Information Security: Corporate Culture and Organizational Commitment

Ioannis Koskosas
Department of Informatics and Telecommunications Engineering
University of Western Macedonia
Konstantinos Kakoulidis
Technological Educational Institute of Western Macedonia
Department of Finance, Department of Accounting and Business Administration
Christos Siomos
SY.F.FA.S.DY.M (Pharmaceuticals of Western Macedonia)
KOZANI, 50100, Greece
E-mail: ikoskosas@uowm.gr

Abstract
Information is the most valuable asset in the so-called 'information society'. The main purpose of information security is to protect information and specifically, the integrity, confidentiality, authenticity and availability of data through an organization's network and telecommunication channels. Although information security is critical for organizations to survive, a number of studies continue to report incidents of critical information loss. To this end, there is still an increasing interest to study information security from a non-technical perspective. In doing so, this research focuses on the effect of strong corporate cultures and organizational commitment as important aspects for enhancing information security. That is, manipulating more effectively information security among end-users. Achieving the required level of information security within organizations usually requires more than security awareness and control but also a better understanding of the organizations' culture in which security measures are tailored, too. In effect, organizations have a clearer insight into how to commit more effectively to such security measures.

Keywords: Information Security Culture, Organizational Commitment, Information Technology.

1. Introduction

The reliance by every organization upon information technology has increased dramatically, as technology has developed and evolved. Over recent years, information has developed into a strategic asset, while the computerized information systems have become ultimate strategic tools for both government and organizations [24,33]. Due to globalization and competitive economic environments, efficient information management is critical to business survival and effective decision making activities. As the society and its economic patterns have evolved from the heavy-industrial era to that of information, in terms of providing new products and services to satisfy people's needs, organizational strategies have changed too. In effect, corporations have altered their organizational and managerial structures as well as work patterns in order to leverage technology to its greatest advantage. Economic and technology phenomena such as downsizing, outsourcing, distributed architecture, client/server and e-banking, all include the goal of making organizations leaner and more efficient. However, information systems are deeply exposed to security threats as organizations push their technological resources to the limit in order to meet organizational needs [6,7].

While security attacks are either internal or external, 66% of computer attacks in Greece come from employees within organizations [37]. To this end, the success of information security appears to depend, in part, upon the effective behavior and understanding of the individuals involved in its use. Constructive behavior by end users and system administrators can improve the effectiveness of information security. Human behavior is complex and multi-faceted, and this becomes more complicated in organizations whereas their culture defies the expectations for control and predictability that developers routinely assume for technology. In support of this, the OECD (2002) Guidelines for the Security of Information Systems, also state that: "The diversity of system user-employees, consultants, customers, competitors or the general public-and their various levels of awareness, training and interest compound the potential difficulties of providing security". The present research takes a different perspective on this issue by focusing on organizational information security: the values and beliefs held within organizational cultures that influence the confidentiality, availability, authenticity and integrity of data through the organizations' information systems. To this end, this research examines the extent to which information security behaviors, as part of an organizational culture, relate to a common work attitude variable known as organizational commitment.

The main research assumption is that organizational commitment would relate positively to the enactment of information security behaviors such as following new security policies and new technologies that are in effect of the organizations' business objectives. Hence, information security should support the mission of the organizations, it must be cost effective and fit into the organizations' culture seamlessly; that is, integrate technology, processes and people.

2. Organizational information security background

Although a number of IS security approaches have been developed over the years that reactively minimize security threats such as checklists, risk analysis and evaluation methods, there is a need to establish mechanisms to proactively manage IS security. That said, academics' and practitioners' interest has turned on social and organizational factors that may have an influence on IS security development and management. For example, Reference [29] have emphasized the importance of understanding the assumptions and values of different stakeholders to successful IS implementation. Such values have also been considered important in organizational change [34], in security planning [39] and in identifying the values of internet commerce to customers [14]. Reference [7] have also used the value-focused thinking approach to identify fundamental and mean objectives, as opposed to goals, that would be a basis for developing IS security measures. These value-focused objectives were more of the organizational and contextual type.

