Exploring the Type of Relationship between Information Security Management and Organizational Culture

(Case Study in TAM Iran Khodro Co.)

Alireza Pour Ebrahimi
Faculty member of Islamic Azad University
E-Campus
drpourebrahimi@iauec.com

Payvand Fartash Naini
MA degree in IT Management, Islamic Azad University, Science and Research Branch-Tehran, Faculty of Management and Economics
payvandfn@yahoo.com

ABSTRACT

A culture conducive to information security practice is extremely important for organizations since information has to be critical assets in modern enterprises. Thus, for understanding and improving the organizational behavior with regard to information security, enterprises may look into organizational culture and examine how it affects the effectiveness of implementing ISM. This study aims to examine the relationship between Information Security Management and Organizational Culture. Based on a literature review, a model of the relationship between organizational culture and ISM was formulated, and both organizational culture characteristics and ISM effectiveness were measured empirically to investigate how various organizational culture traits have correlation with information security management by administrating questionnaires (based on five-point Likert scale) to respondents with significant use of information systems in TAM Iran Khodro CO. The collected data were given to SPSS for analysis, and the Pearson correlation coefficient was used to test the hypotheses. Results of testing the hypothesis indicate that the flexibility-oriented organizational culture traits, cooperative and innovative, have a significant relationship with information security management, whilst the stability-oriented organizational culture traits, consistent and goal-oriented, are not significantly associated with information security management. The research results can be used not only to identify key organizational culture traits related to ISM implementation, but also to derive guidelines and best practices for enterprise managers and decision makers to devise the correct tactics for achieving their goals of ISM practice.

Keywords

Information security, Information system, Information security management, Organizational culture

1. INTRODUCTION

Nowadays, in information era, providing information assets security has become one of the major challenges in organizations. Some researchers have likened the information to blood in the organization's vessels which is considered as a life-giving factor [10,27], and if the blood circulation is restricted or endangered, the organization will be faced with death [8]. On the other hand, the advent of new technologies continuously changes modern societies and information technology is the most effective one. Information technology has been raised as a powerful tool in the hand of business owners and has quickly transformed to do activities, interactions, etc. Therefore, the information and

its related technologies are considered as critical factors in organizations.

Since most information systems are inherently unsecure, every organization depending on the level of information (in terms of economic value), requires designing an information security management system to protect its information assets. Since creating an effective information security management system is considerably important, identifying factors affecting this system is essential. Information security management is mainly influenced by two factors including technical and non-technical factors. Technical factors include hardware and software which have been discussed in different references and articles. However, in non-technical factors, the factors affecting the information security management are awareness and information security knowledge, security policies, organization size, employee participation and training, budget, IT competence (of business managers), management support, organizational culture, environmental uncertainty and industry type. Thus, it is clear that technical solutions are only a part of a holistic method for information security, and as it was mentioned, various factors influence information security management.

Siponen and Oinas-Kukkonen study has shown that researches on non-technical aspects of information security are needed more than researches on its technical aspects [23]. Recent researches also suggest that in addition to technical factors, understanding the impact of human and organizational factors are the keys to the success of information security [4,5,22]. In many articles, information security has been mentioned as a socio-technical matter, since technical systems should be implemented and used by people. Therefore, given the fact that technology cannot address all information security risks alone and the role of human factors is undeniable [12], it seems that more attentions should be given to non-technical factors, especially human factors. Since the individuals' behavior in the organization is included in the form of organizational culture, examining how organizational culture, as one of the effective factors, affects the information security management is important to create an efficient information security management system.

This research is targeted to study the relationship between organizational culture and information security management. To achieve the research objectives, organizational culture has been considered with 4 components (cooperative, innovative, consistent and goal-orientated) as independent variables and information security management with 7 indices (confidentiality, integrity, availability, accountability, authenticity, non-repudiation and reliability) as dependent variables. The aim of this research is to provide a framework for information security management proportional to the dominant culture of the organization.

