2005

Value Sensitive Approach to IS Security - A Socio-Organizational Perspective

Ella Kolkowska
Oerebro University, ella.kolkowska@esi.oru.se

Value Sensitive Approach to IS security – a socio-organizational perspective

Ella Kolkowska
Örebro University, Department of Informatics
ella.kolkowska@esi.oru.se

ABSTRACT

In this paper we present a *Value Sensitive Approach* (VSA) to information systems security (ISS) within organizations. The approach helps to identify organizational and individual values, since we believe that objectives suitable for each organization can be identified by eliciting these values. We then discuss how organizational goals, strategies and culture together with individual values decide what relevant security issues for this particular organization are. We then discuss how organizational goals, strategies and culture, together with individual values decide the relevant security issues for a particular organization.

Different methods to observe and identify values are discussed and evaluated. Then two different methods for identifying values are presented. Values – focused thinking is presented as a method for identifying values that guide decision makers and security managers. Scenarios are presented as a method to elicit values from actor groups who are less used to thinking in terms of information security issues.

The *Value Sensitive Approach* to *ISS* presented in this paper will contribute to the ongoing research efforts to view security problems from a more holistic, socio-organizational perspective.

Keywords

Security values, IS Security, socio-organizational perspective, security objectives.

INTRODUCTION

Taking information systems security (ISS) issues in modern organizations seriously requires more than what traditional technology-centered security approaches can offer us. Equally important are relevant socio-technical aspects, such as individual and organizational values. Traditional security approaches have been developed with monolithic, centralized, and hierarchical organizations in mind. Such approaches focus on the formal part of an information system and suggest technical solutions to a limited set of security problems. Attempts have been made to apply these approaches into today's ambiguous organizational structures (Dhillon and Backhouse 2000). Their conclusion is that traditional security approaches do not satisfy the new challenges arising in ISS and that serious security breaches still occur, harming individuals and organizations. Various authors suggest that a new approach that considers social and organizational aspects is needed to deal with ISS problems (e.g., Baskerville, 1993; Dhillon and Backhouse 2000, 2001; Dhillon and Torkzadeh, 2001; Siponen and Baskerville, 2001; Straub and Welke, 1998). They point out that conceptualization and assessment of ISS within organizations should be re-examined.

Various researchers argue that information security management and security objectives should differ between organizations because different organizations have different goals, strategies, cultures and structures (e.g. Baskerville, 1993; Von Solms, 2000). Because problems within organizations are different from the ones that are external, ISS should be managed differently within the organization and outside the organization. According to Von Solms (2000), ISS outside the organization should be managed with the help of an internationally accepted framework (like e.g. BS7799) while managing of ISS within an organization should be managed by a measurement system suitable for each organization. There are a few methods to manage ISS outside organizations, but it is unclear which methods to use for managing ISS within organizations and which objectives different organizations have with ISS.

Today's organizations are characterized by high professionalism and offer the employees a great deal of freedom to exercise discretion in their work (Robbins and Barnwell, 2002). In such organizations employees' security behaviors are difficult to formalize by rules, procedures and regulations and sometimes relevant rules to follow may be missing. (Robbins and Barnwell, 2002). Solely technical solutions do not work either. There is an evident need for new approaches for managing ISS that can reflect on users' behavior in information handling (Dhillon and Backhouse, 2000). Humans' behavior depends

on values they hold. (Mumford, 1981) Values determine and guide human actions, feelings and beliefs and consequently determine the organization where they work. Because of that, managing of ISS in organizations ought to begin with values.

A conclusion from the discussion above is that there is a need for new approaches for ISS within organization. The new approaches should vary between different organizations and they ought to consider aspects like humans' behavior in information handling. Ultimately, a value focus seems valid. The conclusion leads us to following research questions: How can we handle value dimensions in ISS management in different organizations? What are values and how are they expressed? What methods can we use to study organizational and individual values? How can we study values?

