December 2006

Influences on Espoused and Enacted Security Cultures in Organizations

Sriraman Ramachandran
The University of Texas at San Antonio.

Influences on Espoused and Enacted Security Cultures in Organizations

Sriraman Ramachandran
Doctoral Candidate
Department of Information Systems and Technology Management
The University of Texas at San Antonio.
sriraman.ramachandran@utsa.edu

ABSTRACT

Approaches to the management of Information Systems (IS) security in organizations have relied mostly on complex technical controls. In recent years, management of IS security by developing a security culture in organizations is emerging as an important stream in IS security research. The intent of this study is to contribute to the body of knowledge dealing with security culture. Security cultures include both security-related beliefs and security-related behaviors. The first premise of the study is that such beliefs and behaviors may not be consistent with each other. The study will examine the factors affecting both security-related beliefs and behaviors to explain differences between the two. The second premise of the study is that the security culture may vary across different groups within an organization. The study will examine factors, internal and external to the organization, which influence security cultures in different groups. A positivistic case-study based approach will be used.

Keywords

Security culture, Subcultures.

INTRODUCTION

Von Solms (2000) describes three waves in the progression of the management of Information Systems (IS) security: the technical wave, the management wave, and the institutionalization wave. The first wave focused primarily on technical aspects of IS Security. In the second wave, an equal emphasis was placed on technical and managerial aspects of IS security. The third wave, i.e., institutionalization wave, includes adoption of the best practices and codes of practice of IS security management from inside the organization, in short, on the cultivation of IS security culture as part of corporate culture (Von Solms 2000). Other scholars of IS security have also argued that organizations need a security culture over and beyond technological defenses to ensure a safe environment for information assets (Dhillon, 1995; Siponen, 2000). Security culture is defined as "the totality of human attributes such as behavior, attitudes, values that contributes to the protection of all kinds of information in a given organization" (Dhillon, 1995).

The most common approach to the study of security culture has been to view it as a part of organizational culture and describe it using the models of organizational culture. For example, Schleinger and Teufel (2003), and Zakaria and Gani (2003) adopted Schein's three level model of organizational culture (Schein 1985) and gave examples of IS security issues for each level of the model. Others like Chia et al (2002), and, Tejay and Dhillon (2005) have proposed dimensions based on models of organizational culture to characterize security culture in an organization.

There are two issues that literature dealing with security culture has not addressed adequately. The first issue is that security culture in an organization may be identified in several ways. For example, it may be identified by observing visible artifacts, such as management initiatives to enhance security awareness, implementation of security policies, security training and so on. Alternately, security culture may be identified by eliciting the beliefs of employees about security. Lastly, security culture may be identified by documenting and analyzing the security-related behaviors of employees. The cultures identified by each of these methods may be consistent with one another, or may contradict each other. It is argued in this study that the most important manifestation of culture is the security-related behaviors of the employees. The symbolic manifestations of culture, such as training programs and security policies, affect security in the organization by affecting the security-related beliefs and behaviors of employees. Hence, it is important not to rely only on initiatives such as security policies and training programs as a reflection of security culture, but to fully understand the security-related behaviors component of security culture.

Hawkins (1997) distinguishes between espoused culture and enacted culture. Espoused culture reflects the belief systems that are professed by a group; enacted culture is the culture reflected in the actual behavior of group members. We argue that in the domain of security, espoused and enacted cultures are likely to be different. In professing beliefs, members are likely to favor a secure stance, but actions in the real world may be guided by more than security considerations, e.g., most actions in organizations have to take into consideration performance pressures and productivity needs, which may lead to the compromising of security needs. Hence, one goal of our research is to understand the differences in the factors which influence espoused and enacted security cultures in organizations.

The second issue is that, in the current discussions of security culture, security culture in an organization appears to be treated as a monolithic construct. Organizational scholars have long accepted that culture within an organization is not monolithic. Subcultures usually form around existing divisions, departments, functional groups or professional groups (Trice, 1993a). Boisnier and Cheatam (2002) view organizational culture as a collage of subcultures under the overarching culture. Martin and Siehl (1983) suggest that subcultures may complement each other or conflict with each other. We argue that in the domain of security, security cultures of organizational members may differ between may differ between various professional groups in organizations. We believe that the differences in security subculture across professional groups are critical. The security subculture of each group has to be understood to identify weaknesses in organizational security. Hence, the second goal of our research is to understand the factors which affect the security subculture of diverse professional groups in an organization.

