December 2006

Values for Information System Security in an Academic Environment: A Pilot Study

Ella Kolkowska
Örebro University

Values for Information System Security in an Academic Environment: A Pilot Study

Ella Kolkowska
Örebro University
ella.kolkowska@esi.oru.se

ABSTRACT

In this paper we present a process of identifying individual and organizational values within an academic environment. These values have been identified by using Value Sensitive Approach (VSA) in the area of Information System Security (ISS). VSA is a methodological framework for identifying organizational and individual values. We believe that ISS objectives and ISS strategy suitable for each specific type of organization can be decided by eliciting these values. The study resulted in a number of value areas related to university general issues (UGV) and ISS issues important within an academic environment. The UGV and the ISS values can be further analyzed and transformed into ISS objectives suitable within an academic environment. Furthermore the identified values should be considered when ISS strategy to achieve those objectives is decided. Results presented in this paper will contribute to the ongoing research efforts to view security problems from a more holistic, socio-organizational perspective.

Keywords

Values in information security, ISS objectives, studying values

INTRODUCTION

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 but traditional security approaches do not satisfy the new challenges arising in information system security (ISS) and serious security breaches still occur, harming individuals and organizations. (Dhillon and Backhouse, 2000).

There is an evident need for new approaches and new objectives for maintaining ISS (e.g. Baskerville, 1993; Dhillon and Backhouse, 2000, 2001; Dhillon and Torkzadeh, 2001; Siponen and Baskerville, 2001; Straub and Welke, 1998). The new approaches that consider social and organizational aspects have become more common in the ISS discipline under the last ten years. An important direction in the new security tradition is studies of security behaviour (e.g. Straub and Nance, 1990) and ethical principles that influence such behaviours (Harrington, 1996; Kesar and Rogerson, 1998)

Such directions are especially applicable in today's organizations. Many of the organizations are characterized by high professionalism and offer the employees a great deal of freedom in deciding their work tasks (Robbins and Barnwell, 2001). In such organizations employees' security behaviours are difficult to formalize by rules, procedures and regulations, and sometimes relevant rules to follow are missing (e.g. Dhillon and Backhouse, 2001). Some researchers (e.g., Von Solms, 2000) stress as well that we should use different approaches in different organisations because different organizations have different and specific needs.

Because values decide human actions, feelings and beliefs (Mumford, 1981) we believe that maintaining ISS in organizations may possibly begin with values (Dhillon and Torkzadeh, 2001, Kolkowska, 2005). We further believe that ISS objectives and ISS strategy suitable for each specific type of organization can be decided by eliciting and studying individual and organizational values. According to our beliefs there is a need for methodological framework that can support identifying organizational and individual values within organizations. VSA is such a framework.

The aim of this paper is to empirically test the Value Sensitive Approach (VSA) to ISS by applying it in a pilot study at one department at a Swedish university. The contributions of this paper are: (1) empirically verifying the usefulness of the VSA to ISS and (2) identifying and understanding the values that guide people in an academic environment.

The paper is organized in five sections. The following section describes method and realization of the pilot study. In section three, the results of the pilot study are presented in form of *university general issues* (UGV) and ISS values. After that we reflect on the study and the use of a VSA. In the last part we present the conclusions.

RESEARCH METHOD

In the study we identify individual and organizational values important in an academic environment. To identify the values we used a methodological framework, VSA. We applied VSA in a pilot study at one department at a Swedish university. During the study we even wanted to empirically verify the usefulness of the VSA to ISS.

The pilot study

"*A case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident* (Yin 1994, p. 13)". The case study research method is well-suited to my study, since the object of study is values and a value concept is ambiguous and difficult to study. Considering the nature of the research questions this study is classified as interpretive (Walsham, 1995).

An important component in case study research is a study's propositions and unit of analysis. The study's proposition directs attention to what is within the scope of the study (Yin, 1984). The scope for this study is values important in an academic environment.