The Aim of this paper is to present a *Value Sensitive Approach* (VSA) to ISS within organizations. VSA to ISS is an attempt to provide a methodological framework for identifying organizational and individual values. The values can then be transformed to objectives suitable and adapted for each organization, since we believe that the objectives should vary between different organizations.

The result of the VSA will be a long list of individual and organizational values. The values will then be converted into objectives. Important questions in this context are: what objectives are important in different organization? How should we engage in trade-offs among competing objectives in different organizations? (e.g. autonomy vs. security, or anonymity vs. trust)? Should moral values (e.g. a right to privacy) have greater weight than, or even trump, non-moral values. We believe that there might be a pattern in different organizations on how the objectives should be prioritized. For example in some organizations openness may be most important and this should always be prioritized before e. g. confidentiality.

PRINCIPLES FOR MANAGING IS SECURITY

People tend to interpret ISS differently. According to the technical tradition, security concerning IT and information is typically defined by three aspects; confidentiality, integrity and availability (CIA) (see e.g. Gollman, 1999; Harris, 2002; Jonsson, 1995). Confidentiality is the prevention of unauthorized disclosure, integrity is the prevention of unauthorized modification and availability means ensuring authorized access of computer systems and data when required. The concepts are viewed as the *objectives* with managing information security in organizations. There are two main problems with the traditional objectives: (1) They are mostly (eller only) applicable when information is viewed as "data". Because of that, they are insufficient when we have to take social and organizational aspects in information security into consideration. (Dhillon and Backhouse 2000) (2) They focus on security breaches made by unauthorized users and are consequently insufficient for managing ISS within organizations since security breaches often come from authorized users (Dhillon and Backhouse 2000).

The traditional objectives (CIA) should be complemented by new objectives that consider ethical, social, and organizational implications of IT use. Dhillon and Backhouse (2000) suggest that the traditional concepts (CIA) ought to be complemented by new principles: responsibility, integrity, trust and ethicality (RITE). *Responsibility* means knowledge of rules and understanding of responsibilities. *Integrity* means a feeling of integrity as a member of an organization and loyalty to the organization. *Trust* means that the relationships within organizations should be built on trust rather than control. *Ethicality* means that members of an organization should act according to ethical principles instead of formal rules. These new principles can help to generate a more holistic perspective on security problems which also considers social and organizational aspects.

Another attempt to find new objectives for managing of information security according to a socio-organizational perspective is the study of Dhillon and Torkzadeh (2001). The authors used Keeney's (1992) value-focused thinking approach to elicit values which security managers might have in managing IS security. The values have then been converted to objectives deemed essential in the protection of information resources of an organization (Dhillon and Torkzadeh, 2001). The study shows that CIA is only a small part of all possible objectives in managing of ISS. Objectives like maximizing awareness, developing and sustaining an ethical environment, enhancement of the integrity in business processes, maximizing data integrity, maximizing organizational integrity, maximizing privacy etc. have shown to be essential in managing ISS within organizations. Based on this study, we have made some reflections we believe could be further investigated.

Further research about values in ISS

Values exist on both collective and individual levels (Hofstede, 1980). On the collective level there are values that an individual share with some, but not all other people (e. g within a group or organization). Collective values arise in a social context where people share the same experiences and are used to show what is important and how things ought to be (Legge, 1984). Both collective values and individual values decide what is relevant for a person in a certain situation (March and Olsen, 1989). Individual values are unique and provide a wide range of alternative behavior within a given collective (Hofstede, 1980). Consequently, values can be considered at an individual level (Shaw, 1980), as well as at a collective level

(Weick and Bougon, 2001). Because both organizational and individual values determine peoples' behavior, we believe that both individual and organizational values should be considered when objectives for the management of ISS within organization are decided. Furthermore, we believe that consideration of organizational values in the creation of objectives for managing ISS can contribute to differentiation of security solutions providing suitability for various organizations.

There are different groups of actors within an organization. The different groups might hold different values. Dhillon and Torkzadeh (2001) interviewed decisions makers to elicit individual values. We think that it may be interesting to know if all other actor groups in an organization share the same values. We believe that end-users are an important group that ought to be investigated. Security managers decide which security methods to implement in an organization, but the users are the ones have to use and accept them. It is often said that one of the biggest security risk related to IT-systems are the people using them (e.g. Schultz et al, 2001; Sasse et al, 2001).