A number of studies investigated inter-organizational trust in a technical context. Some of them have studied the impacts of trust in an e-commerce context [9,10,25] and others in virtual teams [31,32]. Reference [42] studied trust as a factor in social engineering threat success and found that people who were trusting were more likely to fall victims to social engineering than those who were distrusting. Reference [16] used a goal setting approach to identify weaknesses in security management procedures in terms of the trust employees put on other group members to communicate security goals efficiently. Reference [35, p. 1551] also reviewed 1043 papers of the IS security literature for the period 1990-2004 and found that almost 1000 of the papers were categorized as 'subjective-argumentative' in terms of methodology with field experiments, surveys, case studies and action research accounting for less than 10% of all the papers.

3. Information security culture

Information security culture is part of the corporate culture and defines how employees see the organization [33]. Most of the literature on organizational culture focuses on the hypothesis that strong cultures enhance organizational performance [17,2]. This hypothesis is based on the notion that having widely shared and commonly held strong organizational norms and values leads to higher performance through at least three ways. First, a strong culture enhances coordination and control within the organization. Second, it improves goal alignment between the organization and its members. Third, a strong corporate culture improves employee efforts. Similarly, organizational culture is a system of learned behavior which is reflected on the level of end-user awareness and can have an effect on the success or failure of the information security process. Reference [1] found that users considered a user-involving approach to be much more effective for influencing user awareness and behavior in information security. Reference [19] studied influences that affect a user's security behavior and suggested that by strengthening security culture organizations may have significant security gains. Reference [5] investigated security information management as an outsourced service and suggested augmenting security procedures as a solution, while [40] suggested a model based on the Direct-Control Cycle for improving the quality of policies in information security governance.

Reference [13] discussed the importance of gaining improvements from software developers during the software developing phase in order to avoid security implications. Reference [36] advanced a new model that explains employees' adherence to IS policies and found that threat appraisal, self-efficacy and response efficacy have an important effect on intention to comply with information security policies. Culture is a perception of organizational norms and values and so it exists within the organizations, not in the individual. To this end, individuals with different backgrounds or at different levels in the organization may tend to describe the organization in similar way. Security culture is used to describe how members perceive security within the organization. Since security and risk minimization are embedded into the organizational culture, all employees, managers and end-users must be concerned of security issues in their planning, managing and operational activities. In order to ensure effective and proactive information security, all staff must be active participants rather than passive observers of information security. In doing so, staff must strongly held and widely share the norms and values of the organizational culture in terms of information security perception.

5. Organizational commitment

Reference [22] suggests that commitment is the determination to try for a goal and the persistence in pursuing it over time.

In the current research paper, commitment is defined as a state of mind that holds people and organizations in line of behaviour [38] and encompasses psychological factors that force individuals to take action [15] in effect to information security planning. The successful development of an information system has long been believed to depend on the commitment to the project [23,18]. It also affects an organization's effectiveness in converting information technology investments into useful outputs [41]. On the contrary, lack of commitment could lead to indifference or deliberate resistance [11] and may even cause project development to be abandoned [8]. In a similar vein, commitment is clearly important to the success of IS development projects, but managers may sometimes become too committed to certain IS projects [26]. Sometimes decision makers are too committed to an information system project, even though, they are faced with indications that the project may be failing. In some cases, information systems development projects may take too much time, or even fail, if commitment is erratic, as in situations where the champion for the project departs in the middle of the project [30]. Considering that there is feedback on goal achievement, goal commitment, and task knowledge and given requisite ability and task familiarity, the more difficult and specific the project, the higher the performance [20, 21].

