İşletme Araştırmaları Dergisi
ISSN: 1309 - 0712

Journal Of
Business Research
Turk
www.isarder.org

The Relationship between Organizational Culture and the Perception of Information Security on the Axis of Cameron-Freeman Organizational Culture Types: An Application in Government Universities

Ertuğrul AKTAN
Banking Regulation and Supervision Agency,
İstanbul, Turkey
ertugrulaktan80@gmail.com

Belgin AYDINTAN
Gazi University
Faculty of Economics and Administrative,
Sciences, Department of Business,
Ankara, Turkey
belginaydintan@gmail.com

Extensive Summary

1. Introduction

As a result of attacks to computer systems and networks, encountering the loss of money, time, prestige and information is inevitable for the organizations. Therefore, dependency on computer systems in over all business processes raises the need to ensure the security of information held in electronic form. Implementing effective information security involves understanding security-related risk, then developing and implementing appropriate controls. In general the better employees are at applying the controls the more secure the organization will be, because even the best designed technical controls and procedures will be of limited value if the staff involved do not understand why they have been implemented and what they are accomplishing (Woodhouse, 2007, p. 767). Therefore, senior management must recognize that information security can no longer solely rely on technical and physical controls (Lim et al., 2009, p. 88). The role of the employees is vital to the success of any company, yet unfortunately they are also the weakest link when it comes to information security. In order to understand the enormous influence that the employee has on the business with regard to information security, the role that people play in securing information must first be examined (Vroom and Solms, 2004, p. 193).

If there's no management support and the culture change that embraces security and management's backing, all information security programs will fail even if technology is great. Without management's visible support, running an effective security program will be an uphill battle (Knapp and Ford, 2006, p. 34). In this respect, organizational culture has a strategic importance in achieving information security success. Because of the organizational culture has values and preconscious assumptions that affect the behavior of employees and organizational artifacts, the existence of relationship between organizational culture and the employees' perception of information security is discussed. In order to achieve the desired level of information

security, as investment in technological solutions, information security awareness of employees, organizational cohesions and understanding the purposes of information security are increasingly becoming an important case (Chang and Lin, 2007, p. 439).

Hence, in this research, defining the overall cultural profile of the government universities in Turkey on the axis of Cameron-Freeman organizational culture types, presenting the academicians' perception of information security based on the principles of information security and investigating the relationship between the organizational culture types and the academicians' perception of information security by correlation analysis were aimed.

Cameron-Freeman Organizational Culture Types: Cameron and Freeman (1991) developed an approach to representation of organizational culture, consisting of four dimensions that describe opposing or competing values of culture types. This framework is referred as the Competing Values Framework (CVF) and is illustrated in Figure 1. This framework includes four types of cultures, namely hierarchy, market, clan and adhocracy. The hierarchy concerns the internal maintenance with control and stability. The organizational culture compatible with hierarchy is characterized by a formalized and structured place to work. The market focuses on the outside positioning, control and stability and so defines a results-oriented workplace. The clan focuses on internal maintenance with a sense of flexibility. It is called a clan because of its similarity to a family-type organization. The fourth culture type, adhocracy is characterized by a dynamic, entrepreneurial, and creative workplace. The focus of adhocracy is on the external positioning with a high degree of flexibility and individuality (Cameron and Freeman, 1991, p. 30; Cameron and Quinn, 2006, pp. 38-45).

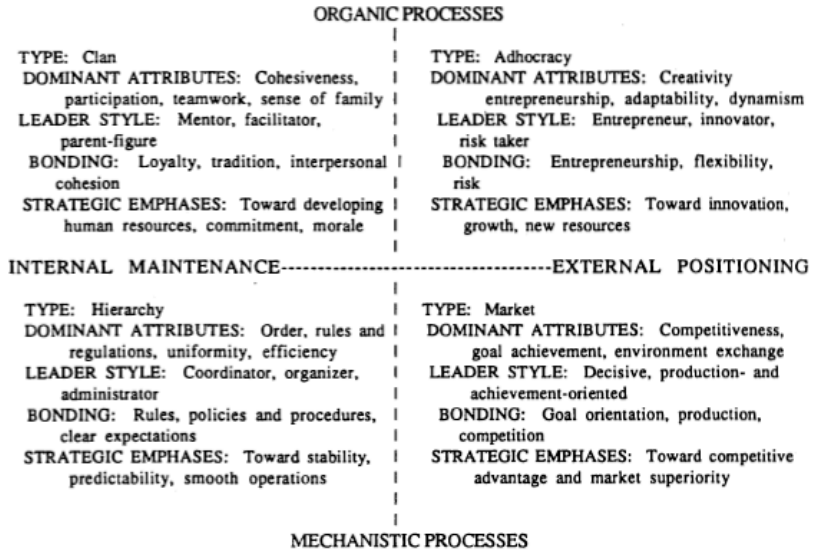

Figure 1. Cameron-Freeman Organizational Culture Types
Reference: Cameron and Freeman, 1991, p. 29