2. REVIEW OF RELATED LITERATURE

2.1 Information Security Management

Given that modern economics and businesses completely depend on IT to survive, the need to protect information has already increased [13]. In other words, since the organizations have been more and more dependent on information systems to conduct their daily businesses, this dependence has highlighted the need to manage the security of these systems [28]. According to [16] definition, information security is often known as protector of following cases:

- Confidentiality: Ensures that information is accessible only to authorized individuals or departments.
- Integrity: Ensures that data is changeable only by authorized individuals and methods.
- Availability: Ensure that information is available to authorized individuals when it is needed.

The three mentioned factors are called CIA which consists of confidentiality, integrity and availability. Moreover, information security also includes other factors such as accountability, authenticity, non-repudiation and reliability.

- Accountability: The concepts of accountability are responsibility, commitment and sense of responsibility of individuals towards the organization's information security.
- Authenticity: In information security, it is necessary to ensure that data, transactions, communications or documents are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.
- Non-repudiation: It implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.
- Reliability: Reliability means that whether each of the other factors of information security (confidentiality, integrity, availability, accountability, authenticity, and non-repudiation) is reliable in the organization's information security system and generally how reliable the information security system is.

Totally, seven factors mentioned are considered as the main factors of information security, and in this research, they have also been defined as indicators of information security management.

The concept of information security management refers to the activities which are along with controlling the security of information assets of an organization. The activities such as assessing threats and reviewing the current state of information security in organization, designing and implementing to control the administrative security (information security procedures for employees, etc), security technical controls (access control systems, etc) and using daily activities to maintain information security (documentation, events re-

sponse, employees training and etc). In fact, information security management deals with ensuring business continuity and minimizing damages and events which threaten information assets of an organization [15].Though it seems that content and field of information security are related to technology, in fact they are related to the areas of economics, sociology, technology, business and law and this matter increases its difficulty [24]. Interestingly, according to the survey conducted by CSO magazine, 7596 information security senior managers of 54 countries have claimed that security breaches are not related to technology and their organizations are not usually affected by such events and the main problem is non-technical issues. The fact is that information security is a management problem not technical. Experience has proven that technology cannot respond to the problems which are imposed by employees in the field of information security management. According to CSI/FBI research, although 89% of organizations have installed firewall and 60% of them have user ID, 40% of them still have not reported hacking the system by hackers [18]. This reveals an obvious weakness of management of these systems. In fact, information security management is a part of organization management structure and its approach is usually top-down. This means that its management is based on the business needs and aligns with organization objectives [26]. One of the important points in information security management is to consider it as a part of the business process and not as a separate supporting process. Therefore, the responsibility of its managing and administering should also be considered as the organization's everyday tasks [17].

2.2 Organizational Culture

1980s should be considered as the starting point of performing further researches on the issue of organizational culture. The interest for doing further researches on organizational culture is derived from a variety of factors including: First, 1980s is the decade of organizations and businesses globalization; therefore, the issue of coordination among employees was the day's issue. Second, in this decade, it became clear that different levels of the organization's performance can be related to the kind of organizational culture. Third, organizational culture can act as a source for creating stable competitive advantages, because some cultures cannot be imitated by competitors and the other reason is the advent of Japan's economic and industrial power as a significant competitor against US and according to the researchers, one of its main reasons is the cultural difference between two countries [9,19].