Also, Reference [4] reported that when individual and group goals were congruent, group members were committed to increasing group performance. A major need for effective information security arises from the poor state of security caused by low awareness levels within organizations. To this end, there is need for increased security awareness in all employees and users at all levels, in terms of task knowledge and familiarity to information security. There was a belief that information technology and security were difficult issues to be understood by non-IT staff. Nowadays, it is believed that people make the difference to information technology and security and that training on the ethical, legal and security aspects of information technology usage should be ongoing at all levels within organizations [27]. Since people react differently to poorly constructed security messages, communication will broken down and may confuse task knowledge and security risk awareness among the employees. Thus, the main implication for information security management is to focus on changing attitudes and human behaviour which are part of the organizational culture in order to enhance awareness among the employees about information security task related tasks. In doing so, organizational commitment will increase since it is important to realize that awareness is one of the first steps to obtain active employee's participation in the information security process and vice versa. That is, a well established security awareness will ensure project commitment though active participation of employees to security task related projects.

6. Survey of perceptions

Two hundred and twenty seven (93 women and 134 men) employees of a large sized bank in Greece took part in the survey. The respondents ranged from junior staff to senior management and were between the ages of 22 and 65. They completed an anonymous survey questionnaire that was circulated personally by the principal researcher and consisted by 18 items. The questions were designed to solicit a response on the participant's perception of risk, their perception of the likelihood of others being committed to organizational norms and values and their perception of information security in the corporate culture. Table 1 below shows an example of questions. For the risk behaviour based questions, respondents evaluated their likelihood of engaging in risk behaviours (i.e., '…indicate the likelihood of engaging in each activity) on a five point rating scale raging from 'Very likely' (1) to Very unlikely' (5). For the security perception questions, respondents rated their perception of the risk presented by each risky behaviour (i.e., …indicate how risky you perceive each activity to be) on a five point scale ranging from 'Very significant' (1) to 'Very insignificant' (5).

For the commitment based questions, respondents rated their perception of the likelihood of other people in the organization committing in activities (i.e., …your opinion what is the likelihood of people in the organization committing in the following activities) on a five point rating scale raging from 'Very likely' (1) to 'Very unlikely' (5). The information in this report is based on the initial response of the a hundred and twenty seven participants. Using a variation of Cochran's [3] formula suggested by Israel [12] to determine sample sizes necessary for given combinations of precision, confidence levels and variability, this survey should have a confidence level of 95% with a precision level of greater that ±4%. The main purpose of the survey was to find out mainly the following: What is the individual's perception of the risk involved with certain activities? What is the individual's perception of the likelihood of other in the organization committing to certain security activities? What is the individual's perception of information security culture within the organization? The intended outcome of this research is to develop a strategy to improve information security culture and an improved organizational commitment to security activities within the organizations. The questions analyze the different components relating to information security: 1) individual perception of risk, 2) individual perception of other committing to information security activities,

3) individual perception of risk behaviour in the cultural context. Table 2 below, shows the responses in percentages of the individual perception of risks for certain activities (perceived values), the individual perception of other committing to security activities (commitment), and the individual perception of risk behaviour (culture). The results give interesting insights and reveal gaps in the individual's perception of information security and commitment in the context of organizational culture. Male and female respondents don't differ significantly in their perceptions of risk in all activities with the exception of challenging another's knowledge on security tasks where 62% of females perceived very significant risk in undertaking this activity. It would appear that generally female respondents are less likely to engage in risky behaviour. Surprisingly 38% of both male and female respondents perceive that it is likely or very likely that people within the organization are sharing passwords with other people. In addition, 84% of male and 78% of female respondents perceive it to be a significant risky activity. While 11% of male and 13% of female respondents implied that they would share a password with other people. Thus, it appears that while sharing passwords with others is considered risky, the culture of the organization ignores such behaviour.

In the context of committing to risky activities, 23% of male and 33% female respondents perceive hiding information from a co-employee as a risky activity yet 82% of male and 73% of female respondents said it was unlikely or very unlikely they would participate in the activity. This may imply that while individuals don't perceive this as a very risky activity, they intent to share information with others which means that the organization's culture enables cooperation and overall commitment among the employees. Of the total respondents 42% said that they would reuse the same password many times and in terms of information security projects 53% said that they would ask for clarity of goal achievement in case they are confused. Finally, 53% said that project commitment initiates from top-executives. The questionnaires were taken anonymously to enhance true value, although there is an uncertainty of answers that conform to what the security policy state as well as the employee's actual behaviour.

