Available online at www.sciencedirect.com

SciVerse ScienceDirect

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

Computers & Security

Organizational power and information security rule compliance

Ella Kolkowska [a,*], *Gurpreet Dhillon* [b,1]

[a] *Örebro University School of Business, Sweden*
[b] *Virginia Commonwealth University, USA*

ARTICLE INFO

Article history:
Received 9 March 2012
Received in revised form
26 June 2012
Accepted 1 July 2012

Keywords:
Dimensions of power
Information security
Security compliance
Security rule implementation
Non-compliance

ABSTRACT

This paper analyzes power relationships and the resulting failure in complying with information security rules. It argues that an inability to understand the intricate power relationships in the design and implementation of information security rules leads to a lack of compliance with the intended policy. The argument is conducted through an empirical, qualitative case study set in a Swedish Social Services organization. Our findings indicate that various dimensions of power and how these relate to information security rules ensure adequate compliance. This also helps to improve configuration of security rules through proactive information security management.

1. Introduction

Lack of compliance with security policies occurs because of a number of reasons. Foremost amongst them are the inability of the policy to reflect current practices (Mattia and Dhillon, 2003) and stakeholder resistance to security rules (Lapke and Dhillon, 2006). The organizational studies literature has intricately linked the concept of resistance to organizational power (Markus, 1983; McFarland, 2004). Following on from the arguments presented in the dominant literature, we make a call to better understand organizational power in the context of information security policy compliance. Information security policy consists of a number of rules for protecting information in an organization. Whenever security rules are implemented or modified, there is a resultant organizational change – business processes get re-engineered, reporting structures get modified, technical controls get redesigned. However as Hardy (1996) suggests, organizational power provides the energy to realize change. Thus, by developing a good understanding of organizational power dimensions, it will be possible to ensure better security rule compliance. Correspondingly we also argue that a better appreciation for organizational power will ensure correct configuration of security rules.

The objective of the paper is to apply Hardy's dimensions of power to understand compliant and non-compliant behavior. Our findings also suggest how managers can use such an understanding to improve compliance with security rules. Thus the topic dealt within this paper is useful for many security management related persons, especially those who are responsible for implementation of information security rules and processes in an organization.

Three classes of definitions ensue from our argument – organizational power, information security and compliance.

* *Corresponding author*. Tel.: +46 19 30 37 24; fax: +46 19 33 25 46.
E-mail addresses: ella.kolkowska@oru.se (E. Kolkowska), gdhillon@vcu.edu (G. Dhillon).
[1] Tel.: +1 804 828 3183; fax: +1 804 828 3199.
0167-4048/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2012.07.001

In this paper we refer to organizational power as "the probability within a social relationship of being able to secure one's own ends even against opposition" (Parson, 1968). We refer to information security as the protection of all information handling activities, may these be technical or non technical (Dhillon, 2007). And compliance refers to a "relationship in which an actor behaves in accordance with a directive supported by another actor's power, and to the orientation of the subordinated actor to the power applied" (Etzioni, 1975, p. 3).

2. Security rule compliance and organizational power

In a seminal paper, Ranson et al. (1980), while discussing specialization of tasks in organizations, have argued that over time the path of internal differentiation leads to a "process of perpetual fission that fragments the collective enterprise of adequate understanding". This means that over time, in any enterprise, as complexity sets in, organization power is bound to get manifested. Hence compliance with a certain "paradigm or problematics" (cf. Ranson et al., 1980) is an attempt to articulate the latent relationships amongst stakeholders.

In the context of our research, and in using Ranson et al. (1980) terminology, a security rule is a form of organizational structure, which has its own "devotees". With time security rules get transformed (i.e. structures evolve) as do the "devotees". The constant interplay between the evolving structures and those who believe in them results in *power*, which as Hardy (1996) notes, helps in "bringing about strategic action". In the literature this interplay has been termed as structures being "constituted and constitutive" (see Benson, 1977; Ranson et al., 1980).