According to the discussion above, we argue that it is important to consider both organizational and individual values when objectives for managing ISS within organization are decided. We also propose that different actor groups' values should be considered in the process.

STUDYING VALUES

Values have been defined in different ways: as concepts that express people's feelings and attitudes or by intentions that decide people's behavior (Bergström, 1992). As a concept that expresses feelings and attitudes, a value refers to what a person or group of persons consider important in life (Pearsall, 1998).

Another way to define values is as intentions that decide peoples' behavior. It means that people always, more or less, act with conscious intentions. Values represent a person's principles, deciding how the person acts (Pearsall, 1998).

Because the value concept is relatively unspecific, it is quite challenging to study. Values are subjective and often unconscious and they are exposed on different levels (collective and individual). In every specific situation there is seldom only one single value. Instead, there are several different, sometimes conflicting values, which can be studied (Lundquist, 1991). Values are not observable directly because they are based on peoples understanding and translation of the world (Mumford, 1981). However, values are manifested by words and actions and by studying these, one can they analyze the underlying value base (Hofstede 1980, Kluckholn, 1951).

There are different strategies for studying values based on words and actions. In this paper, we present a classification by Hofstede (1980). The author has studied national and organizational cultures by focusing a few value dimensions. His work; Culture's Consequences (1980) is one of the most influential piece of work in the study of cross cultural management. According to Hofstede (1980) the action related to values can be either provoked (stimulated by the researcher for research purposes) or natural (taking place or having taken place regardless of the research and the researcher). The actions can be observed directly (actions and behavior) or through verbal descriptions (words). The combination of these two classifications leads to four types of strategies for studying values (see Table 1).

	Provoked	Natural
Words	1. Interviews Questionnaires Projective tests	2. Content analysis of speech acts Discussions Documents
Actions	3. Laboratory experiments Field experiments	4. Direct observation Use of available descriptive statistics

Table1 Four available strategies for studying values (Hofstede, 1980, p 5)

Hofstede (1980) points out that it is difficult to achieve validity in studying values because the ambiguous matter of the value concept and because unclear correspondence between observed actions and words and the underlying values constructs. To achieve validity in a study, the researcher must combine different types of strategies for studying values (see Table 1).

Through a literature review, Hofstede (1980) has found that questionnaires are the most common method to identify values and that methods in cells 2, 3, 4 are rarely used for this task. However, the human computer interaction (HCI) community has had a longstanding interest in designing systems that support human values and they have tested many of these methods for this chore (Friedman and Kahn, 2003). Because values can be studied by studying actions that manifest those values, an entire range of quantitative and qualitative methods used in social science research can be used. Any human action can be studied by observations, experimental manipulations, collection of relevant documents, and measurements of user behavior and human physiology and those methods are potentially applicable in studying values (Friedman and Kahn, 2003).

We have recognized two possible strategies to identify organizational and individual values: a quantitative strategy and a qualitative strategy. In the quantitative strategy we could use the values identified by Dhillon and Torkzadeh (2001) and the principles identified by Dhillon and Backhouse (2000) to formulate questions for a standardized questionnaire. Advantages with this strategy would be that respondents that are less used to thinking in terms of information security issues would have an easier task answering structured questions. Disadvantages of this strategy would be that respondents might be limited to the presented alternatives and consequently, some important values could be missed out. Furthermore, standard behavioral research methodology textbooks (e.g. Blalock and Blalock, 1971) recommend starting with a qualitative orientation and following up with a quantitative verification. Thus, we believe that it may be a good idea to start with a qualitative method (like in-depth interviews) for exploration within the ISS area and then follow up the study with a quantitative verification in further research. Interviews in comparison with questionnaires allow asking follow up questions and more detailed questions which can lead to deeper understanding of the answers. Hence, we have decided to use a qualitative strategy to identify the individual and organizational values. In line with the qualitative strategy, unstructured methods should be used to identify organizational and individual values. In-depth interviews and projective tests can be used to identify individual values, and interviews, discussions and documents analysis can be used to identify organizational values.