Insert table (1) about here
Insert table (2) about here

7. Conclusions

The more organizations rely on information systems to survive in competitive markets, the more increasing becomes the need to maintain the confidentiality, availability, integrity and authenticity of data through the organization's network and telecommunication channels. However, the technology advancement rate for the use and management of these information systems is more radical than the development of means for ensuring the confidentiality, availability, integrity and authenticity of data through them. That is, as organizations become aware of security issues, security threats remain high. Although achieving the required level of information security within organizations requires also security awareness and control, a better understanding of the organizations' culture in which security measures are tailored to, is also important. In this way, organizations may have a clearer insight into how to commit more effectively to such security measures. This research examined the extent to which information security behaviors, as part of an organizational culture, relate to a common work attitude variable known as organizational commitment.

The main research assumption was that organizational commitment would relate positively to the enactment of information security behaviors such as following new security policies and new technologies that are in effect of the organizations' business objectives. Information security needs to be embedded in the organizational culture though which organizational commitment can be achieved by having a clear insight into the security measures and objectives of the organization. A well established culture and well trained end-users can address the security planning and management of information within an organization. Overall, information security should support the mission of the organizations, it must be cost effective and fit into the organizations' culture seamlessly, that is integrate technology, processes and people. Future research could focus on the perception and communication of security risk messages and how they are circulated among the employees in relation to the determinants of organizational commitment to information security projects.

References

1. Albrechtsen, E. 2007 A Qualitative Study of User's View on Information Security,
2. Computer and Security, 26(4), pp. 276-289.
3. Burt, R.S., Gabbay, S.M., Holt, G., Moran, P. (1994) Contingent Organization as a Network Theory: The Culture-Performance Contingency Function, Acta Sociologica, 37(4), pp. 345-370.
4. Cochran, W. 1977 Sampling Techniques, Canada: John Wiley & Sons Inc.