Therefore in this section we explore the relationship between organizational power and security rule compliance. It is important to address this issue since dominant literature illustrates a rather consistent pattern of lack of compliance with security rules (Nash and Greenwood, 2008; PWC, 2008; Stanton et al., 2005; Whitman and Mattord, 2008). The notion of lack of compliance as a consequence of organizational power manifestations has been well documented in the literature. Lapke and Dhillon (2006) identified resistance to security policies as one of the major reasons for failure. Lapke and Dhillon (2008) also consider the importance of understanding organizational power in formulation and implementation of security policies. While aspects of compliance have been touched upon in the work of Lapke and Dhillon (2006, 2008), they do not explicitly focus on organizational power and it's utility (or limitation) in security rule compliance.

Beyond the literature on organizational power, compliance with security rules has been studied. The literature on security rule compliance falls into two broad categories. First are approaches that emphasize the use of sanctions. In this case the emphasis is on penalties and pressures that one party might apply on the other. Such power is usually coercive in nature (Kim and Lee, 1991). Coercive power and rewards have been extensively researched in the management literature. In the context of information security as well, a number of researchers have argued that coercion, sanctions and rewards have a significant impact on compliance or non-compliance (Herath and Rao, 2009; Kankanhalli et al., 2003). Such a conception has lead to using deterrence theory to suggest that individual expectations about external contingencies (e.g., rewards, punishments, etc.) direct compliant behaviors (Straub, 1990; Straub and Welke, 1998).

The second category of compliance research is behavioral in nature (Herath and Rao, 2009). Such studies are based on the belief that human nature is complicated and consequently compliant and non-compliant behaviors may not always be explained by fear of sanctions or desire for rewards. Studies within this category aim to increase understanding of the reasons behind compliance and non-compliance by closely studying of human behaviors (see Boss et al., 2009; Phanila et al., 2007; Siponen and Vance, 2010). The emphasis within such behavioral research (Herath and Rao, 2009) is on the modification of one kind of attribute (value congruence, legitimacy, etc) or another, to ensure compliance. A number of behavioral studies especially emphasize the importance of value correspondence and cultivation of a security culture. According to these studies compliance can be improved if employees internalize information security values in their daily work practices (Thomson, 2009). In this way "proper" security behavior will become a natural part of an employees' daily work activities (Knapp et al., 2007; Leach, 2003; Thomson et al., 2006; Vroom and von Solms, 2004). A similar approach is also suggested in 'awareness studies' (Puhakainen, 2006). These studies argue that increased security awareness of employees and educational programs leads to better compliance with information security rules (Furnell et al., 2002; Siponen, 2000).

There is no doubt that compliance with security rules can be achieved by any or all of the above identified approaches and clearly there may be more. However a limited number of current studies in the area emphasize the relationship between compliance behaviors and the sociological constructs such as power, which can be utilized to enforce these behaviors. In every organization there is a relation between those actors who have power in the organization and those who have less power (Lukes, 1974). Those actors who have power use different means in such a way that other actors find following the directive rewarding, while not following it incurs sanctions. Organizational power, as discussed above and its influence on users, has not been well explored in the compliance literature. Our study addresses this gap showing the value of applying the dimensions of power to understand compliant and non-compliant behaviors. This is because it allows for clarity on the nature and scope of existing domination and how it plays out in the context of a strategic change, particularly when a new security rule gets instituted.

Organizational power and its implications on various aspects of business have been well researched and there are a number of conceptions of power. In recent years the work of Cynthia Hardy has had a profound impact in organizational (see Hardy, 1996) and information systems research (see Dhillon, 2004). From Hardy's (1996) perspective, power is defined in neutral terms as a force that affects outcomes and allows beneficial results for all involved actors. She suggests a four dimensional framework that helps in understanding the consequences of organizational power from multiple perspectives.