We have called the process of identifying organizational and individual values, the Values Sensitive Approach (VSA) to ISS. VSA is further elaborated in the following section.

VALUE SENSITIVE APPROACH TO ISS

VSA to ISS is an effort to provide a methodological framework to handle the value dimensions in ISS management within an organization. The approach helps identifying organizational and individual values which then can be transformed into relevant ISS objectives suitable for various organizations. The VSA to ISS is a complement to the ideas presented in Dhillon's and Torkzadeh's (2001) study (see "*principles for managing IS security).*

Identifying Organizational Values

Organizational values are part of an organizational culture (Robbins and Barnwell, 2002). It is difficult to decide what an organizational culture is. Many researches consider an organizational culture as an unclear phenomenon. It has previously been defined as "the dominant values espoused by an organization" (Robbins and Barnwell, 2002, 438) and "the basic assumptions and beliefs that are shared by members of an organization" (Robbins and Barnwell, 2002, 438). All definitions of organizational culture refer to a system of shared meaning. In every organization there are patterns of beliefs, symbols, rituals, myths and practices which have evolved over time (Hofstede, 1990; Schein, 1985). These in turn, create common understandings among members concerning what the organization is and how its members ought to behave. Symbols are words or objects that have a special meaning within a given culture. Myths are persons who are important in the culture and who are models for behavior. Rituals are collective activities that actually are unnecessary, but nonetheless socially important within a culture. Symbols, myths and rituals can be considered as "practices" because they are visible to an observer. However, we stress that the most important aspects in an organizational culture are the values (see Fig. 1). Dimensions that describe organizational values are: individual initiative, risk tolerance, direction, integration, management support, control, identity, reward system, conflict tolerance, and communication patterns (Robbins and Barnwell, 2002).

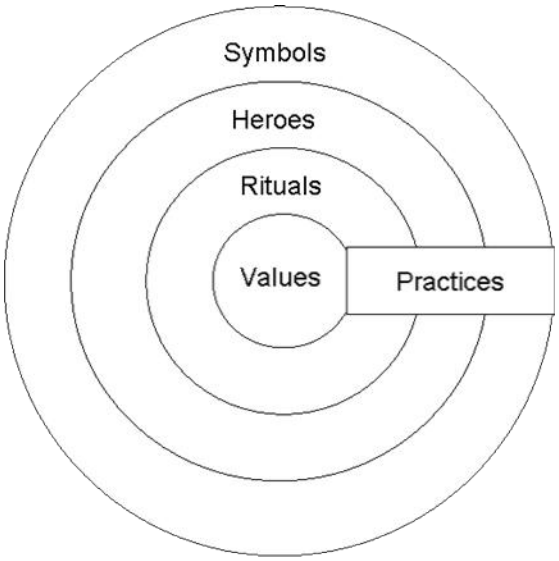

Figure 1. Manifestations of culture: From Shallow to deep.
(Hofstede, 1990, p 291)

Both practices and values are essential in studying of organizational values. An important question is what characterizes "an organization" from a cultural point of view? There is both a theoretical and an empirical problem when we want to decide analytical the level for studying organizational culture. One organization may include a number of culturally different departments, and these departments may consist of culturally different work groups. In determining the sufficient amount of units to be used for studying organizational values, we will take a pragmatic approach, i.e. we will follow the management's judgment about whether a unit is culturally homogeneous. Depending on the management's judgment we will decide if we will study the entire organization and/or parts of the organization. If the research results show us that the chosen level of analysis is inaccurate and the unit is culturally heterogeneous, we can choose a more appropriate level afterwards.

