Available online at www.sciencedirect.com
ScienceDirect
Journal of Strategic Information Systems 16 (2007) 153–172
Strategic Information Systems
www.elsevier.com/locate/jsis

The role of external and internal influences on information systems security – a neo-institutional perspective ☆

Qing Hu [a,*], Paul Hart [a], Donna Cooke [b]

[a] *Department of Information Technology and Operations Management, College of Business, Florida Atlantic University, Florida, United States*
[b] *Department of Management, International Business and Entrepreneurship, College of Business, Florida Atlantic University, Florida, United States*

Available online 25 June 2007

Abstract

This research is an attempt to better understand how external and internal organizational influences shape organizational actions for improving information systems security. A case study of a multi-national company is presented and then analyzed from the perspective of neo-institutional theory. The analysis indicates that coercive, normative, and mimetic isomorphic processes were evident, although it was difficult to distinguish normative from mimetic influences. Two internal forces related to work practices were identified representing resistance to initiatives to improve security: the institutionalization of work mobility and the institutionalization of efficiency outcomes expected with the adoption of company initiatives, especially those involving information technology. The interweaving of top–down and bottom–up influences resulted in an effort to reinforce, and perhaps reinstitutionalize the systems component of information security. The success of this effort appeared to hinge on top management championing information system security initiatives and propagating an awareness of the importance of information security among employees at all levels of the company. The case shows that while regulatory forces, such as the Sarbanes-Oxley Act, are powerful drivers for change, other institutional influences play significant roles in shaping the synthesis of organizational change.

☆ An earlier version of this paper was presented at the 39th Hawaii International Conference of Systems Science on January 4–7, 2006 and published in the conference proceedings.

[*] Corresponding author.
E-mail addresses: qhu@fau.edu (Q. Hu), hart@fau.edu (P. Hart), cooke@fau.edu (D. Cooke).

0963-8687/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.jsis.2007.05.004

Keywords: Institutional theory; Neo-institutionalism; Information security; Sarbanes-Oxley Act; Institutional isomorphism

1. Introduction

The significant advances in networking technologies, epitomized by the explosive growth of the Internet, have exacerbated the complexity and vulnerability of networks used by individuals and organizations throughout the world. The high level of connectivity, the availability of sophisticated hacking tools, the enormous growth of electronic commerce, and other factors have created unprecedented opportunities for the dark side of the technological advancement to emerge and prosper. Attacks by computer viruses and spyware and security breaches in computer systems are almost daily occurrences. These attacks have resulted in financial losses amounting to at least hundreds of millions of dollars each year to U.S. companies and other organizations including government agencies (Gorden et al., 2004, 2005; Power, 2002; Richardson, 2003), and possibly in the trillions worldwide (Cavusoglu et al., 2004; Mercuri, 2003). The rampant spread of computer viruses from one organization to another and the denial-of-service attacks often launched from thousands of computers on unsuspecting organizations highlight the challenges faced by security managers and IT professionals today.

At the same time, the recent anecdotal evidence of data theft in recent months at the U.S. Energy Department (Stout, 2006) and Office of Veterans Affairs (Files, 2006) have highlighted the critical role of human and organizational factors for ensuring security. These factors have also been the focus of a number of studies on information systems security (Goodhue and Straub, 1991; Hu and Dinev, 2005; Straub and Welke, 1998; Von Solms and Von Solms, 2004; Vroom and von Solms, 2004). Noting the dominance of technical and functional issues in information security research, Dhillon and Backhouse (2001) call for the use of a socio-organizational perspective for understanding information systems security issues. Socio-organizational factors are important for ensuring information systems security because information systems comprise technologies that are designed, maintained, and used by human agents in organizations to facilitate collaboration, to support information sharing and work processes, and to conduct business transactions. While considerable resources have been devoted to developing increasingly sophisticated technologies to combat threats to information systems security, it is often the organizational factors, including employees, company policies, and organizational culture, rather than or in addition to technological weaknesses that create the most significant threats to the security of the organization. On the other hand, information systems security based on an understanding of organizational factors provide a significant defense against these threats.

The above discussion leads to the following research questions: (1) what are the external and internal institutional factors salient to information systems security, and (2) how do these institutional factors shape the cognition of managers and employees about information systems security and inform their actions? Given the limited literature on the socio-organizational perspective of information systems security, we attempt to explore these questions using a case study methodology. Instead of attempting to develop a comprehensive list of the influential factors, our focus is to understand those that are evident and how