The unit of analysis is related to defining what the case is all about (Yin, 1984) and what knowledge the case study leads to. The case generate knowledge about (a) general values important in an academic environment (b) values related to ISS issues important in an academic environment (c) usefulness of VSA to ISS.

The empirical work in this paper is based on a pilot study at an academic department of one of Swedish Universities. The University's organization is very unlike the centralized, formalized organizations that traditional security objectives and methods have been developed for. It is isolated, fragmentized and ambiguous and difficult to manage and formalize (Ehn 2001). Furthermore high professional employees' behaviour is difficult to formalize by rules and regulations (Ehn, 2001). Academicians' behaviours in the organization are not formalized by rules but are formed by professionalism and socialization. Socialization refers to an adaptation process by which academicians learn the values, norms and expected behaviour for the job and the organization of which they are part of (e.g. Bennet, 1998; Cahn, 1990; Carr, 2000). Consequently it is difficult to maintain ISS in such organizations by using traditional security methods and objectives. Therefore the university organization was a suitable object for the aim of this study.

Data collection – VSA in ISS

Data was collected according to Value Sensitive Approach to ISS (Kolkowska, 2005)[1]. According to the VSA to ISS the values are elicited in the following two steps:

- Identifying organizational values

Organizational values are values that individuals share with other people e. g within a group or organization (Hofstede, 1980). Organizational values come up in a social context with people that share the same experiences and are used to show a direction about what is important and how something should be (Legge, 1984). These values are visible or partially visible within an organization (Shein, 1999).

- Identifying individual values

Individual values are unique and provide a wide range of alternative behaviors in the same collective (Hofstede, 1980; Shaw, 1980). Individual values express individual feelings and attitudes and referred to what a person considers important in life Pearsall, 1998). These values are hidden and most unconscious (Shein, 1999).

According to VSA organizational values could be found by analysing documents and by interviews; individual values could be found by interviews. Different types of interviews are suggested in the approach (se later).

In the pilot study organizational values were identified by studying different important documents. We identified a number of strategic documents for the department. In the study we included university's documents like business vision, policies and guides as well as department's important documents like development plan 2005-2007 and protocols from meetings.

[1] The approach is based on ideas found in Dhillon and Torkzadeh (2001) and Friedman (2003).

Organizational values were also identified by interviewing people who is considered responsible for decision making at the university and at the department. Those people have even formal responsibilities for making decisions considering information security. We interviewed 5 people who we considered relevant in this context: university's director at the Vice Chancellors Office, chief at the Campus Affairs responsible for computer department, Information System Security manager, the headmaster of the ESI department, administrative coordinate and IT responsible for the department.

Individual values were identified by interviewing different groups of people. Members of a group share the same values and are united by a common technological frame (e.g. Orlikowski & Gash, 1994; Bijker, 1995). We attempted to achieve a representative sample of employees of the department therefore we selected persons from the different users' groups at the department. We interviewed 10 employees in this study.

Interviews

Two different methods for interviews for identifying values are proposed in the VSA: (1) values–focused thinking (Keeney, 1994) for identifying values that are held by security managers and (2) in-depth interviews using scenarios to elicit values that are held by actor groups who are less used to thinking in terms of information security issues. During the interviews we wanted to discuss general work situation and information handling (organizational issues) and ISS issues. For that reason all interviews were composed of two parts: part 1 related to organizational issues and part 2 related to ISS issues. We used no structured interviews.

Identifying values by value-focused thinking

In the beginning of the interviews we explained our goal was to understand values that people have in the organization considering both GUV and ISS issues. We explained as well what we mean with information security. We used Baskerville's (1989) definition: "IS security is protection of information resources of a firm and such protection can be through both technical means and by establishing adequate procedures, management controls, and managing the behaviour of people".