MODEL DEVELOPMENT

The model (see shown in Figure 1) is developed in three major segments.

Factors Influencing Enacted Security Subculture of Professional Groups

The first segment focuses on the factors affecting the enacted security subculture (security-related behaviors) of various professional groups within organizations. Enacted culture is conceptualized by Bath Consultancy Group as representing the lived culture that is externally noticed, and represents the culture that is reflected in actual actions (Hawkins, 1997). In the current study, enacted security subculture of professional groups within organizations is conceptualized to represent the actual, externally noticeable, security-related behavior of members of the group (Hawkins, 1997). The set of security-related behaviors discussed in the current study include those sets of actions on which employees within the organization have total control, can decide whether to perform or not, and has the potential to create security concerns. Enacted security subculture of professional groups within organizations is the dependent variable of the study.

We believe that enacted security subculture of various professional groups within organizations are influenced by two sets of factors: group level factors and managerial level factors. Group level factors represent the relevant belief structures of a professional group within the organization. Theoretical support for the influence of professional group's relevant belief structure on the group's security-related behavior (enacted security subculture) is drawn from Schein's (1985) three level model of organizational culture. According to Schein's three level model of organizational culture (1985), artifacts of culture, like behaviors (enacted security subculture) of members of the group, could be driven by the group's relevant beliefs (espoused security subculture). Espoused culture is conceptualized by Bath Consulting Group as the culture as represented through the stated beliefs and values, which the group claim to profess (Hawkins, 1997). In the current study, espoused security subculture of professional groups is conceptualized to represent the security-related beliefs professed by the group (Hawkins, 1997).

> *Proposition 1: Espoused security subculture of professional groups i.e. the group's security-related beliefs will influence the group's enacted security subculture i.e. the group's security-related behaviors.*

We also argue that the group's beliefs related to performance pressure will moderate the influence of the group's beliefs to security on the group's enacted security subculture. The theoretical basis for the moderating influence is drawn from research in the safety culture literature. Safety culture literature (Dawson et al., 1988; Embrey, 1992; Klen, 1988; Wright, 1986) argues that in addition to the direct influence from safety related beliefs of employees, safety performance of the employees will also be influenced by their beliefs related to performance pressure. When performance pressure is low, safety beliefs will be consistent with safety behavior; when performance pressure is high, safety beliefs and safety behaviors may vary. Analogously,

> *Proposition 2: Professional group's beliefs related to performance pressure will moderate the influence of the group's security-related beliefs (espoused security subculture) on the group's security-related behaviors (enacted security subculture).*

Managerial initiatives, such as security-related policies, guidelines, procedures, training programs, reward structures and penalty structures, are reflective of managerial emphasis on information security. Such emphasis is expected to influence security-related behaviors of employee groups. The theoretical basis for the influence of managerial security initiatives on enacted security culture of various professional groups within organizations is drawn from safety culture literature. Researchers in safety culture literature (Flin et al., 2000; Yule, 2003; Zohar, 1980), argue that managerial safety initiatives can influence employee's safety related behaviors by providing structures. Analogously,

> *Proposition 3: Managerial security initiatives will influence enacted security subculture of professional groups within organizations.*

Factors Influencing Espoused Security Subculture of Professional Groups

In the second segment, it is argued that espoused security subculture of professional groups within organizations (security-related beliefs) are influenced by two sets of factors: factors internal to the organization and factors external to the organization.

Internal factors include managerial initiatives, top management team's (TMT) beliefs and IS professional beliefs. Managerial security initiatives, such as training, awareness programs, policies, guidelines, procedures, reward and penalty structures are expected to influence the espoused security subculture of professional groups in organizations. Theoretical basis for such influence is drawn from IS literature. According to IS researchers like Leonard-Barton and Deschamps (1988), Purvis et al (2001), and Sharma and Yetton (2003), whose studies are focused on eliciting the influence of management initiatives on success of IS efforts within organizations, argue that management initiatives play a symbolic role in conveying the support of the management for such cause and could influence the employee's beliefs about the innovation in hand. Analogously,

> *Proposition 4: Espoused security subculture of professional groups will be influenced by managerial security initiatives.*