There is no consensus among different scientific views about the concept of culture; however, from organizational view, culture has been explained as a strong chain which provides the stability of the organization [14]. Organizational culture indicates common understanding of organizational members which influences their behavior. In every organization, there are beliefs, values, symbols, mottos and rituals which continuously change over time. These common values determine how employees understand their environment and respond to it [20]. As there are different definitions for organizational culture and every researcher has given a definition due to his/her mental attitude, there are also different classifications of organizational culture and every researcher has classified this issue with special and different criteria and has considered different aspects for his/her classification. Therefore, there are different models of organizational culture. For example, some scientists have insisted more on the environmental factors which influence on organizational culture while others have paid more attention to the organization's internal structure, reward internal systems and mechanisms. Some scientists have stressed on the organization's focus (inside-outside) and the amount of flexibility and stability. In fact, based on the two axes, four types of cultures are defined for the organization. The most popular and widely used models are Cameron and Quinn which include cultures of (clan, hierarchical, adhocracy, market) and the model of Denison which includes cultural traits (involvement, consistency, adaptability, mission). In this research in which organizational culture has been considered as an effective factor on determining the structure of information security in the organization, a model derived from Denison's model is defined that gives four kinds of culture (cooperative, innovative, consistent, and goal-oriented).

Figure 1. Organizational culture trait model

Descriptions of each part of this structure are as follows:

- Cooperative culture: Cooperative culture tends to internal focus and flexibility. These organizations stress on cooperation and involvement, information sharing, trust, empowerment and teamwork. In an organization in which such culture dominates, people are like an extended family.
- Innovative culture: Innovative culture tends to external focus and flexibility. These organizations stress on creativity, entrepreneurship, adaptability and dynamism. The company emphasizing innovativeness supports a fully creative and dynamic environment.

• Consistent culture: Consistent culture tends to internal focus and stability. These organizations stress on order, rules and regulations, uniformity and efficiency. The company emphasizing consistency is typically a formalized and regular organization.

• Goal-oriented culture: Goal-oriented culture tends to external focus and stability. These organizations focus on competition, achieving goals, production, effectiveness, and benefit-oriented measures. The company emphasizing goal-orientation is primarily a result-oriented and benefit-oriented organization.

Generally, to take any action in the organization, culture should be taken into consideration, because the culture can be leveraged to facilitate change and stabilize new orientations in the organization; even in some definitions, for expressing planned changes, the change of culture has been referred [1]. Therefore, culture identification helps managers to use the strengths of the organization with full awareness of the organization environment and predict necessary measures and actions for its weaknesses [21].

2.3 Organizational Culture and Information Security Management

Since all the fundamental values and behavior patterns of staff have been called organizational culture [3] and information security of the organization will be affected by these behavior patterns [4], in this research, organizational culture has been selected as one of the factors affecting information security management. Also, Deal and Kennedy have pointed out that culture is considered as the most important factor in explaining the success or failure of an organization [6]. As organizational culture will definitely affect the organization's performance and the effectiveness of information security activities, managers should pay special attention to the organizational culture as an important factor for advancing security goals.

Unfortunately, most of the organizations consider technical solutions fast and immediate response to their security problems. However, if the best hardware or software systems are used but users or human factors involved in an information system do not follow security parameters or are not aware of them, or in general, the organization's security solutions do not match its culture, a proper organization information security will not be expected. In other words, without a deep change in organization security culture which directly affects security practices, purchasing and employing security products and equipments will provide little safety [27]. Thus, the role of human factors in information security is unavoidable. As it has been reported, 80% of security problems have been as a result of staff's poor security behavior, so that in the incidence of these problems, the staff's negligence is much important than technical issues. Therefore, it is important to train and manage the problem-prone people.

3. RESEARCH METHODOLOGY

This research is counted as an applied research, and its method of data collection is descriptive. It has been carried out in a survey in TAM Iran Khodro Co. To collect data from this organization, all managers and experts in software, hardware and network departments have been targeted. Among 30 respondents, 10 were between 25 to 30 years old, 12 between 30 to 35 years old, and 5 between 35 to 40 years old and 3 did not answer this question. 6 employees had associate degree, 18 had bachelor degree, 4 had master degree, and 2 did not answer this question. 4 employees had less than 5 years of work experience, 10 had between 5 to 10 years, 8 had between 10 to 15 years, 2 had between 15 to 20 years, and 6 did not answer this question. These people's opinion was collected through a questionnaire that was designed based on five-point Likert scale. The questionnaires which consisted of 65 questions were presented in two separate parts related to organizational culture and information security management that 30 questions of which were about organizational culture and 35 questions were about information security management. Organizational culture was evaluated in these questionnaires with the components of cooperative, innovative, consistent and goal-oriented cultures, and information security management with the components of confidentiality, integrity, availability, accountability, authenticity, non-repudiation and reliability. The questionnaire of this research had face and content validity and its reliability was checked using Cronbach's alpha coefficient which had acceptable reliability for using in a research.