The process of eliciting values was done in two steps. In the beginning the respondent was asked to write down a wish list with all ideas and goals he/she could have in the work situation and information handling and the context of ISS. Once the list was completed, we asked the 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 (1994) suggests words, such as problems, consequences, impacts that should trigger questions to elicit more values.

Identifying values by scenarios

VSA proposes in-depth interviews with scenarios to elicit users' values. This group is not used to think in terms of information security issues and because of that we cannot use a security specific terminology during the interviews.

At the first part of the interview the informant was asked to describe tasks that he/she usually does at his/her job, the work situation, and the organization. These issues were not difficult to discuss. Employees expressed their general beliefs and work goals.

In the second part of the interview we wanted to find out values related to ISS issues. These issues are more difficult to discuss with the common user. Because of that we used scenarios as help in the communication. Scenarios were based on the work description from the first part of the interview.

Data analysis

Both identified documents and the recorded interviews were analyzed in agreement with inductive analysis according to Grounded Theory (GT) (Strauss and Corbin, 1998). The analysis began with detailed line by line analysis necessary to generate initial categories. During analysis of the collected data we paid particular attention at the areas in which values are exposed (Kluckholn, 1951):

- actions or words that express approval or disapproval.
- actions intending to achieve a certain goal or result.

The analysis resulted in a long list of statements. Then we analyzed the statements more focused by using axial coding. We identified three actor groups among the respondents: decision-makers, security managers and users. Analysis was done for each group. In the table below (Table 1) we show an example of how we worked with the analysis of interviews with decision-makers.

Statement	Concept	Value	Type of value: ISS/UGV
"I think that people here is here to do what they are suppose to do," (Interview with university's director, 2005-12-9)	Employees' trustworthiness	Trust	UGV
"I do not know anything about information security! I expect the security managers to bring up those question…they are supposed to formulate policies" (Interview with university's director, 2005-12-9)	Taking initiatives	Responsibility	UGV

Table 1. Analysis of interviews with decisions -makers

VALUE IDENTIFIED AT THE UNIVERSITY

In this section we present values identified during the study. The identified values are presented in values areas: academic freedom, trust, responsibility, privacy, development, cooperation and openness.

Academic freedom v

Academic freedom (AF) is one of the key value areas at the university. All actor groups: decision-makers, security managers and users valuated AF as very important. However different actor groups emphasized different values in this value area and interpreted the values differently. Significant values in this area are: autonomy, flexibility, creativity. At the university autonomy means that the employees (particularly teachers and researchers) have the possibility to plan their own work and their own time. They can decide and plan their work and they own the material they produce at work. The teachers and researchers appreciate this possibility very much "*it is challenging and stimulating to formulate my own tasks*", "*…the flexibility and freedom stimulate creativity in the work.*"

Different actor groups interpret the autonomy differently. Teachers and researchers do not want to have any rules or restrictions that limit the autonomy. They believe that they manage to handle the autonomy by themselves "*as long as you do your job you should not be restricted by any rules, rules limit creativity that is so important in our job."* The decision-makers would like to limit the autonomy to some extent by overall rules, goals and policies. They often express that the university is a public authority and its name can not be challenged by careless use of recourses or by violating laws and rules. Security managers believe that it is important to support the autonomy and flexibility at the university through ISS work. *"we can not limit peoples' growth by such measures, they complain directly and refer to the academic freedom."* Security managers believe that the level of autonomy depends on the information that is handled in the organization *"…broad autonomy is possible in our organization because we do not handle any secret information here…there is no any reason to limit the freedom …"* Security -managers as well as decision makers would like to slightly limit the autonomy by some overall rules and policies. The security managers emphasize importance of education and security awareness *"the only way to achieve a good security here is to educate and explain"*.

The most important ISS values within academic freedom are: clear overall rules and policies, limited control, maximal freedom and flexibility, maximal awareness.