Values and practices can be exposed in different strategic documents (e.g. business vision, policies) or protocols. They can be manifested by actions or words during strategic meetings. By analyzing these documents and meetings and interviewing people we can identify what is deemed important in an organization? For example, we can ask us questions like: What is the special vocabulary that only insiders understand? (To understand organizational symbols). What kinds of people are most likely to make a fast career here? (To identify organizational heroes) In which meetings do the employees participate? How do people behave during these meetings? (To identify organizational rituals). What do people like to see happen here? What is the biggest mistake a person can make? Which work problems can engage the employees? (To identify organizational values)

On this way we can find answers about organizational practices and values like e.g. the work atmosphere (if a lot of freedom is given to the employees, cooperation vs. competition), leadership, decision-making (democratic vs. undemocratic) etc.

Identifying individual values

The individual values can be identified through interviews with relevant people. Interviews can be carried out either on an individual or group basis. To identify individual values two methods are proposed: values – focused thinking and in-depth interviews with scenarios. Value – focused thinking is proposed as a method for identifying values that are held by decision makers and security managers. In-depth interviews with scenarios are presented as a method to elicit values that guide actor groups who are less used to thinking in terms of information security issues.

Identifying values by value-focused thinking

Decision makers' and security managers' values can be identified by using values – focused thinking (Keeny, 1999; Dhillon's and Torkzadeh's, 2001). We believe that these groups are used to thinking in terms of information security issues and can formulate a wish list in that context. There are several techniques that stimulate the identification of possible values recommended by value – focused thinking (see Table 2).

According to Keeny (1992) the process of eliciting values begins with a wish list that the respondents are asked to write down. The interviewer can ask the respondent; "What goals would you like to achieve in this situation?" Values in the list do not need to be presented with consideration to ranking or priorities. The phase results in a list of potential values the respondents might have for the specific context. The list is a basis for further probing. When questions like "If you had no limitations at all, what would your wishes be?" may be asked to expand the list.

Once the list is complete, it is useful to ask respondents to think about problems and shortcomings applicable to each and every wish on the list. Since individuals may have difficult to express values, Keeney (1992) suggest words, such as tradeoffs, consequences, impacts, concerns, fair, and balance, that should trigger questions to make implicit values more explicit. In our decision context of IS security, a possible value might be "maintain privacy", a suitable follow up question could be "do you think there are any problems with maintaining privacy?" The respondent's answer can generate more values: "It is difficult to know which information is considered private"; "Too many people have access to private information". In a similar way we can ask about consequences, goals, and alternatives (see Table 2).

	Possible questions
A wish list	What do you want? What do you value? What should you want?
Alternatives	What is a perfect alternative, a terrible alternative, some reasonable alternative? What is good or bad about each?
Problems and shortcomings	What is wrong or right with your organization? What needs fixing?
Consequences	What has occurred that was good or bad? What might occur that you care about?
Goals. Constraints and guidelines	What are your aspirations? What limitations are placed upon you?
Different perspectives	What would your competitor or your constituency be concerned about? At some time in the future, what would concern you?

Table 2. Techniques that stimulate the identification of values Keeny, 1992 p 543

Identifying values by scenarios

In-depth interviews with scenarios can be used as a method for identifying user values in IS security. We believe that these groups are not used to think in terms of information security issues. Because of that we cannot use a security specific terminology during the interviews. Value-focused thinking has been tested empirically in a limited study among users at Örebro University. The end users had difficulties to write down the wishes and goals they might have in relation to IS security. They wanted to hear some examples that could help them thinking in ISS terms. Unfortunately the examples limited their creativity and they didn't go beyond the example list presented by the researches. Hence, there is an apparent need for another method to identify the users' values.

According to the discussion in *studying values,* interviews are an available method for the identification of values. During the interviews we wanted to discuss user work situations and information handling. We wanted the users to reflect over the process with a focus on ISS issues. Since end users often do not know the terminology and scope of IS security, this could be difficult. One way to facilitate the discussion about complicated issues with users is using scenarios.