Finally, for analyzing the collected data, descriptive and inferential statistics techniques were employed. To describe data (the demographic and main variables of the research), frequencies, percentages, and graphs were used. Also, in inferential statistics, Pearson's correlation coefficient was used to test the hypotheses and determine the strength and type of relationships between variables. Subsequently, multiple regressions were used to examine the casual relationships between variables.

4. EMPIRICAL FINDINGS

The following graphs show the results of descriptive statistics which present the quality of information security of the organization.

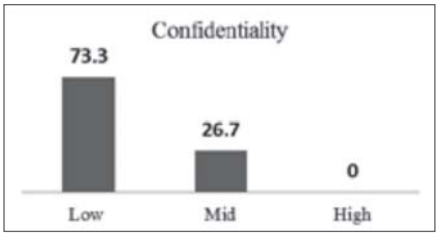

Figure 2. The description of Confidentiality

Figure 3. The description of Integrity

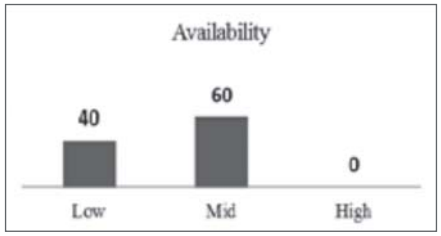

Figure 4. The description of Availability

Figure 5. The description of Accountability

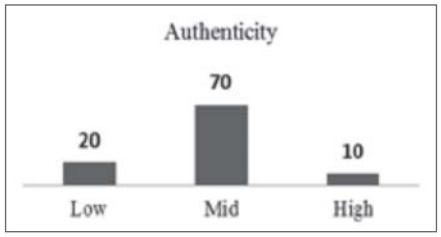

Figure 6. The description of Authenticity

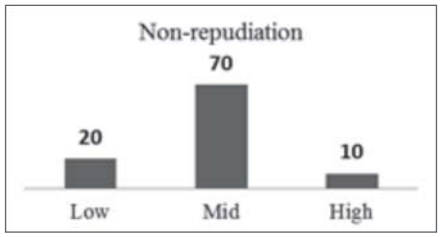

Figure 7. The description of Non-repudiation

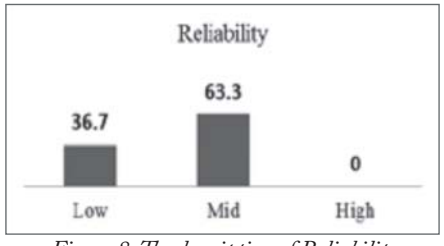

Figure 8. The description of Reliability

According to the graphs, all information security indicators of the organization are in average level; apart from two indicators, confidentiality and integrity, which are in low level.

Figure 9. The description of Information Security

In general, information security of the organization has been estimated %33.4 low, %63.3 medium and %3.3 high.

The results of inferential statistics are as follows:

First hypothesis: There is a significant relationship between "cooperative culture" and "information security".

The obtained results of hypothesis testing indicate that Pearson's correlation coefficient of this relationship equals to 0.49 (R= 0.49) and due to the obtained significance (P=0.023) which is less than 0.05; it can be concluded with 95% of confidence that there is a positive correlation between cooperative culture and information security. Therefore, considering the statistical findings, the first hypothesis is substantiated, and it means that in the population under study, cooperative organizational culture has a positive impact on information security.