TMT beliefs can influence espoused security subculture either directly, or, indirectly through managerial security initiatives. TMTs are empowered to make decisions which will have repercussions throughout the organization, and, such decisions made by TMTs are tightly coupled to their beliefs and values (Hambrick et al., 1996). Upper echelon theory (Hambrick et al., 1996) argues that TMT beliefs and values will influence employee beliefs. Thus TMT beliefs about the relative importance of security and productivity will directly influence the security beliefs of the employee groups. Further, upper echelon also suggests TMT beliefs will affect organizational actions, i.e., managerial initiatives. Thus, TMT beliefs about the relative importance of productivity and security will affect managerial security initiatives. Thus,

> *Proposition 5: TMT's beliefs about the relative importance of security and productivity will influence the espoused security subculture of professional groups.*

> *Proposition 6: TMT's beliefs about the relative importance of security and productivity will influence the managerial security initiatives within the organization.*

The indirect effect of TMT beliefs on espoused security subculture results from the combinations of propositions 6 and 4.

The theoretical basis for the influence of security-related beliefs of IS professional group within organizations on the espoused security subculture of professional groups is drawn from the management literature, which argues that boundary spanning units (e.g., IS professional group within organizations) are units within organizations that have the potential to play a wide and greater role on different units within and outside organization, and thus can act as a source of social influence within organizations (Pfeffer and Salancik, 1978; Thompson, 1967). Hence, in the current study it has been argued that IS professional groups in organizations, who are cognitively associated with IS security issues within organization, will influence the security-related beliefs (espoused security subculture) of professional groups within organizations.

> *Proposition 7: Espoused security subculture of professional groups will be influenced by security-related beliefs of IS professional group in the organization.*

External factors which affect security-related beliefs include the group's professional association. Professional associations act as an important source of beliefs for members of professional groups within organizations. Hence, it is argued that professionally based beliefs about security will influence the espoused security culture of the group within organizations. Theoretical base for the argument is drawn from occupational culture literature (Trice, 1993b). Trice argues that the culture of a profession plays a significant role within organizations, as it transcends organizations and provides an anchor for the employee group's belief systems within organizations.

Proposition 8: Espoused security subculture of professional groups will be influenced by security-related beliefs derived from their profession.

Factors Influencing the Professional Group's Beliefs Related to Performance Pressure

The last segment argues that professional group's beliefs related to performance pressure will be influenced by TMT beliefs, directly, and, indirectly through managerial initiatives. Again, the upper echelon theory (Hambrick et al., 1996) suggests that TMT beliefs about relative importance of security and productivity will affect managerial initiatives to support productivity.

Proposition 9: TMT beliefs about the relative importance of security and productivity will influence the level of support for management initiatives to improve productivity within the organization.

TMT's beliefs about the relative importance of security and productivity, and managerial initiatives supporting productivity, will directly influence professional group's beliefs related to performance pressure. Theoretical base for such influences is drawn from safety culture literature. Safety culture literature (Dawson et al., 1988; Embrey, 1992; Wright, 1986) argues that the professional group's beliefs related to performance pressure will be influenced by management cues of performance expectations through their beliefs and actions related to productivity. Management initiatives play a symbolic role in conveying the support of the management for a cause (Purvis et al., 2001; Sharma and Yetton, 2003). Thus,

Proposition 10: Beliefs of professional groups related to performance pressure within organizations will be influenced by TMTs beliefs about the relative importance of security and productivity.

Proposition 11: Professional group's beliefs related to performance pressure will be influenced by management actions emphasizing productivity like productivity related policies, procedures, training programs and reward structures.

The integrated model is shown in Figure 1.