Scenarios are a commonly used method in HCI to expose users' experiences of using an information system (Nielsen, 1994). A scenario is a story which describes how a user uses an information system for a certain task (Carroll, 1995). Scenarios need to be representative for the tasks the users carry out in the normal course of work. To identify the scenarios it is vital to understand the work situation and tasks that the user usually does at his/her job (Nielsen, 1994). Advantages with scenarios are that they are very flexible and easy to understand. We find scenarios interesting to use in our study because their great communicative possibilities. We further believe that scenarios allow the use of projective tests (i.e. technique that involves

inferring values from the way respondents describe specific third persons) because we can use scenarios that describe a specific third person and discuss the scenarios with the respondent. It can be easier to discuss such scenarios, especially when the scenario describes some situation of crisis. Using scenarios this way can improve the validity of the study. Subsequently, we decide to identify users' values through in-depth interviews where the researches and users can discuss scenarios, prepared earlier.

Informants in the interviews should be chosen non-randomly in discussions with a contact person in the organization. To attain a representative sample of employees', we want to select: men and women, long time employees and new staff members in different jobs from all levels.

At the start of the interview the informant is asked to describe tasks that he/she usually does at his/her job, their work situation and the organization. These issues are not difficult to discuss. Employees express what their general beliefs and work goals are. They describe how they feel about the organization, if the organization is a desirable employer (with good pay, benefits and job security) or not. What they appreciate with the organization. Further the informant are asked to describe the working atmosphere in the organization i.e. relations to other employees. Areas that can be discussed then are: e.g. conflicts and direct confrontations, loyalty, friendliness, modesty etc. The researcher ought to ask follow-up questions to elicit users´ values. The researcher could ask e.g. "Do you like the competitive situation in the organizations? " "Why? Why not?" "Do you think that colleges should cover other people's mistakes?" "Why? Why not?" Identified values in this part of the interview are related to the individual's personal preferences in work and life-related issues, such as his or her preferred type of boss, such as whether competition among employees is a good or a bad thing etc.

In the second part of the interview the researches should find out values related to ISS issues. These issues are more difficult to discuss with the common user. Because of that the researches ought to use scenarios as help in the communication. Scenarios are based on the work description from the first part of the interview. For example the researcher can illustrate a simple situation when a user leaves the computer to do something else: "Imagine that you are working with an important document on your computer. One of your colleges asks you to come with him for a coffee break. What do you do?" The user could answer: "I just leave the computer and follow my colleges", suitable follow up question could be "why do not you log of the computer when you leave? The respondent might answer: "it takes too long time to log in again". The respondent's answer shows that he/she estimate usability as more important that security.

CONCLUSIONS AND DISCUSSION

The *Value Sensitive Approach* to information security presented in this paper contributes to the ongoing research efforts to view security problems from a socio-organizational perspective. The VSA is an attempt to handle the value dimensions in ISS management which can contribute to other research about new objectives for ISS management within organizations.

The VSA is a methodological framework for the identification of organizational and individual values. Values – focused thinking is proposed as a method for identifying values that guide decision makers and security managers. Scenarios are presented as a method to elicit values that guide other actor groups who are less used to thinking in terms of information security issues. Discussions and document analysis are presented as methods to identify organizational values.

Organizational and individual values identified by the VSA can be transformed into objectives suitable for various organizations, since we believe that the objectives should vary between different organizations. The processes of structuring values and developing objectives are beyond the scope of this paper and will be investigated in further research.

REFERENCES

1. Baskerville, R. (1997) New Organisational Forms for Information Security Management. *Computers and Security*, 16, 210.
2. Baskerville, R. (1993) Information systems security design methods: implications for information systems development, *ACM Computing Surveys*, 25, 375-414.
3. Bergström, L. (1992) Grundbok i värdeteori (2 ed.), Bokförlaget Thales, Stockholm.
4. Blalock, H. M.,Jr and Blalock, A. B. (1971) Methodology in Social Research. McGraw-Hill, London.
5. Caroll, J. (1995) Scenario –based design, John Wiley, New York.
6. Dhillon, G. and Backhouse, J. (2001) Current directions in IS security research: towards socio-organisational perspectives, *Information Systems Journal*, 11, 127-153.