Second hypothesis: There is a significant relationship between "innovative culture" and "information security".

The obtained results of hypothesis testing indicate that Pearson's correlation coefficient of this relationship equals to 0.44 (R= 0.44) and due to the obtained significance (P=0.046) which is less than 0.05; it can be concluded with 95% of confidence that there is a positive correlation between innovative culture and information security. Therefore, considering the statistical findings, the second hypothesis is substantiated, and it means that in the population under study, innovative organizational culture has a positive impact on information security.

Third hypothesis: There is a significant relationship between "consistent culture" and "information security".

The obtained results of examining the relationship between the two variables of consistent culture and information security shows that although there is a weak positive correlation between these two variables (R=0.156), the obtained significance level (P=0.498) indicates that the relationship between two variables is not statistically significant. Therefore, according to the findings of this study, there is not a significant relationship between consistent culture and information security. As a result, the third hypothesis is not substantiated.

Fourth hypothesis: There is a significant relationship between "goal-oriented culture" and "information security".

The obtained results of examining the relationship between the two variables of goal-oriented culture and information security shows that although there is a weak positive corre-

lation between these two variables (R=0.208), the obtained significance level indicates that the relationship between two variables is not statistically significant. Therefore, according to the findings of this study, there is not a significant relationship between goal-oriented culture and information security. As a result, the fourth hypothesis is not substantiated.

Also, in order to examine the impact of every independent variable on dependent ones, multiple regressions were used.

Table 1: Summary of Regression Model

Model	Correlation Coefficient (R)	Coefficient of Determination (R*)	Adjusted Coefficient of Determination	Standards Error of Estimate
1	0.519	0.270	0.262	12.67046

The results of regression analysis indicate that there is a positive correlation between the four independent variables: cooperative culture, innovative culture, consistent culture, and goal-oriented culture and independent variable: information security. The correlation equals to 0.519 which has a relatively strong intensity. Adjusted coefficient of determination which is 0.262 indicates that mentioned independent variables in the regression model can totally explain about 26% of the variances of the dependent variable. Table 2 shows the exact extent of standardized impact of every independent variable on dependent ones. As it is seen in this table, three variables (cooperative culture, innovative culture, and goal-oriented culture) of the four independent variables of the research have positive impact on the variable of "information security". Also, the results show that in terms of intensity, the variable of "innovative culture" has the highest beta coefficient (0.383), and the variable of "goal-oriented culture" has the lowest beta coefficient (0.180). Also, the variable of "cooperative culture" with beta coefficient of 0.280 has the second place in terms of intensity (table 2).

Table 2- Regression analysis

Dependent variable	Independent variables	Standardized coefficient (β)	t-value	Significance level
Information Security Management	Cooperative culture	0.280	2.734	0.024
	Innovative culture	0.383	3.675	0.007
	Consistent culture	0.012	1.001	0.999
	Goal-oriented culture	0.180	2.415	0.045

5. DISCUSSIONS AND IMPLICATIONS

It is derived from our study result that the flexibility-oriented organizational culture traits, cooperative and innovative, have a significant relationship and positive correlation with information security management, whilst the stability-oriented organizational culture traits, consistent and goal-oriented, are not significantly associated with information security management. Therefore, if the organizational culture of a company is stability oriented, it is unfavorable for the development of ISM in that company. Managers of such organizations need to understand the ISM disadvantage resulting from their stability oriented culture, and carefully lead their organizations with suitable counter measures, such as the proactively and carefully designed instructions and directions.

Although at first glance the results were unexpected, since it was expected that in an organization which has a formal structure and rules and instructions are strongly dominant, information security is maintained more and better; while, the people who know the dominant culture of their organization as such, believe that their organization do not have high security. However with a little reflection, its reasons can be explained as follows. In organizations with cooperative and innovative culture which give people authority, power of decision making and targeting so that the person feels that he has an important and key role in the organization, Intensifies his sense of responsibility. Generally, when he is treated like an adult, his reaction is also like an adult and he will be diligent and responsible in protecting the information of the organization. But, in contrast, when strict and formal rules govern the organization's atmosphere and human demands and individual capabilities are ignored, individuals' sense of belonging and empathy for organization decreases and some people cross-react, and willingness to disobey the rules and violate them will increase.

