Information Security Culture: A Survey

Oleksiy Mazhelis and Hannakaisa Isomäki

University of Jyväskylä, Finland
oleksiy.mazhelis@jyu.fi
hannakaisa.isomaki@jyu.fi

Abstract: Appropriate information security culture (ISC) is seen by researchers as critical for the organizations. This paper surveys the state-of-the-art in the field of ISC research, in order to reconcile the theoretical achievements adopted to ISC from adjacent disciplines with the core meaning of the ISC concept. Based on the conducted literature review, the theories, frameworks, and models created, tailored, or adopted by the ISC researchers are identified and discussed in the paper.

1 Introduction

The information security culture (ISC) has been seen from different viewpoints as: I) a set of information security characteristics valued in the organisation; ii) the assumption about what is acceptable; iii) the assumption about encouraged information security behaviour; and iv) the way people behave towards information security in the organisation [ME02a]. It has been also often defined as the set of shared, taken-for-granted, learned over time assumptions and beliefs [ST03, TVL06].

The ongoing endeavours to establish scientifically valid explanations of the ISC necessitate rigour in the very basic constructs of theory development. As argued in [GLT08], a good theory and its development rests in clear, insightful, and powerful concepts. Therefore, it is fruitful to look at the current ISC literature through the lenses of conceptual analysis. By doing so, theoretical achievements from other adjacent disciplines can be reconciled with the core meaning of the concept of ISC.

This paper surveys the contemporary ISC research from the viewpoint of the concepts used. Being a relatively young, the research on security culture employs theories, models, frameworks, concepts, from adjacent disciplines; e.g. organisational culture [RMC07], organisational behaviour [ME02b], knowledge creation [TVL06], and organisational learning [VV05], to name a few. The paper follows the systematic literature review method based on the structured approach [WW02]; the results of the review and conceptual analysis are reported in the paper.

2 Information security culture research

Contemporary research on ISC employs a variety of theoretical foundations from reference disciplines; these foundations were employed to construct management tools aimed at the successful establishment, assessment, and development of ISC, as described below.

2.2 Theoretical foundations

Organisational culture. Schein [Sc92] describes organizational culture as consisting of the visible artefacts level, the espoused values level, and the level of basic shared beliefs and assumptions which partially determine employees' behaviour. The ISC researchers have often taken this three-level model as their theoretical foundation [ME02a, VV04, Jo06, ST03, VV06]. Besides, by combining the works of Schein with the research on competing values and organisational culture profile, eight cultural dimensions were derived and applied in ISC research [RMC07].

Organizational behaviour. A change of the organizational behaviour is seen as a prerequisite for the emergence of a culture "conductive to the protection of information assets", and this change needs to be implemented at organization, group, and individual levels [ME02b, VV04]. Also Woodhouse [Wo08] bases his study on organisational behaviour. He proposes a referential process maturity model for assessing Information Security Management System within an organisation, where maturity is seen as changes in ISC reflecting the views and attitudes of organisational actors.

Education and organizational learning. Outcomes based education (OBE) has been suggested as an approach towards increased information security awareness, which in turn is seen as a means to establish an ISC in an organization [VV04a]. The OBE, as well as the NIST security training model and the Malhorta's organizational learning model, encompass key elements of a successful educational program, including thorough planning, goal setting, feedback, the insight into why learning is needed, and the customization of learning materials [VV04a].

Conscious competence learning matrix. Information Security Capability Maturity Model (CMM) has been introduced to evaluate, to what extent information security is embedded in the organization's corporate culture [TV06]. The CMM assumes that the individuals' competence progresses from unconscious incompetence, through conscious incompetence and conscious competence, to the stage of unconscious competence. It is assumed, that at the final fourth stage, critical information security practices adhering to the vision of the top management should become a part of the corporate culture.

Knowledge creation. Nonaka's model of knowledge creation [No94] differentiates tacit knowledge (beliefs, attitudes, skills) and explicit knowledge (overt, objective, rational, ready to communicate). Interacting tacit and explicit knowledge produces new knowledge, and four types of such knowledge creation are identified. Thomson, Von Solms, and Louw [TVL06] have applied the Nonaka's model to facilitate the creation and dissemination of security-related knowledge throughout the organization.

Holistic framework. Rather than borrowing from related disciplines, Dojkovski, Lichtenstein, and Warren [DLW07] attempt to build a new holistic conceptual ISC framework (focusing on Australian SMEs) by following the qualitative, interpretivist approach. The authors created a preliminary version of the framework based on literature review, and revised it in a focus group. Interpretative case studies were then conducted by using semi-structured interviews, in order to build the framework.

2.2 Managerial tools: standards, architecture, governance frameworks

Information security architecture (ISA) refers to the comprehensive set of managerial and technical means aimed at fostering the information security in an organization. Some of the ISA suggestions include security culture as one of the aspects to be taken into account: the information security architecture [Tu00] mandates that the corporate culture should be taken into account to avoid pitfalls (e.g. policies need to be customized); in Integrated ISA [EE05], security culture is seen as one of the aspects which a successful ISA has to take into account.

Security management frameworks. The international standard ISO/IEC 17799 [Is05] sets the overall requirements for the information security management in an organization. One of the success factors for this standard is the adoption of "an approach to implementing security that is consistent with the organizational culture" [Is05].

Information security governance. Security governance specifies the involvement, decision rights, and accountability with respect to security-related decisions, leaving decision making and enforcing decisions to the management. Koh et al. [Ko05] found the ISC to be affected by the security governance, with the degree of social participation in decision making being arguably the most influencing factor. In [VE07], the security governance is seen as critical in establishing a security-conscious culture, and a holistic governance framework is proposed. In the COBIT® Security Baseline [Co07], the failure to communicate the right security culture and control framework is listed among the security risks to which executives are exposed.