Information Security: Information security consists of three main attributes: 1) Availability that is the prevention of loss of, or loss of access to, data and resources. 2) Integrity that is the prevention of unauthorized modification of data and resources. 3) Confidentiality that is the prevention of unauthorized disclosure of data and resources (Harris, 2013, p. 298). Accountability was also mentioned as another important

principle of information security by previous researchs (Chang and Lin, 2007, p. 444; Harris, 2013, p. 298; Kanday, 2012, p. 302). Accountability is holding employees fully accountable for their conduct related to information security (Chang and Lin, 2007, p. 444). Accountability is tracked by recording user, system, and application activities, is done through auditing functions and mechanisms within an operating system or application (Harris, 2013, p. 248).

Research hypotheses are defined as follows;

H1: There is a meaningful relationship between organizational culture and the perception of information security.

H1a: There is a meaningful relationship between organizational culture and the perception of confidentiality principle of information security.

H1b: There is a meaningful relationship between organizational culture and the perception of integrity principle of information security.

H1c: There is a meaningful relationship between organizational culture and the perception of availability principle of information security.

H1d: There is a meaningful relationship between organizational culture and the perception of accountability principle of information security.

2. Method

The study was conducted on academicians working in the government universities in Turkey. The data was collected from 3,023 academicians of 106 government universities in Turkey via survey method between 19.01.2016 and 21.04.2016. For measuring organizational culture, the Organizational Culture Assessment Instrument (OCAI) developed by Cameron and Quinn (2006, pp. 26-28) was utilized. For the scale of the perception of information security, reliable questionnaire developed by Chang and Lin (2007, pp. 457-458) was used. The respondents were supposed to answer 24 questions for OCAI and 19 questions for the perception of information security questionnaire, both based on a five point Likert scale between strongly disagree and strongly agree. In data analysis phase, SPSS 21 package program was used.

3. Findings

Reliability statistics (Cronbach's Alpha) for the CVF culture types and the perception of the principles of information security were greater than 0.7 that suggested that measurement model exhibited adequate reliability. According to the findings of the research, in overall cultural profile of the government universities in Turkey it was concluded that hierarchy was dominant culture and the perception level of availability was greater than other principles' perception of information security. Moreover, in between the Cameron-Freeman organizational culture types (hierarchy, market, clan and adhocracy) and the academicians' perception of information security based on the principles of information security (confidentiality, integrity, availability and accountability), positive and statistically significant relationship was observed by the Pearson correlation coefficients (r) between 0.450 to 0.561 at significance level $p<0.01$. According to the result of Pearson Correlation Analysis, H1a, H1b, H1c, H1d and therefore H1 hypotheses were accepted.

4. Discussion

The hierarchy has been dominated in general cultural profile of the government universities in Turkey. The dominance of hierarchy cultures should be meaningfully addressed when universities in the research are thought to be government institutions dominating the formal processes of formal rules, policies, procedures, understandable definitions and tasks. In addition, it has been observed that market culture in universities take a significant place after the hierarchy culture. This can be explained in terms of result orientation with the strategy of achieving the advantages in the competitive environment in higher education. When common aspects of hierarchy and market cultures are evaluated together, the general cultural profile of the government universities can be defined with a sense of mechanical processes.

When the academicians' perception of information security is evaluated, the perception level of availability principle has been greater than other principles' perception of information security. This is a general indication of the academicians' perception that information systems in universities are open to access by students, staff, other researchers and trainers over the Internet and Intranets.

Preconscious assumptions that form the basis of organizational culture also shape the employees' perception of information security. In support of this, meaningful relationship has been found between the culture types possessed by government universities in Turkey and the academicians' perception of information security.

Findings in the current research are meaningful in terms of defining the general cultural profile of the government universities in Turkey, revealing the academicians' perception level of information security based on the principles of information security and determining the relationship between the organizational culture types and the academicians' perception of information security. It is envisaged that these findings will also be meaningful for other organizations except for the government universities. From this point of view, it is hoped that the employees' perception level of information security and the relationship between organizational culture and the perception of information security will contribute to the establishment of awareness of information security in the direction of long-term information security strategies.