The culture of an organization can be built or changed by important factors of culture, such as norms, beliefs, values, and expectations. For the purpose of information security, organization leaders can make appropriate choices and adopt various approaches to shape the culture of their organizations, and eventually foster an environment conducive to the success of information security initiatives. A culture of information security is extremely important for organizations since the human dimension of information security cannot totally be solved by technical and management measures.

6. CONCLUSION

Information security is a major concern in electronic commerce and knowledge economy, a higher level of perceived security leads to higher customer satisfaction and trust [7,11], and a higher level of customer satisfaction can eventually create more transaction opportunities and benefit the

businesses [25]. The enterprises invest more and more in information security system, due to the fact that virus and hacker attacks have become the vogue in recent years. However, this upsurge has been slowing down in 2005, partly because the cost of information security system is very high and it is difficult for enterprises to keep up with the huge increasing expense needed. While the information security systems are still fundamentally important, it has become more and more important for enterprises to pay attention to the management of information security, which has the ultimate goal of designing and implementing information security strategies in an efficient and effective way.

Since all technical security products need to be operated and managed by people, a technical security solution alone cannot protect an organization without a good security management policy and practice. A good practice of information security strategies between intra-organization and inter-organization partners can be supported and facilitated by information security systems and technologies, but it is not assured by them. Information security technology is necessary but not sufficient for successful ISM, whether at the intra-organizational level or across inter-organizational partners. Therefore, enterprises should adopt an integrated strategy combining both information security and organization culture aspects, and focusing not only on the "outside" artifacts and behavior patterns which are visible and audible, but on the "inside" human nature, activity, and relationships which are hidden and mostly unconscious. The efficiency and effectiveness of the "outside" aspect of information security requires the "inside" aspect of an organization culture which is embedded in the values and beliefs of information security shared by all units at all levels in an organization.

Since organizational culture is affected by organizational behavior at each level of an organization, for understanding and improving the organization behavior with regard to information security, enterprises may look into organizational culture and examine how it affects the effectiveness of implementing ISM. Overall, an appropriate and effective ISM implementation requires a combination of favorable organizational culture, competent information security technology, and the management's supportive attitude toward information security. This research contributes to a better understanding of the relationship between various organizational culture attributes and the effectiveness of implementing information security management. In fact, a better understanding of such relationships can provide a better picture of how to help information security initiatives succeed.

Since this research is one of the first known researches for examining the relationship between organizational culture and information security management, exploring the influence of other culture factors, such as different culture attributes or different culture types, upon the effectiveness of ISM may help understand the relationship between organizational culture and ISM better. Furthermore, since this empirical study analyzed data collected from TAM Iran Khodro Co., it would be interesting and valuable to conduct similar surveys in other industries and different organizations with increased sample size for comparative studies.

REFERENCES

[1] Alvani, S. M. 2005. General Management. Tehran, Ney.

[2] Berti, J., and Rogers, M. 2004. Social Engineering: The Forgotten Risk. Information security management handbook – fifth edition. Boca Raton : Auerbach Publications.

[3] Beveridge CAR. Behaviour in organisations. [online] [cited 23 January 2003]. Available from: <http://www.carb.fsnet.co.uk/bio97.pdf >; December, 1997.

[4] Beznosov, K., and Beznosova, O. 2007. On the Imbalance of the Security Problem Space and Its Expected Consequences. Information Management & Computer Security, 15(5): 420-31.