3 Discussion and concluding remarks

In the paper, the advances in the ISC research were surveyed, with the aim to identify the theories, frameworks, and models created, tailored, or adopted by the research community.

Some of the key concepts found are summarized in Table 1. As can be seen from the table, the assessment, development, and improvement of ISC are among the concepts most commonly met in publications. Concepts often are borrowed from reference disciplines, such as organizational culture, organizational behaviour, knowledge creation, or refer to managerial tools. Several other key concepts identified are included in the table (e.g. safety culture), although, due to space constraints, these were not considered in the paper.

Prevailing in the literature is the *normative* approach describing, how a proper ISC should be established [TVL06], measured [ST03, Jo06], and improved [NZW05, Jo06]. For establishing or changing the culture, though, it is critical to understand, what the concept of the culture is, how it can influence (security-conscious) behaviour, and how the culture change can be effectively managed. To build such understanding, the researchers have adopted theoretical foundations including concepts, models, frameworks, and theories from reference disciplines. Meanwhile, little empirical evidence is available in the publications to support these normative claims. The *descriptive* approach is also used, e.g. as a means of determining, what the ISC is [Do07], how it manifests itself [ST03], and what is the relationship between the culture and other organizational phenomenon [KC07].

Citation	Improving or developing culture	Assessment of security culture	Theoretical foundations						Holistic framework	Managerial tools			Other issues		
			Organisational culture framework	Organisational & corporate culture	Organisational behavioural levels	Organisational learning & education	Conscious competence learning matrix	Modes of knowledge creation		Security standards	Architecture Information Security	Security governance frameworks	Safety culture	Work system elements	Security culture in global value network
[Ko05]	X	X	X									X			
[RMC07]		X	X									X			
[VE07]	X									X	X	X			
[ME02a]		X		X	X										
[TV06]				X			X								
[Kn06]	X	X													
[KC07]														X	
[HK03]															X
[EE05]										X	X				
[Jo06]	X	X		X									X		
[VV04b]	X	X		X	X										
[TVL06]	X			X			X	X							
[TV05]				X								X			
[KI03]	X														
[KNV04]					X				X						
[DLW07]	X								X						
[BF08]										X					
[ST03]		X		X											
[VV06]		X		X											
[VV04a]	X					X									
[Wo08]		X		X											

Table 1. Concept matrix based on the survey of information security culture literature

The results of the analysis suggest the directions, where the future work is needed. In particular, due to the scarcity of the descriptive approach, in future work, interpretative approach is important for studying the essence of the information security culture in organizations. In order to identify and categorize the elements of the security culture and relationships among them, the grounded theory research will be used, based on conducted semi-structured interviews.

References

[BF08] Barlette, Y.; Fomin, V.: Exploring the suitability of IS security management standards for SMEs. In Proc. of the 41st Hawaii International Conference on System Sciences, 2008.

[Co07] COBIT: COBIT® Security Baseline: An Information Security Survival Kit, 2nd edition, 2007.

[DLW07] Dojkovski, S.; Lichtenstein, S.; Warren, M.: Fostering information security culture in small and medium size enterprises: an interpretive study in Australia. In Proc. of the 15th European Conference on Information Systems, 1560-1571, 2007.

[EE05] Eloff, J.H.P.; Eloff, M.M.: Information security architecture. Computer Fraud & Security, 10-16, November 2005.

[GLT08] Grover, V.; Lyytinen, K.; Tan, B.C.: Contributing to Rigorous and Forward Thinking Explanatory Theory. Journal of the Association for Information Systems 9(2), 40-47, 2008.

[Is05] ISO/IEC 17799: Information technology – Security techniques – Code of practice for information security management. ISO/IEC, 2005.

[Jo06] Johnsen, S. O.; Hansen, C. W.; Nordby, Y.; Dahl, M. B.: Measurement and improvement of information security culture. Measurement and control, 39 (2), 52-56, 2006.

[HK03] Helokunnas, T.; Kuusisto, R.: Information Security Culture in a Value Net. Proc. of the.2003 IEEE International Engineering Management Conference, pp.190-194, 2003.

[HF82] Howell, W.C.; Fleishman, E.A.: Human performance and productivity, Information processing and decision making 2, Erlbaum, Hillsdale, New Jersey, 1982.

[Kn06] Knapp, K.: Information Security: Management's effect on culture and policy. Information Management & Computer Security 14(1), 24-36, 2006.

[Ko05] Koh, K.; Ruighaver, A.B.; Maynard, S.B.; Ahmad, A.: Security governance: Its impact on security culture. In Proc. of the 3rd Australian information security management conference, Perth, Australia, 2005.

[KC07] Kraemer, S; Carayon, P.: Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. Applied Ergonomics 38, pp. 143–154, 2007.

[KI03] Kuusisto, T.; Ilvonen, I.: Information security culture in small and medium size enterprises, Frontiers of e-Business Research, 2003.

[KNV04] Kuusisto, R.; Nyberg, K.; Virtanen, T.: Unite Security Culture: May a unified security culture be plausible? In A. Jones (Ed.), Proc. of the 3rd European conference on Information Warfare and Security, pp 221-236, 2004.

[ME02a] Martins, A.; Eloff, J.H.P.: Assessing Information Security Culture. ISSA 2002, Muldersdrift, South Africa, 10-12 July 2002.