5. Crown, D.F. and Rosse, J.G. (1995) Yours, Mine and Ours: Facilitating Group Productivity Through the Integration of Individual and Group Goals, Organizational Behaviour and Human Decision Processes, 6(4), pp. 138-150.
6. Debar, H. and Viinikka, J. 2006 Security Information Management as an Outsourced Service, Computer Security, 14(5), pp. 416-434.
7. Dhillon, G. 2001 Challenges in managing information security in the new millennium. In: Information security management: global challenges in the new millennium, ed. Dhillon, G. USA: Idea Group Publishing, pp. 1-8.
8. Dhillon, G. and Torkzadeh, G. 2006 Values-focused assessment of information system security in organizations, Information Systems Journal, 16(3), pp. 293-314.
9. Ewusi-Mensah, K. and Przasnyski, Z.H. (1999) On Information Systems Project Abandonment: An Exploratory Study of Organizational Practices, MIS Quarterly 15(1), pp.67-88.
10. Gefen, D., Karahanna, E. and Straub, D. (2003) Trust and TAM in online Shopping: An Integrated Model, MIS Quarterly, 27(1), pp. 51-90.
11. Gefen, D. and Straub, W. (2004) Consumer Trust in B2C e-Commerce and the Importance of Social Presence: Experiments in e-Products and e-Services, Omega, 32(6), pp. 407-424.
12. Grover, V., Lederer, A.L., and Sabherwal, R. (1988) "Recognizing the Politics of MIS", Information and Management 14(3), pp.145-156.
13. Israel, G. 2002 Determining Sample Size, Food and Agricultural Sciences, University of Florida, USA.
14. Jones, R.L. and Rastogi, A. 2004 Secure Coding: Building Security into the Software Development Life Cycle, Information Systems Security, 13(5), pp. 29-39.
15. Keeney, R.L. (1999) The Value of Internet Commerce to the Customer, Management Science, 45(3), pp. 533-542.
16. Kiesler, C.A. (1971) The Psychology of Commitment: Experiments linking behaviour to beliefs, New York: Academic Press.
17. Koskosas, I.V. (2008) Goal Setting and Trust in a Security Management Context, Information Security Journal: A Global Perspective, 17(3), pp. 151-161.
18. Kotter, J.R. and Heskett, J.L. (1992) Corporate Culture and Performance, New York: Free Press
19. Kwon, T.H. and Zmud, R.W. (1987) Unifying the Fragmented Models of Information Systems Implementation, In: Critical Issues in Information Systems Research, R.J. Boland and R.A. Hirschheim (eds.) Wiley, New York.
20. Leach, J. 2003 Improving User Security Behaviour, Computers and Security, 22(8), pp. 685-692.
21. Locke, E.A. and Latham, G.P. (1990) A Theory of Goal Setting and Task Performance, Englewood Cliffs, NJ: Prentice-Hall.
22. Locke, E.A. and Latham, G.P. (2002) Building a Practically Useful Theory of Goal Setting and Task Motivation, American Psychologist, 57(9), pp. 705-717.
23. Locke, E. A., Shaw, K. N., Saari, L. M., & Latham, G. P. (1981) Goal setting and task performance: 1969-1980. Psychological Bulletin, 90, pp. 125-152.
24. Lucas, H.C. Jr. (1981) Implementation: The Key to Successful Information Systems, Columbia University Press, New York.
25. McCumber, J. 2005 Assessing and managing security risk in IT systems: a structured methodology, USA: Addison- Wesley.
26. McKnight, D.H., Cummings, L.L. and Chervany, N.L. (2002) Developing and Validating Trust Measures for E-Commerce: An Integrative Typology, Information Systems Research, 13(3), pp. 334-359.
27. Neumann, S. (1994) Strategic Information Systems: Competition Through Information Technologies, MacMillan College Publishing Company, Inc. New York.
28. Nolan, J. 2005 Best practices for establishing an effective workplace policy for acceptable computer usage, Information Systems Control Journal, 6(2), pp. 32-35.
29. OECD-Organization for Economic Co-operation and Development (2002) *Guidelines for the Security of Information Systems and Networks Towards a Culture of Security*, report.
30. Orlikowski, W. and Gash, D. (1994) Technological Frames: Making Sense of Information Technology in Organizations, ACM Transactions on Information Systems, 12(3), pp. 174-207.
31. Reich, B.H. and Benbasat, I. (1990) An Empirical Investigation of Factors Influencing the Success of Customer-Oriented Strategic Systems, Information Systems Research, 1(3), pp.325-347.
32. Ridings, C., Gefen, D. and Arinze, B. (2002) Some Antecedents and Effects of Trust in Virtual Communities, Journal of Strategic Information Systems, 11(3/4), pp. 271-295.

33. Sarker, S., Valacich, S.J. and Sarker, S. (2003) Virtual Team Trust: Instrument Development and Validation in an IS Educational Environment, Information Resources Management Journal, 16(2), pp. 35-55.
34. Sherwood, J., Clark, A. and Lynas, D. 2005 Enterprise Security Architecture: A business- Driven Approach, San Francisco, CA, USA: CMP Books.
35. Simpson, B. and Wilson, M. (1999) Shared Cognition: Mapping Commonality and Individuality, Advances in Qualitative Organizational Research, 2, pp. 73-96.
36. Siponen, M. and Willison, R. (2007) A Critical Assessment of IS Security Research Between 1990-2004, The 15th European Conference on Information Systems, Session chair: Erhard Petzel, pp. 1551-1559.
37. Siponen, M., Pahnila, S. and Mahmood, A. 2007 Employees' Adherence to Information Security Policies: An Empirical Study, In: IFIP International Federation for Information Processing, Vol. 232, New Approaches for Security, Privacy and Trust in Complex Environments, eds. Venter, H., Eloff, M., Labuschagne, L., Eloff, J. von Solms, R., (Boston: Springer), pp. 133-144.
38. Souris, A., Patsos, D., and Gregoriadis, N. 2004 Information Security, ed. New Technologies, Athens, in Greek, First Edition.
39. Staw, B.M. (1982) Counterforces to change, In: P.S. Goodman and Associates (eds), Change in Organizations: New Perspectives on Theory, Research and Practice, pp. 87-121, San Francisco: Jossey-Bass.
40. Straub, D. and Welke, R. (1998) Coping with Systems Risks: Security Planning Models for Management Decision Making, MIS Quarterly, 22(4), pp. 441-469.
41. Von Solms, R. and Von Solms, S.H. 2006 Information Security Governance: A model based on the Direct-Control Cycle, Computers and Security, 25(6), pp. 408-412.
42. Weill, P., & Olson, M. H. (1989). An Assessment of the Contingency Theory of Management Information Systems. Journal of Management Information Systems, 6(1), pp. 59-85.
43. Workman, M. (2007) Gaining Access with Social Engineering: An Empirical Study of the Threat, Information Systems Security, 16(6), pp. 315-331.