[5] Botta, D., Werlinger, R., Gagne, A., Beznosov, K., Iverson, L., Fels, S. and Fisher, B. 2007. Towards understanding IT security professionals and their tools, Proceedings of the Symposium on Usable Privacy and Security (SOUPS), ACM, Pittsburgh, PA, pp.100-11.

[6] Deal, T., and Kennedy, A. 1982. Corporate Culture: The Rites and Rituals of Corporate Life, Addison - Wesley, New York, NY.

[7] Flavia´n, C. and Guinalı´u, M. 2006. Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. Industrial Management & Data Systems, 106(5): 601-20.

[8] Fulford, H, and Doherty NF. 2003. The Application of Information Security Policies in Large UK-Based Organizations: An Exploratory Investigation. Information Management & Computer Security, 11(3): 106–114.

[9] Goffee, R. and Jones, G. 2001. Organizational Culture: a sociological perspective, Handbook of organizational culture and climate , John Wiley, First Edition.

[10] Halliday, S., K. Badenhorst, et al. 1996. A business approach to effective information technology risk analysis and management. Information Management & Computer Security, 4(1): 19-31.

[11] Huang, J.H., Yang, C., Jin, B.H. and Chiu, H. 2004. Measuring Satisfaction with Business-to-Employee Systems. Computer in Human Behavior, 20(1): 17-35.

[12] IT Governance Institute 2008. Information security governance: Guidance for information security managers. ITGI Publishing.

[13] Knapp, K.J., Marshall, T.E., Rainer, R.K. and Ford,

F.N. 2006. Information Security: Management's Effect on Culture and Policy. Information Management & Computer Security, 14(1): 24-36.

[14] Korte, R. and Chermack, T. 2007. Changing organizational culture with scenario planning. Journal of Futures, 39: 645- 56.

[15] Mitchell, R.C., Marcella, R., and Baxter, G. 1999. Corporate Information Security Management. New Library World, 100(1150): 213-227.

[16] Pfleeger, C.P. 1997. Security in Computing. Prentice Hall, New Jersey. 2nd Edition.

[17] Posthumus, S., von Solms, R. 2004. A Framework for the Governance of Information Security. Computers & Security, 23(8).

[18] Power, R. 2002. 2002 CSI/FBI Computer Crime and Security Survey. Computer Security Institute. Available from: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2002.pdf (accessed on July 25, 2006).

[19] Quinn, R., and Cameron, K. 2006. Diagnosing and Changing Organizational Culture, The Jossey-Bass publishing, Revised Edition.

[20] Robbins, S.P. 2005. Management, eighth edition, entice Hall of India.

[21] Rahimnia, F., and Alizadeh, M. 2009. Exploring Dimensions of Organizational Culture Based on Denison Model. Ferdowsi University of Mashhad, 10(1).

[22] Rayford, B., Vaughn, R.H., JrandFox, K. 2001. An empirical study of industrial security engineering practices. The Journal of Systems and Software, 61: 225-32.

[23] Siponen, M.T. and Oinas-Kukkonen, H. 2007. A review of information security issues and respective research contributions. The Database for Advances in Information Systems, 38(1): 60-81.

[24] Stewart, J.N., Establishing an organization's security culture – partII. Retrieved online on 30 August 2006 from, http://www.cisco.com/web/about/security/intelligence/05_08_security-culture_II.html; 2006.

[25] Sudaporn, S., and Ogenyi, O. 2004. The Store Loyalty of the UK's Retail Consumers. The Journal of American Academy of Business, Cambridge, 5(1/2): 503-509.

[26] Vermeulen, C., and von Solms, R. 2002. The Information Security Management Toolbox–Taking; The Pain out of Security Management. Information Management & Computer Security, 10(2/3): 119-125.

[27] von Solms, B., and von Solms, R. 2004. The 10 Deadly Sins of Information Security Management. Computers & Security, 23(5): 371-406.

[28] Zuccato, A. 2007. Holistic Security Management Framework Applied in Electronic Commerce. Computers and security, 26: 256-265.