, and to ensure the information's integrity, and confidentiality. Balancing these demands is a major challenge for successful information use in health care (Gaunt, 2000).

Not all groups perceive information security in the same way. Previous research 'suggests that information security holds different meanings for different occupational communities' (Vaast, 2007). This is supported by Albrecthsen and Hovdena (2009) who argue that because users and information security managers have different responsibilities, their actions are based on different rationalities. This difference in rationalities can also be seen where demands between information