Table 1. Example of Questions

15. In your opinion what is the likelihood of people in the organization participating in the following activities: Share their passwords with other employees. Access files they are not authorized for.
16. For each of the following activities, please indicate how risky you perceive each activity to be: Share your password with another employee. Access files you are not authorised for.
17. Please indicate your perception of others committing to these activities: Challenge the knowledge of another employee on security related tasks. Hide information from a co-employee in order to prove your skills.
18. For each of these activities, please indicate the likelihood of you engaging in the activity: Do not meet expiration dates on given tasks. Do not share your knowledge with others due to competitive reasons.

Table 2. *Risk perception, perception of others and likelihood ratings by gender*

All figures are shown as percentage (%)	**Male**	**Female**	**Male**	**Female**	**Male**	**Female**	**Male**	**Female**	**Male**	**Female**
Perception of risks for these activities	Very Significant		Significant		Neutral		Insignificant		Very Insignificant	
Share password with others	50	47	34	31	14	14	12	10	7	5
Challenge new employee in work place	20	24	38	38	17	12	11	13	6	4
Allow another to use ID pass/card	38	47	33	32	16	16	21	19	7	3
View or download prohibited material	32	47	31	33	20	10	7	11	5	4
Forge someone's signature	26	34	45	39	19	6	5	9	3	6
Access unauthorised files	37	31	41	34	17	17	19	13	4	3
Challenge another's knowledge on security tasks	40	62	30	22	12	11	32	29	12	5
Hide information from other employees	19	21	22	19	12	14	12	21	11	12
Perception of others in the organization committing in these activities	**Very Likely**		**Likely**		**Neutral**		**Unlikely**		**Very Unlikely**	
Share password with others	18	21	22	19	12	13	29	30	21	22
Challenge new employee in work place	16	14	12	11	13	18	24	21	11	22
Allow another to use ID pass/card	6	7	3	10	17	13	33	21	19	21
View or download prohibited material	3	1	3	12	11	10	32	29	51	14
Forge someone's signature	1	1	2	6	5	3	33	21	59	26
Access unauthorised files	2	3	5	4	15	13	20	19	50	61
Challenge another's knowledge on security tasks	25	31	24	21	12	11	21	19	48	72
Hide information from other employees	21	20	19	24	11	19	34	25	29	26
Likelihood of personally participating in these activities	**Very Likely**		**Likely**		**Neutral**		**Unlikely**		**Very Unlikely**	
Share password with others	6	4	7	9	11	14	21	18	49	50
Challenge new employee in work place	30	21	32	28	16	11	29	19	46	10
Allow another to use ID pass/card	7	3	3	2	17	12	23	18	33	30
View or download prohibited material	3	2	9	11	1	5	37	31	7	23
Forge someone's signature	4	1	8	2	1	6	11	9	43	56
Access unautorised files	3	2	8	4	11	5	12	9	77	56
Challenge another's knowledge on security tasks	35	31	23	21	16	10	19	21	44	43
Hide information other employees	32	29	31	28	17	22	33	41	49	32