Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2006 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2006

Security Cultures in Organizations: A Theoretical Model

Sriraman Ramachandran
The University of Texas at San Antonio

Srinivasan Rao
The University of Texas at San Antonio

Follow this and additional works at: http://aisel.aisnet.org/amcis2006

Recommended Citation
Ramachandran, Sriraman and Rao, Srinivasan, "Security Cultures in Organizations: A Theoretical Model" (2006). *AMCIS 2006 Proceedings*. 417.
http://aisel.aisnet.org/amcis2006/417

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2006 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Security Cultures in Organizations: A Theoretical Model

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

Srinivasan V. Rao
Department of Information Systems and Technology Management
The University of Texas at San Antonio
chino.rao@utsa.edu

ABSTRACT

Development of a security culture in an organization needs an understanding of the factors that influence the security-related beliefs and behaviors of organizational members. Security culture in an organization includes the culture of management and the culture of employees. The focus of the current study is on the security culture of employees. First, we argue that the security culture of employees of an organization is not monolithic, but comprises a collection of the security sub-cultures of the diverse professional groups in the organization. Thus understanding security culture of employees equates to understanding the factors that influence the security sub-cultures of professional groups in the organization. Next, we argue that security-related beliefs (espoused security culture) may be different from the security-related behaviors (enacted security culture). Hence, models of security culture should incorporate both constructs. With these goals in mind, we propose a preliminary theoretical model of the security sub-cultures of professional groups in organizations.

Keywords

Security culture, Sub-cultures.

INTRODUCTION

Scholars of information security have 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). As organizations consist of both managers and employees, security culture of an organization includes both the security culture of managers and the security culture of employees. The focus of the current study is on security culture of the employees. Researchers in organizational culture emphasize that organizational culture is not monolithic (Jermier et al., 1991); instead, it may vary over across groups, such as professional groups, in organizations. Analogously, it may be said that security culture as held among employees in organizations may vary across the diverse professional groups in the organization. One goal of our research is to understand the factors that affect the security sub-cultures of various professional groups.

Literature on culture also suggests that it may be necessary to distinguish between espoused culture and enacted culture (Hawkins, 1997). 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 not likely to favor a risky or insecure 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 efficiency and productivity needs, which may lead to the compromising of security needs. Hence, the second goal of our research is to understand the differences in the factors which influence espoused and enacted security sub-cultures of professional groups in organizations.

In this work-in-progress, we develop a preliminary theory-based model that relates antecedents of security sub-culture among professional groups in organizations, espoused security sub-culture, and, enacted security sub-culture. In section 2, we discuss key concepts in the literature. In section 3, we describe the proposed model, and provide rationale for the proposed

theoretical linkages. In section 4, we outline a proposed methodology to test such models. Last, we make some concluding remarks.

LITERATURE REVIEW

Security Culture

Von Solms (2000) describes three waves of Information Systems (IS) security: technical wave, management wave, and institutionalization wave, and argues that the field of IS security is currently riding the third wave. The technical wave focused on technological solutions, such as firewalls, access control, virus protection and so on, to the security problem.. The management wave was characterized by security policies, Chief Information Security Officers, organizational structures for IS security, and so on. The components of institutionalization wave include "information security standardization, international information security certification, cultivating an information security culture throughout a company, and implementing metrics to continually and dynamically measure information security aspects in a company" (Von Solms, 2000). Von Solms (2000) argues that cultivating security culture will ingrain security-related behaviors into the day to day activities of the employees. Others (e.g., Dhillon, 1995; Siponen, 2000) have also argued the importance of security culture.

The most common approach to the study of security culture has been to describe it using the models and frameworks of organizational culture. For example, Schleinger and Teufel (2003) adopt Schein's (Schein, 1985) three level (assumptions, beliefs and artifacts) model of organizational culture and give examples of security issues for each level of the model. At the assumption level, Schleinger and Teufel (2003) cite viewing employees as security assets as an example. At the belief level, they cite the belief that employees can have a positive effect on the organization's security. At the artifact level, they cite employee participation in security awareness course as an artifact. Others like Chia et al (2002) apply Detert's (2000) framework from management literature to identify eight topics of security which could help in defining security culture. Recently, Tejay and Dhillon (2005) developed seven constructs from the work of Dhillon (1995), which could be used to describe security culture of an organization..