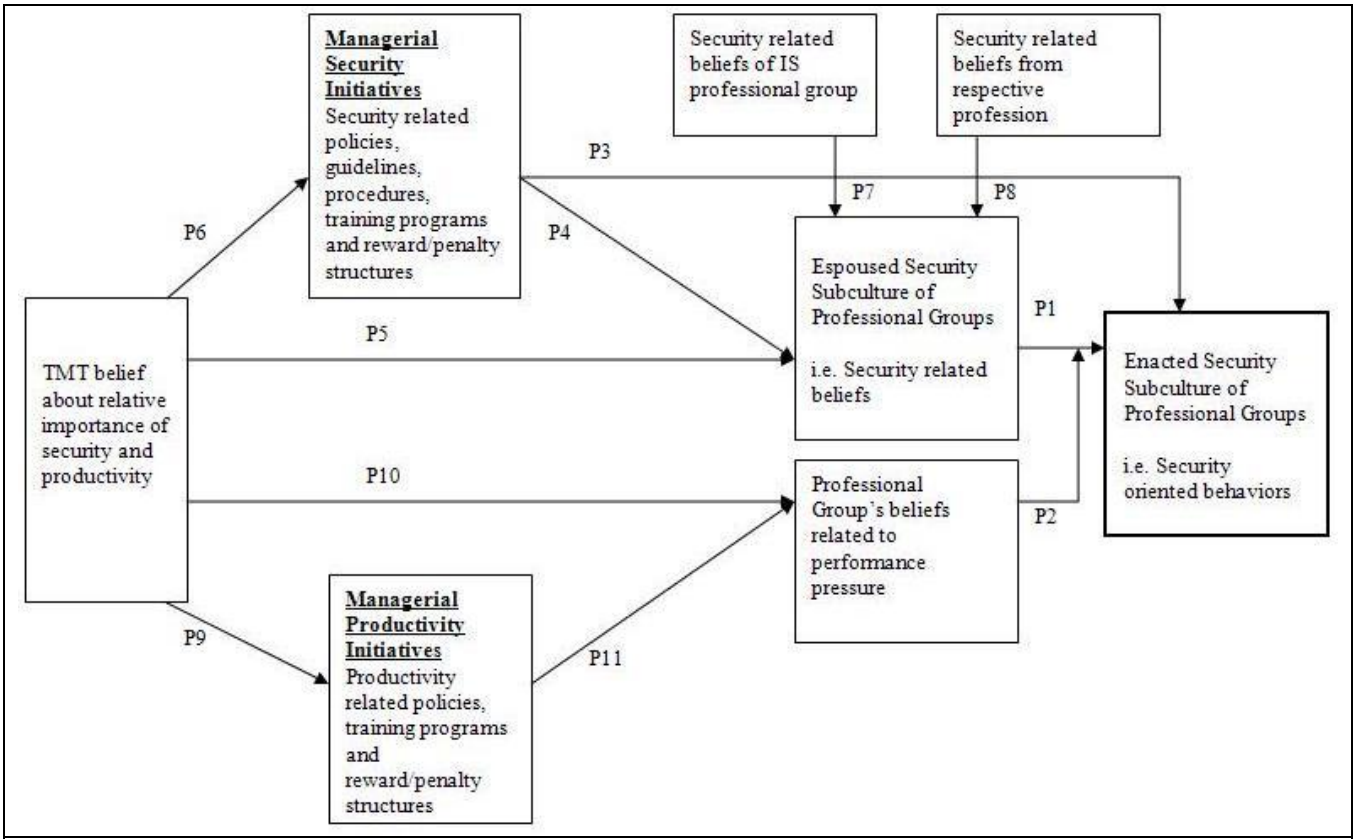

Figure 1. Security Cultures of Professional Groups in Organizations

PROPOSED METHODOLOGY

The model will be tested using a single site positivistic case study. Guidelines for the use of single site positivistic case study have been published by Benbasat et al (1987), and Lee (1989). As part of the pilot study, exploratory interviews of respondents from multiple organizations have been conducted. Presently, the interviews are being transcribed and analyzed. The exploration has two goals. First, we are seeking preliminary qualitative confirmation of the causal links included in the model. Second, we are refining the interview questions that will be used at the case site. The case study will include interviews of TMTs, members of IS department, and members of three other professions (e.g., accounting, marketing, and human resources). Our plans include examination of security policies, procedures and training programs. Following the interview, we will conduct a survey of larger number of respondents from each professional group within the organization. The multi-method approach is generally recommended in case studies to triangulate findings Yin (1994).

CONCLUSION

The current study builds on existing research on security culture by examining factors which may influence the espoused and enacted security cultures of professional groups within an organization. A theoretical framework is proposed, which will be assessed using a single site positivist case approach.

