Chapter 67
Composition of the Top Management Team and Information Security Breaches

Carol Hsu
National Taiwan University, Taiwan

Tawei Wang
University of Hawaii – Manoa, USA

ABSTRACT

Given the multifaceted problems and complexities of information security, the manner in which top management teams make investment and management decisions regarding security technologies, policy initiatives, and employee education could have a significant impact on the likelihood of information security breaches in organizations. In the context of information security management, it is not clear from management literature regarding how the characteristics of the top management team are associated with the possibility of information security breaches. The results demonstrate that the average length and heterogeneity of tenure could increase the possibility of breaches. However, age heterogeneity and the size of the top management team are negatively related to such a possibility. In addition, the findings suggest a nonlinear association between average age and tenure and the possibility of security breaches. The authors conclude the chapter with theoretical and practical implications on the organizational and managerial aspects of information security management.

INTRODUCTION

In recent years, the growing number of information security incidents (e.g., TJ Maxx, Sony, and Target), together with the pressure of regulatory compliance (e.g., the Sarbanes–Oxley Act, SOX) has focused managerial attention on the issue of effective information security management in organizations (Johnson & Goetz, 2007). The purpose of information security management is to develop and maintain a sound policy for the protection of an organization's information technology (IT) and non-IT information assets. To achieve this objective, managers need to implement an information security program whose scope encompasses physical, operational, and human resource management.

DOI: 10.4018/978-1-4666-8111-8.ch067

Numerous studies stressed the significance of top management support in the implementation of an information security program in an organization (Kankanhalli, Teo, & Wei, 2003; Straub & Nance, 1990) and highlighted how managerial perceptions and an understanding of information security issues influence the implementation process of information security programs (Hsu, 2009; Hu, Hart, & Cooke, 2007). In particular, the research on information security shows that an information security program requires top management to be involved in, and take responsibility for, defining the parameters of risk management to preserve organizational assets, and that such a process requires a degree of collective managerial effort.

With a focus on the composition of the top management team, we draw on the literature on organizational demography to investigate the characteristics of the organizational decision-making team in relation to the likelihood of information security breaches in organizations. The stream of organizational demography literature has shown that the heterogeneity (i.e., diversity) of the top management team can lead, directly or indirectly, to different organizational outcomes, such as financial performance (e.g., Kilduff, Angelmar, & Mehra, 2000), innovation levels (e.g., Bantel & Jackson, 1989), and competitive advantage (e.g., Hambrick, Cho, & Chen, 1996). We argue that the composition of the top management team is an issue that deserves the attention of information security researchers. For instance, one needs to know the extent to which the likelihood of information security breaches is associated with the diversity of top management skills, the manner in which the team's demography influences the organization's appetite for risk, and how such an appetite is reflected in attitudes toward security management. Our empirical research explores some of these issues. However, insightful and empirical analyses on the potential relation between the composition of the top management team and the likelihood of information security breaches in organizations are lacking. Building on the above arguments, we contend that the efficacy of decision making and information sharing among different senior managers could have an impact on the implementation and success of an organization's initiatives concerning information security management, which would in turn be reflected in the likelihood of information security breaches in such organizations.

To address our research question, we collect the sample from 1992 to 2008 based on S&P 1500 firms. Our results indicate that the average tenure, defined as the number of years the executives has served in the firm, and the heterogeneity of tenure are positively associated with the possibility of information security breaches. Differently, age heterogeneity and the size of the top management team are negatively related to such a possibility. In addition, our findings suggest a nonlinear association between average age and tenure and the possibility of security breaches. Our findings generally support the arguments regarding the influence of top management on information security breaches in prior literature (Hsu, 2009; Hu et al., 2007; Kankanhalli et al., 2003) and provide empirical evidence that the diversity of top management can influence the efficacy of information security management.

The remainder of the paper is organized as follows. In the next section, we review the literature on information security management with a focus on studies dealing with top management behavior. We then introduce our proposed hypotheses. Next, we present the research methodology and discuss the findings from our empirical analysis. In the last section, we conclude with the implications of the present study and suggest avenues for future research.

LITERATURE REVIEW AND STATEMENT OF HYPOTHESES

From the practical viewpoint, a number of practitioner-oriented reports have highlighted the

Related Content