There are two issues that literature has not addressed adequately. The first issue is that security culture in an organization may be identified in several ways. One, 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. Two, security culture may be identified by eliciting the beliefs of employees about security. Three, security culture may be identified by documenting and analyzing the security-related behaviors of employees. It is likely that the cultures identified are consistent with one another, but contradictions are also possible.

The second issue is that, in the current discussions of security culture, security culture in an organization appears to be treated as a monolithic culture. Organizational scholars have long accepted that culture within an organization is not monolithic. Boisnier and Chatman (2002) view organizational culture as consisting of subcultures under the overarching culture. Martin and Siehl (1983) suggest that the subcultures may be interlocked with each other, complementary, or conflicting. Sub-cultures usually form around existing divisions, departments, functional groups or professional groups (Trice, 1993). We believe that differences in security cultures across groups are critical. Thus, any aggregate measure of organizational security culture may be misleading. The security sub-culture of each group has to be understood to identify weaknesses in organizational security.

MODEL DEVELOPMENT

The model, as shown in Figure 1 is developed as follows. First, the dependent variable of interest is security-related behaviors of various professional groups within the organization. We argue that security-related behaviors of group members are influenced by security-related beliefs, and, the relative rewards for security-related behaviors and actual productivity. Second, the security-related beliefs of various professional groups in organizations are influenced in turn by the security beliefs of the professional culture, and, the organizational initiatives to enhance security awareness and security compliance. Last, both organizational initiatives for enhancing security awareness and security compliance, and, reward structures for security-related behaviors and productivity are in turn influenced by beliefs of the top management teams (TMT).

Top Management Teams

The influence of top management teams on security-related initiatives is based on arguments from "Upper Echelon Theory," which suggests that upper level managers influence organizational outcomes because they are empowered to take decisions which might have repercussions throughout the organization (Hambrick and Mason, 1984). Upper level managers make decisions consistent with their cognitive base, and, the "givens" they bring into to the decision (March and Simon, 1958), which are tightly coupled with their values and beliefs.

Thus, in our model, TMT beliefs will influence the steps taken to raise security awareness and security compliance of employees.

In strategic management literature, it has been shown that upper level manager's belief about value of change was found to influence organization strategy to be innovative (Hage and Dewar, 1972), and similarly the upper level manager's belief about sales and profit was found to explain the success of manufacturing firms in the same industry (Narayanan and Fahey, 1990). Parallel reasoning based on these studies would suggest that upper management beliefs about security will lead to successes in security efforts. However, it should be noted that the dependent variables in each of the studies cited (strategic decision process, innovation, success of manufacturing firms) is consistent with organizational productivity and efficiency, and consequently profitability. Security goals, in contrast, are often at odds with productivity goals in an organization. Thus, it is the upper management beliefs about security and productivity that are relevant to the success of the security efforts. In the theoretical model, upper management beliefs are shown to affect managerial initiatives to enhance organizational security, and, the reward systems for security-related behaviors and productivity

Belief Systems

Belief systems of various professional groups are influenced by factors internal and external to the organization. The internal factors are primarily the management initiatives, such as security policies, security standards and security training programs. Such initiatives are expected to cultivate favorable beliefs about the need for security, and enhance compliance (Chia et al., 2002; Tejay and Dhillon, 2005). External forces refer primarily to the influences of the profession that the employee belongs to. For instance, Tejay and Dhillon (2005) suggest that "synergy between IS security practice and codes influenced by the member's profession" as one of the several constructs for security culture. This suggests that beliefs about security among members of a profession will influence the belief systems of members in that profession within the organization.

Security-related behaviors

Belief systems influence behavior strongly when there is only one objective. For instance, if security is the only objective, belief systems about security will strongly influence security-related behavior. In instances when conflicting objectives are present, the influence of beliefs about one objective may not be sufficient to achieve the behaviors with respect to that objective and the behavior is based on trade-off between multiple objectives (Besnard and Arief, 2003). For instance, in most organizations, efficiency and profitability are important goals. In such instances, reward structures for the security and productivity goals will also play a role in addition to the security-related beliefs.