REFERENCES

1. Benbasat, I., Goldstein, D. K., and Mead, M. "The Case Research Strategy in Studies of Information Systems," *MIS Quarterly* (11) 1987, pp 369-386.
2. Boisnier, A., and Chatman, J. A. "Cultures and Subcultures in Dynamic Organizations," in: *The Dynamic Organization*, R. Peterson, and Mannix, E. (ed.), Lawrence Erlbaum Associates, Mahwah, NJ, 2002, pp. 87-114.
3. Chia, P.A., Maynard, S. B., and Ruighaver, A. B. "Understanding Organizational Security Culture," Pacific Asia Conference on Information Systems, 2002.
4. Dawson, S., Willman, P., Clinton, A., and Bamford M. *Safety at Work The Limits of Selfregulations* Cambridge University Press, Cambridge, England, 1988.
5. Dhillon, G. "Interpreting the Management of Information Systems Security," London School of Economics and Political Science, London, 1995.
6. Embrey, D.E. "Incorporating Management and Organisational Factors into Probabilistic Safety Assessment," *Reliability Engineering and System Safety*, (38) 1992, pp 199-208.
7. Flin, R., Mearns, K., O'Connor, P., and Bryden, R. "Measuring Safety Climate: Identifying the Common Features," *Safety Science* (34) 2000, pp 177-192.
8. Hambrick, D.C., Cho, T. S., and Chen, M. "The Influence of Top Management Team Heterogeneity on Firms' Competitive Moves," *Administrative Science Quarterly* (41) 1996, p 659–684.
9. Hawkins, P. "Organizational Culture: Sailing Between Evangelism and Complexity," *Human Relations* (50:4) 1997.
10. Klen, T. "Subjective and Objective Risk Estimate in Logging Work," International Conference on Ergonomics, Occupational Safety and Health and the Environment, Beijing, China, 1988.
11. Lee, A.S. "A Scientific Methodology for MIS Case Studies," *MIS Quarterly* (13) 1989, pp 33-50.
12. Leonard-Barton, D., and Deschamps, I. "Managerial Influence in the Implementation of New Technology," *Management Science* (34:10) 1988, pp 1252-1265.
13. Martin, J., and Siehl "Organizational Culture and Counterculture: An Uneasy Symbiosis," *Organizational Dynamics* (12:2) 1983, pp 52-65.
14. Pfeffer, J., and Salancik, G. R. *The External Control of Organizations: A Resource Dependence Perspective* Harper and Row, New York, 1978.
15. Purvis, R.L., Sambamurthy, V., and Zmud, R. W. "The Assimilation of Knowledge Platforms in Organizations: An Empirical Investigation," *Organization Science* (12:2) 2001, pp 117-135.
16. Schein, E.H. *Organizational Culture and Leadership* Jossey-Bass, San Francisco, 1985.

17. Schlienger, T., and Teufel, S. "Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture," 14th International Workshop on Database and Expert Systems Applications, 2003.
18. Sharma, R., and Yetton, P. "The Contingent Effects of Management Support and Task Interdependence on Successful Information Systems Implementation," *MIS Quarterly* (27:4) 2003, pp 533-555.
19. Siponen, M.T. "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management & Computer Security* (8:1) 2000, p 31.
20. Tejay, G., and Dhillon, G. "Developing Measures of Information Security," in: *The Fourth Workshop on e-Business (WeB 2005)*, Las Vegas, 2005.
21. Thompson, J.D. *Organizations in Action: Social Sciences Bases of Administrative Theory* McGraw Hill, New York, 1967.
22. Trice, H., and Beyer, J. M. *The Culture of Work Organizations.* Prentice-Hall, Englewood Cliffs, NJ, 1993a.
23. Trice, H.M. *Occupational Subcultures in the Workplace* ILR Press, Ithaca, NY, 1993b.
24. Von Solms, B. "Information Security - The Third Wave?" *Computers & Security* (19) 2000, pp 615-620.
25. Wright, C. "Routine Deaths: Fatal Accidents in the Oil Industry," *Sociological Review* (4) 1986, pp 265-289.
26. Yin, R.K. *Case Study Research, Design and Methods*, (2 ed.) Sage Publications, Beverly Hills, CA, 1994.
27. Yule, S. "Senior Management Influence on Safety Performance in the UK and US Energy Sectors," University of Aberdeen, Aberdeen, Scotland, 2003.
28. Zakaria, O., and Gani, A. "A Conceptual Checklist of Information Security Culture," 2nd European Conference on Information Warfare and Security, Reading, UK, 2003.
29. Zohar, D. "Safety Climate in Industrial Organizations: Theoretical and Applied Implications," *Journal of Applied Psychology* (65:1) 1980, pp 96-102.