Trust

Another important value at the university is trust. During the interviews all groups emphasized the value of trust as a precondition for autonomy. Decision makers underlined the need of trust between different professional groups. They also point out that people who works at the university is trustworthy: "*I think that people here is here to do what they are suppose to do,*" *"I cannot imagine that people who are working here would do anything illegal."* The employees want to be trusted that they can handle their autonomy of the university and that they will not risk the university's name and recourses by careless using of the autonomy. Security managers focused on trust in managing of ISS at the university "*we trust all users from the beginning, we think that they are responsible and trustworthy."* However the security managers point out that there are some examples of misuse of trust and autonomy. Often these problems can be solved by education but sometimes the users' autonomy has to be restricted. They emphasized importance of clear overall rules and policies that could guide the users and decide the level of autonomy at the university. Otherwise the users have to decide the level by themselves and it sometimes leads to misuse of the autonomy. ISS values here are maximal trust between all parties.

Responsibility

Nearly connected to autonomy and trust is value of responsibility. Decision-makers stress importance of responsibility at the university. They mean that employees are supposed to think about finding knowledge of rules, laws and ethical and moral practices at the university. Both individuals and departments are responsible for taking initiative for organizational and personal development and for formulating desires and requests to the management. In this way all people in the organisation participate in decision making and experts in different areas stimulate development of the university: *"I do not know anything about information security! I expect the security managers to bring up those question…they are supposed to formulate policies"* Unfortunately the expectations are not clearly formulated at the university. The employees mean that the organization is responsible for providing information about rules, regulations and practices while it is clear from the documents that the organization expects their employees to learn about it. Security managers point out that responsibilities do not go with authority. They took an initiative to formulate the security policy but the decision-making process is very long "*we have eventually succeeded to create an information security policy, but it has taken two years."* Thus all groups think that responsibility is an important value in the academic environment, but the responsibilities and rights should be clarified at the university. Important ISS values here are: clear employees' rights and responsibilities; taking initiative for change, formulating security requirements.

Privacy

Within the academic environment people do not want to be controlled. In this context value of privacy is important. Privacy refers to right of an individual to determine what information about himself or herself can be communicated to others. This value is most emphasized by decision-makers. They mean that *"privacy can never be violated" "employees can not be controlled or traced...it is completely unacceptable"*. Employees at the university do not want to be controlled but they understand that sometimes maintaining information security means that their privacy is violated. They think that the most important thing is to know what information is seen by the security staff and how they use it. Security managers explain that privacy is important to them as well. They would like to have possibility to trace the information to guarantee documents authenticity and to find errors in the systems. But this request gets no understanding in the organisation. Maximal privacy is an important ISS value here.

Development

Another value area that we identified at the university is development values. This value area refers to values like: improvement, renewal, personal growth, knowledge development. Development values associated to organization were emphasized in strategic documents and interviews with decision-makers, while values related to personal growth were emphasized in the interviews with users. Decisions-makers believe that it is important that employees grow in their professional role but as well in their role as administrators at the university. Employees focused their role as teachers and researchers and wanted to develop their skills in their interest areas: *"The job is my hobby; I like to be a jour…"* The consequence of this is that the employees are not interested in administrative issues or security issues. They just want to have access to the information and to the systems to be able to do their job. Security managers understand the importance of employee's´ personal growth and point out that security and IT should support the growth and not to hinder it. Because of that the important ISS value is maximal information and system availability.

Security managers experience that security issues are not prioritized at the university and that the management is not interested in these issues. Security managers point out that ISS should be considered in organizations development. They emphasized as well the necessity of including ISS thinking in development strategies and long-terms objectives.

Significant ISS values within this group are: externalized and clear management's attitude to ISS,, increased interest for ISS issues, focusing on long-terms strategy and objectives, transparent security measures and maximal information and system availability.

Cooperation

Cooperation value area includes values like: integration, standardisation, communication, trust. It is pointed out in the strategic documents that cooperation with the world around the university is desirable. All interviewed people emphasized benefits with cooperation and exchange of experiences. It was mentioned in the interviews that precondition for the effective exchange of experiences is standardisation of the solutions. Especially security managers stressed the need of standardisation and more formal cooperation between departments. Employees saw collaboration between colleagues as most important.