Summary of Model

The theoretical model proposed introduces two new issues which have not received much attention so far in literature. First, in the model, espoused and enacted security sub-cultures are included as separate constructs to enable the examination of other factors which may influence security-related behaviors. Second, we have argued that security culture in organizations is not monolithic, and may vary among different professional groups within the organization. This is incorporated by showing the influence of security-related beliefs of professions on the belief systems of employee groups within the organization.

PROPOSED METHODOLOGY

We propose to use 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). Currently, we are conducting exploratory interviews of respondents from multiple organizations. 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). Out plans include examination of security policies, procedures and training programs. We

do not intend to include questions about the sensitive issue of technical defenses. Following the interview, we will conduct a survey of larger number of respondents from the professional groups. The multi-method approach is generally recommended in case studies to triangulate findings (Yin, 1994).

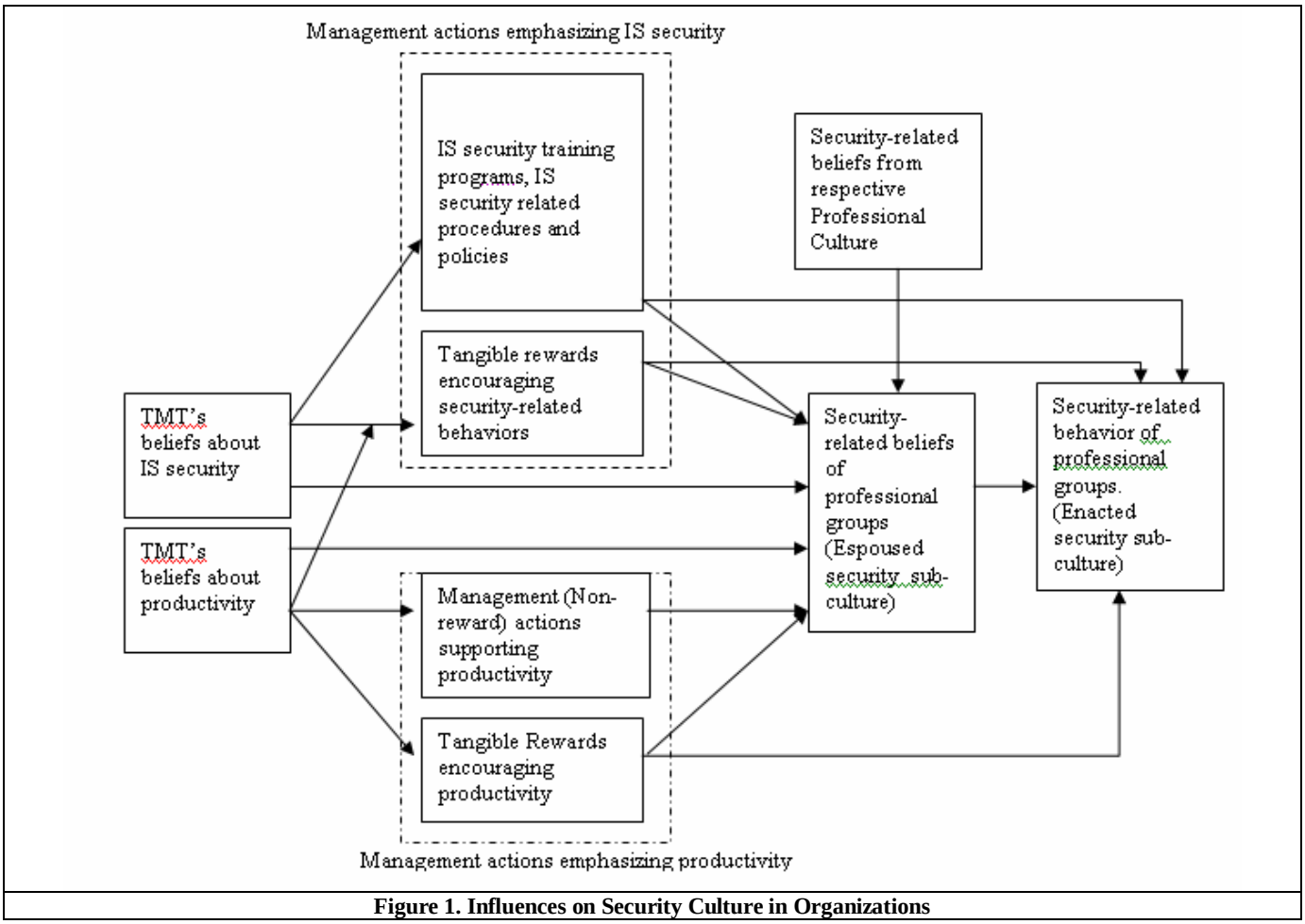

Figure 1. Influences on Security Culture in Organizations

CONCLUSION

Other researchers have argued the need for security culture in an organization to enhance security stance of the organization. We have extended this argument to include two key issues. First, we have argued that the security sub-cultures of various professional groups in the organization need to be considered. Second, we have argued that it may be necessary to consider both espoused security sub-culture and enacted security sub-culture.

REFERENCES

1. Benbasat, I., Goldstein, D. K., and Mead, M. (1987) The Case Research Strategy in Studies of Information Systems, *MIS Quarterly*, 11, 369-386.
2. Besnard, D., and Arief, B. (2003) Computer Security Impaired by Legal Users, *Journal of Computers and Security*.
3. Boisnier, A., and Chatman, J. A. (2002) Cultures and Subcultures, R. Peterson, and Mannix, and E. Mahwah (Eds.) *Dynamic Organizations: The Dynamic Organization*, NJ, Lawrence Erlbaum Associates, 87-114.
4. Chia, P. A., Maynard, S. B., and Ruighaver, A. B. (2002) Understanding Organizational Security Culture, *Pacific Asia Conference on Information Systems.*

