Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Practice-based discourse analysis of information security policies

Fredrik Karlsson [a,*], Karin Hedström [a], Göran Goldkuhl [b]

[a] CERIS, Department of Informatics, Örebro University, SE-701 82 Örebro, Sweden
[b] Information Systems, Linköpings Universitet, SE-581 83 Linköping, Sweden

ARTICLE INFO

Article history:
Available online 30 December 2016

Keywords:
Information security policy
Discourse analysis
Communicative analysis
Quality criteria
Policy design

ABSTRACT

To address the "insider" threat to information and information systems, an information security policy is frequently recommended as an organisational measure. However, having a policy in place does not necessarily guarantee information security. Employees' poor compliance with information security policies is a perennial problem for many organisations. It has been shown that approximately half of all security breaches caused by insiders are accidental, which means that one can question the usefulness of current information security policies. We therefore propose eight tentative quality criteria in order to support the formulation of information security policies that are practical from the employees' perspective. These criteria have been developed using practice-based discourse analysis on three information security policy documents from a health care organisation.

1. Introduction

Information and information systems have become critical assets in most organisations. Consequently, it is not surprising that information security management, where the purpose is to safeguard an organisation's information assets, has become an important strategic issue for most organisations (Van Niekerk and Von Solms, 2010). Information security policies are therefore important for regulating employee security behaviour. Their purpose is to safeguard information and prevent misuse of information systems (Baker and Wallace, 2007). However, most information security breaches are a consequence of employees who violate information security policies (Herath and Rao, 2009; Nash and Greenwood, 2008; Siponen et al., 2014; Stanton et al., 2005), and employees' poor compliance with information security policies has been stressed as a perennial problem for many organisations (Ernst & Young, 2008, 2010; PwC, 2014).

Nonetheless, it has been shown that about half of all breaches caused by insiders are accidental (ENISA, 2014; Vroom and von Solms, 2004). Furthermore, Adams and Sasse (1999) have shown that the design of information security policies themselves can impair employees' information security behaviour because they are cumbersome and incompatible with existing work practices. It means that employees are left to prioritise between information security and their work practice (Kirlappos et al., 2013). When employees prioritise their work practice and circumvent information security policies, it may over time lower employees' information security motivation (Adams and Sasse, 1999). Consequently, one can question the usefulness of today's information security policies in guiding employee behaviours (Doherty and Fulford, 2005).

Despite the importance of information security policies, the design of such artefacts is an understudied area of information security research (Baskerville and Siponen, 2002). Gaskell (2000), one of few scholars to have studied the information security policy design process, characterised the process as ad-hoc. During such a design process, information security managers mainly draw upon elicited information security

* Corresponding author.
E-mail address: fredrik.karlsson@oru.se (F. Karlsson).

http://dx.doi.org/10.1016/j.cose.2016.12.012
0167-4048/© 2016 Elsevier Ltd. All rights reserved.

requirements (Fabian et al., 2010) and international security standards (ISO, 2013). Standards are general guidelines; they do not address the particular context of an organisation (Baskerville, 1993), such as the specific needs of health care. Thus, such elicited requirements are an important complement.

If few studies have focused on information security policy design processes, even fewer have addressed information security policies as communicative objects or investigated what constitutes a useful information security policy from a communicative point of view. Stahl et al. (2012) is a notable and valuable exception. Through a discourse analysis of information security policies they provided six product-oriented recommendations for the design of information security policies. However, it should be noted that they focused on high-level policies (Baskerville and Siponen, 2002); in practice, employees are exposed to, and have to navigate, several documents that together constitute an information security policy.

Against this backdrop, we take an explicit starting point from a practice-based perspective. This means that: (a) we critically assess the role of the information security policy as a practical tool in employees' everyday work, including the use of both high-level and low-level policy documents, and (b) we acknowledge the fact that multiple practices exist in an organisation and that these need to interact. Thus, we view information security policy documents as the results of interaction (or lack thereof) between an information security practice and an operational practice. In this setting, information security policy documents are seen as communicative objects.

The purpose of this paper is to: (a) illustrate the usefulness of practice-based discourse analysis for understanding information security policy design, and (b) provide a set of tentative quality criteria for information security policy design in health care from a practice-based perspective. For this purpose, we carried out a case study at a Swedish emergency hospital. We employed a practice-based discourse analysis on the hospital's information security policy. It meant besides collecting and analysing information security policy texts, we also studied the operational practice through observations and interviews. The latter is important in order to be able to interpret the communicative limitations of a policy from the employees' perspective. Hence, this research responds to the call for more research on employees' behaviour with respect to information security policies within health care (De Lusignana et al., 2007), focusing on the communicative aspects of the information security policy artefact; an area that has received even less research attention. As far as we know there exist no product-oriented quality criteria for information security policy design anchored in a practice-based perspective in a health care setting. We assess the role of an information security policy as a practical tool in employees' everyday work, including both high-level and low-level policy documents. Thus, our study complements research published previously by Stahl et al. (2012).

The remainder of this paper is structured as follows. In the next section we discuss existing research on information security policy design. Following that, we present our research approach. The fourth section is devoted to our analysis and the quality criteria that are produced. The fifth section comprises a discussion of the research findings, their implications for practice and research, research limitations, and ideas for future research. Finally, the paper ends with a short conclusion.

2. Existing research on information security policy design

An information security policy is a "direction-giving document" (Höne and Eloff, 2002b) for defining acceptable behaviour for employees when using an organisation's information assets (Davis and Olson, 1985). Such a policy provides information security management with an important vehicle for establishing information security practices in an organisation (von Solms and von Solms, 2004). Consequently, an information security policy is an important component in the two processes of directing and controlling an organisation that are found in many information security management frameworks (e.g. von Solms et al., 2011). Given the strategic importance of information assets today, there is a strong belief that information security management should be integrated into corporate governance (Hinde, 2002; von Solms, 2001). In an organisation, the executive management operates at a strategic level, outlining a set of directives to indicate the importance of information assets; these are operationalised through the organisation's information security policy design.

While information security governance research fails to offer detailed guidance on how to design information security policies (e.g. von Solms and von Solms, 2006), there exists practitioner-oriented literature that does (e.g. Howard, 2007; Peltier, 2004; Smith, 2010; Wood, 2001). However, this literature focuses on the design process and product guidelines without reflecting on the end products' usefulness from an employee's perspective. Scholarly studies about information security policy design also exist. Although a great deal of consensus can be found with regard to the importance of information security policies (cf. Baskerville and Siponen, 2002; Herath and Rao, 2009; Höne and Eloff, 2002a), less attention has been given to empirical studies on how to design the content of these policies (Doherty et al., 2009; Hong et al., 2006). Doherty et al. (2009) stated that "there are very few studies that explicitly address how the scope or content of information security policies support the employee in their daily work".

From a process perspective, Sibley (1993) and Gaskell (2000) have described information security policy formulation as ad-hoc. At the same time as, Wood (1995), for example, has stressed the importance of a well-thought out design process. In response to these calls, suggestions for process frameworks have been developed to systematise the work with information security policy design. For example, Wood (1995) provided guidelines for the information security policy design process, arguing that different audiences often require tailored policies: "one must understand the special needs of an organization before one attempts to generate specific written management directives". In addition, Beautement et al. (2016) found that employee populations in an organisation are not homogeneous, which means that a policy may translate into different security behaviours. Baskerville and Siponen (2002) suggested a meta-policy for information security that includes design steps, and Rees et al. (2003) put forward the PFIRES framework. Furthermore, it is common in the information