Relevant ISS values within cooperation values are: cooperation between departments in ISS issues, experience exchange with other universities and authorities.

Openness

One of the traditional academic values is openness. Openness means that knowledge is free and should be communicated and spread. "*Very few of the documents produced at the university are confidential and intern.*" Openness means also clear information to the employees. Values included in openness values are: information sharing, transparency of the decisions, comprehensibility, and clarity. Decision-makers particularly emphasize this value. They stress that all information at the university is open and should be shared. Because of that opinion they do not valuate ISS work as important at the university. At the same time they stress that information integrity is extremely important. It is unacceptable to share wrong information to the public.

Significant ISS values in this value area are: maximal openness of information, maximal information integrity, clearly ISS.

REFLECTIONS ABOUT VSA AND THE STUDY

One of the objectives of this paper was empirically verifying usefulness of the VSA to ISS. In this section we present lessons learned in the study.

According to VSA values are identified by using two methods for interviews: (1) value–focused thinking and (2) in-depth interviews using scenarios. The first method was supposed to be used for identifying values that are held by decision makers and security managers and the other method to elicit values that are held by actor groups who are less used to thinking in terms of information security issues (users). In the pilot study we realized that decision makers at the university are not only unfamiliar with ISS issues but even consider the issues as unimportant. We found difficult to use the value-focused thinking in interviews with this actor group. We suggest preparing both methods for each interview and use this one that is more relevant in the situation. Further we found out that techniques suggested by Keeney (1994) to help eliciting values in the value-focused thinking are also applicable in other types of interviews. We successfully used those techniques in in-depth interviews with scenarios. Another reflection is that it is useful to prepare an interview in form of semi structured questions (like discussion areas) before the interviews. This type of interview offers a good balance between the questions of interest and gathering new and unexpected insights. We found as well that it was not necessary to formulate scenarios about all tasks the employees usually do at their job. It was enough to formulate several strategic scenarios and then discuss around these. We notice that the respondents were easily familiar with the ISS area and then managed to discuss further issues. According to VSA scenarios are based on the work description from the first part of the interview. During this study it was possible to combine them both because the interviewers knew the organizations. In other situations it may be necessary to have a pause between parts one and two of the interviews.

Finding informants to the interviews and deciding on the number of people to interviews were difficult. In the study some of the informants were identified in the beginning of the study others were identified inductively under the study. In the beginning we wanted to interview information security manager and the university's director to identify organizational values. Under the study we understood that it was unclear who was responsible for the ISS issues and who has authority to make ISS decisions During the interviews we identified some more actors that might be important decision makers at the university considering ISS issues. We think that it is easier to identify different groups in the organisation and then chose informants from the different groups. The same groups should then help to structure the analysis of values. By doing this we are able to find differences and conflicts between those different groups. It is also possible to study how the different groups understand the organization and what information they consider as most important.

VSA - The next step from values to ISS objectives and strategy

The next step after identifying values is to analyze the values for the reason to find ISS objectives and ISS strategy suitable for an organization.

The result of the VSA is a number of different value areas associated with general issues in the organization and with the ISS issues. The values can then be converted into objectives. It is important to reflect about each value, try to formulate it in form of an objective. We believe that by analyzing identified values we might find out a pattern in different organizations on how the values should be prioritized.

In the case study presented in this paper we have found that the general values are the central values and influence how people work and behave in the organization. Consequently the general values decide how people want to work with ISS issues and what issues they believe are important. For example openness, academic freedom and responsibility are important value areas that influence security thinking at the university.

By using VSA we can understand what different actors consider important at work and how people want to work with ISS. It is important that the ISS strategy is in agreement with organizational and individual values.

