ABSTRACT

Despite the significant resources organizations devote to information security policies, the policies rarely produce intended outcome. Prior research has sought to explain motivations for non-compliance and suggested approaches for motivating employees for compliance using theories largely derived from psychology. However, the socio-cognitive structures that shape employees’ perceptions of the policies and how they influence policy outcomes have received only modest attention. In this study, the authors draw on the socio-cognitive theory of frames and on literature on information security policies in order to suggest a theoretical and analytical concept of Information Security Policy Frames of Reference (ISPFOR). The concept is applied as a sensitizing device, in order to systematically analyze and interpret how the perceptions of policies are shaped by the frames and how they influence policy outcomes. The authors apply the sensitizing device in an interpretive case study conducted at a large multinational internet service provider. The authors’ findings suggest the frames shape the perceptions and can provide a socio-cognitive explanation for unanticipated policy outcomes. Implications for research and practice are discussed.

Keywords: Case Study, Compliance, Frames Of Reference, Information Security Policy, Institutional Shareholder Services (ISS) Policy, Interpretive Study, Policy Outcomes

INTRODUCTION

According to a recent industry survey, over 90% of large enterprises have implemented information security policies (hereafter InfoSec policies) (PricewaterhouseCoopers, 2010). Despite the recognized significance of InfoSec policies and the significant resources organizations have used to formulate and implement them, InfoSec policies rarely produce the intended outcome (Karyda, Kiountouzis & Kokolakis, 2005). Practitioners, however, are not the only ones...
who have devoted significant efforts to Infosec policies. Scholars sharing this concern, have sought to understand the underlying motivations and reasons for non-compliance (e.g., Herath & Rao, 2009; Bulgurcu, Cavusoglu & Benbasat, 2010; Siponen & Vance, 2010) and proposed approaches for motivating and enforcing employees to comply, drawing largely on theories from psychology and criminology (see Puhakainen and Siponen (2010) and Lebek, Uffen, Breitner, Neumann and Hohler (2013) for reviews). The past contributions suggest it is not only one actor or a single group of actors that influence the policy outcomes, but many different actors and groups of actors.

Any approach to information security management, to which InfoSec policies lay the foundation (Doherty, Anastasakis & Fulford, 2009), needs to converge the variety of interpretations organizational members have about the information security measures (Dunkerley & Tejay, 2010). Indeed, Hsu (2009) argues ‘having an appropriate understanding on how different groups perceive IS security can strengthen the design and institutionalization of security management practices’ (p. 149). Understanding how organizational groups perceive the Infosec policies is crucial in order to provide explanations for IS managers on experienced unanticipated policy outcomes and to develop approaches to transform the unanticipated outcomes into anticipated ones. Unfortunately, understanding the perceptions and how they influence the policy outcomes have remained largely absent from the prior literature. To fill some of the identified gap, we draw attention to the perceptions organizational members have formed around InfoSec policies by analyzing how socio-cognitive structures shape groups’ perception and explain adversities and unanticipated policy outcomes. The theory we utilize to make sense of the phenomenon is the socio-cognitive theory of frames of reference (hereafter frames) (Walsh, 1995) widely used in IS literature (e.g., Orlikowski & Gash, 1994; Khoo, 2001; Davidson, 2002; Hsu, 2009). Frames are organized knowledge structures that represent a specific information domain and shape how individuals perceive and understand different phenomena (Walsh, 1995). Although the frames become formed at individual level they can become shared at group, organization or even at industry levels (Walsh, 1995; Davidson, 2002). As organized knowledge, frames contain categories and content (Orlikowski & Gash, 1994). In order to analyze the frames that represent InfoSec policies, we suggest an analytical and theoretical concept of Information Security Policy Frames of Reference (ISPFOR). The ISPFOR represents and shapes how individuals perceive and make sense of InfoSec policies. Building on the concept of incongruence (Orlikowski & Gash, 1994), we argue ISPFOR incongruence is the extent of differences in the category content across frames held by individuals or groups of individuals. In other words, the more the category content differ across individuals or organizational groups, the more incongruent the frames are.

ISPFOR provides theoretical and analytical sensitizing device (Klein & Myers, 1999) to our empirical study. The concept of ISPFOR affords us to systematically organize and analyze the perceptions. The empirical study illustrates the use of ISPFOR to explain adversities and unexpected policy outcomes. We utilize interpretive case study (Walsham, 1995; Klein & Myers, 1999), and use semi-structured interviews to collect data and draw on hermeneutic interpretation (Klein & Myers, 1999) to interpret data. Our results suggest, the frames can largely explain the adversities and unexpected policy outcomes experienced at the case organization.

The paper is structured as follows. First, we introduce the informing theoretical elements of the study in order to develop a conceptual framework for this study by positioning frames to InfoSec policy research. Second, the chosen research method and its data collection and analysis strategy are explained. Third, we discuss the findings and the implication for researchers.
Related Content

A Method to Quantify Corpus Similarity and its Application to Quantifying the Degree of Literality in a Document
[www.igi-global.com/article/method-quantify-corpus-similarity-its/2878?camid=4v1a](www.igi-global.com/article/method-quantify-corpus-similarity-its/2878?camid=4v1a)

Gamification and Interdisciplinarity: Challenges in the Modern Knowledge Society
[www.igi-global.com/article/gamification-and-interdisciplinarity/185779?camid=4v1a](www.igi-global.com/article/gamification-and-interdisciplinarity/185779?camid=4v1a)
The Politics of Establishing ICT Governance for Large-Scale Healthcare Information Infrastructures
[www.igi-global.com/article/the-politics-of-establishing-ict-governance-for-large-scale-healthcare-information-infrastructures/186757?camid=4v1a](http://www.igi-global.com/article/the-politics-of-establishing-ict-governance-for-large-scale-healthcare-information-infrastructures/186757?camid=4v1a)

Driving Factors for Converting Teaching-Oriented Universities Into Entrepreneurial Universities: A Turkish Case Study
[www.igi-global.com/article/driving-factors-for-converting-teaching-oriented-universities-into-entrepreneurial-universities/209688?camid=4v1a](http://www.igi-global.com/article/driving-factors-for-converting-teaching-oriented-universities-into-entrepreneurial-universities/209688?camid=4v1a)