5. Detert, J. R. (2000) A Framework for Linking Culture and Improvement Initiavtives in Organizations, *Academy of Management Review,* 25, 4, 850-863.

6. Dhillon, G. (1995) Interpreting the Management of Information Systems Security. London, London School of Economics and Political Science.

7. Hage, J., and Dewar, R. (1972) Elite Values Versus Organizational Structure Predicting Innovation, *Administrative Science Quarterly,* 17, 279-290.

8. Hambrick, R. C., and Mason, P. A. (1984) Upper Echelons: The Organization as a Reflection of Its Top Managers, *Academy of Management Review,* 9, 2, 193-206.

9. Hawkins, P. (1997) Organizational Culture: Sailing Between Evangelism and Complexity, *Human Relations,* 50, 4.

10. Jermier, J. M., Slocum, Jr., J. W., Fry, L. W., and Gaines, J. (1991) Organizational Subcultures in a Soft Bureaucracy: Resistance Behind the Myth and Facade of an Official Culture, *Organization Science,* 2, 2, 170-194.

11. Lee, A. S. (1989) A Scientific Methodology for MIS Case Studies, *MIS Quarterly,* 13, 33-50.

12. March, J. G., and Simon, H. A. (1958) Organizations, Wiley, New York.

13. Martin, J., and Siehl (1983) Organizational Culture and Counterculture: An Uneasy Symbiosis, *Organizational Dynamics,* 12, 2, 52-65.

14. Narayanan, V. K., and Fahey, L. (1990) Evolution of Revealed Causal Maps During Decline: A Case Study of Admiral,in A. S. Huff (Ed.) *Mapping Strategic Thought,* New York, NY, Wiley: 109-133.

15. Schein, E. H. (1985) Organizational Culture and Leadership, San Francisco, Jossey-Bass.

16. Schlienger, T., and Teufel, S. (2003) Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture, *14th International Workshop on Database and Expert Systems Applications*.

17. Siponen, M. T. (2000) A Conceptual Foundation for Organizational Information Security Awareness, *Information Management & Computer Security,* 8, 1, 31.

18. Tejay, G., and Dhillon, G. (2005) Developing Measures of Information Security, *The Fourth Workshop on e-Business (WeB 2005),* Las Vegas.

19. Trice, H., and Beyer, J. M. (1993) The Culture of Work Organizations, Prentice-Hall, Englewood Cliffs, NJ.

20. Von Solms, B. (2000) Information Security - The Third Wave?, *Computers & Security,* 19, 615-620.

21. Yin, R. K. (1994) Case Study Research, Design and Methods, Sage Publications, Beverly Hills, CA.