7. Dhillon, G. and Backhouse, J. (2000) Information system security management in the new millennium, *Communications of the ACM*, 43, 125-128.
8. Dhillon, G. and Torkzadeh, G. (2001) Value-focused assessment of information system security in organisations, *Twenty-Second International Conference on Information systems*.
9. Friedman, B. and Kahn, P. H. (2003) Human values, ethics, and design. In J. Jacko and A. Sears, Eds., The *Human-Computer Interaction Handbook*. Lawrence Erlbaum Associates, Mahwah NJ.
10. Gollman, D. (1999) Computer Security, Wiley, Chichester, UK.
11. Harris, S. (2002). CISSP Certification Exam Guide, McGraw-Hill/Osbourne.
12. Hofstede, G. (1980) Culture's Consequences, Sage Publications, Beverly Hills.
13. Hofstede, G. (1990) Measuring Organizational Cultures: A Qualitative and Quantitative Study across Twenty Cases, *Administrative Science Quarterly*, 35, 2, 286-316.
14. Jonsson, E. (1995) A Quantitative Approach to Computer Security from a Dependability Perspective. Doctoral Dissertation, Department of Computer Engineering, Chalmers University of Technology, Göteborg.
15. Keeney, R. L. (1992) Value-Focused Thinking, Harvard University Press, Cambridge, MA.
16. Keeney, R. L. (1999) The value of Internet commerce to the customer, *Management Science*, 45, 533-542.
17. Kluckholn C. (1951) Values and value-orientations in the theory of action: an exploration in definition classification. In Talcott Parsons & Edward A. Shils (Eds) Toward a general theory of action. Theoretical foundations for the social sciences. Harper & Row, New York.
18. Legge, K. (1984) Evaluation planned organizational change, Academic Press, London.
19. Lundquist, L. (1991) Etik i offentlig verksamhet, Studentlitteratur, Lund.
20. March, J. and Olsen, J. (1989) Rediscovering Institutions. The Organizational Basis of Politics, The Free Press. A Division of Macmilan, Inc, New York.
21. Mumford, E. (1981) Values, Technology and Work, The Hague Martinus Nijhoff Publishers
22. Nielsen, J. and Mack, R. (1994) Usability inspection methods, John Wiley, New York.
23. Pearsall, J. (1998) The New Oxford Dictionary of English, Clarendon Press, Oxford.
24. Robbins, P. S. and Barnwell, N. (2002) Organisation theory. Concepts and cases, Prentice Hall, Australia.
25. Sasse, A., Brostoff, S., Weirich, D. (2001) Transforming the 'weakest link' — a human / computer interaction approach to usable and effective security, *BT technology journal*, 3, 19, 122-131.
26. Schein E., H. (1985) Organizational Culture and Leadership, Jossey-Bas, San Francisco.
27. Schultz, E. E., Proctor, R. W., Lien, M., Gavriel, S. (2001) Usability and security - An appraisal of usability issues in information security methods, *Computers & Security*, Amsterdam.
28. Shaw, M. L. G. (1980) On becoming a personal scientist: Interactive computer elicitation of personal models of the world, Academic Press, New York.
29. Siponen, M. and Baskerville, R. (2001) A new paradigm for adding security into IS development methods, In Advances in information security management & small systems security, J. Eloff, L. Labuschagne, R. Solms and G. Dhillon (Ed.), Kluwer Academic Publishers, Boston, 99-111.
30. Smircich L. (1983) Concepts of Culture and Organizational Analysis, *Administrative Science Quarterly*, 339.
31. Straub, D. W. and Welke, R. J. (1998) Coping with systems risks: security planning models for management decision making, *MIS Quarterly*, 22, 441-469.
32. Von Solms, S. (2000) Information Security – the Third Wave?, *Journal of Computers & Security*, 9, 7, 615-620.
33. Weick, K. E. and Bougon, M. G. (2001) Organisations as cognitive maps: Charting ways of success and failure, In Making sense of the organisation, K. E. Weick (Ed.), Blackwell Publishers, Malden, 308-329.