CONCLUSIONS

The aim of this paper is empirically testing of Value Sensitive Approach (VSA) to ISS. The VSA to ISS have been applied in a pilot study at one department at a Swedish University. In the study we identified values that different actor groups have in an academic environment. Contributions of this paper are: (1) empirically verifying of usefulness of the VSA to ISS and (2) identifying and understanding of values that guide people in an academic environment.

Our conclusion is that the VSA supports the process of identifying organizational and individual values however, some modification should be done to increase the usefulness of the approach. Although some lessons learnt under this study might be unique to this study. Furthermore we believe that the approach should be further tested in other studies.

In the pilot study we identified values areas that are essential in academic environment: academic freedom, trust, responsibility, privacy, development, cooperation and openness. Within the value areas we found some values that are clearly related to ISS. We found further that the identified values areas influence how people work and behave in the organization. They even decide how people want to work with ISS issues and what issues they believe are important. For that reason the values areas should be considered when ISS strategy is decided.

There are a number different possibilities to follow-up studies: (a) values in an academic environment could be further studied (b) conflicts between values identified in the study could be further investigated (c) ISS objectives and ISS strategy could be formulated according to the identified values (d) VSA could be further verified.

REFERENCES

1. Baskerville, R. (1989) Logical controls specification: an approach to information systems security, *In Systems development for human progress*, H. K. Klein and K. Kumar (Ed.), Elsevier Science Publishers, Amsterdam, 241-255.
2. Baskerville, R. (1993) Information systems security design methods: implications for information systems development, *ACM Computing Surveys*, 25, 375-414.
3. Bennet, John B.(1998) Collegial Professionalism. The Academy, Individualism and the Commaon Good. Phoenix, Arizona:Oryx Press.
4. Bijker, W. (1995) Of Bicycles, Bakelites, and Bulbs. Toward a Theory of Sociotechnical Change. Cambridge, Mass: MIT Press
5. Cahn, S. M. (1990) Morality, Responsibility and the University, Philadelphia: Temple University Press.
6. Carr, D. (2000) Professionalism and Ethics in Teaching, London, Routledge.
7. Dhillon, G. and Backhouse, J. (2001) Current directions in IS security research: towards socio-organisational perspectives, Information Systems Journal, 11, 127-153.
8. Dhillon, G. and Backhouse, J., "Current directions in IS security research: towards socio-organisational perspectives", Information Systems Journal, 11, 127-153, 2001.
9. Dhillon, G. and Backhouse, J. (2000) Information system security management in the new millennium, Communications of the ACM, 43, 125-128.
10. Dhillon, G. and Torkzadeh, G. (2001) Value-focused assessment of information system security in organisations, Twenty-Second International Conference on Information systems.
11. Ehn B. (2001) Universitet som arbetsplats. Reflektioner kring ledarskap och kollegial professionalism, Studentlitteratur, Lund.
12. 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.
13. Harrington, S. (1996) The Effects of Ethics and Personal Denial of Responsibility on Computer Abuse Judgements and Intentions, *MIS Quarterly* 20 (3): 257-277.

14. Hofstede, G. (1980) Culture's Consequences, Sage Publications, Beverly Hills.
15. Keeney, R. L. (1994) Creativity in decision making with value-focused thinking, Sloan Management Reviev, Summer, pp 33-41.
16. Kesar, S. and Rogerson, S. (1998) Developing Ethical Practices to Minimize Computer Misuse, *Social Science Computer* Review 16 (3) 240-251.
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. Kolkowska, E. (2005) Value Sensitive Approach to Information System Security", *Accepted at AMCIS 2005*, Omaha, USA.
19. Legge, K. (1984) Evaluation planned organizational change, Academic Press, London.
20. Mumford, E. (1981) Values, Technology and Work, The Hague Martinus Nijhoff Publishers
21. Orlikowski, W. J., Gash, D. C. (1994) Technological Frames: Making Sense of Information Technology in Organizations. *ACM Transactions on Information Systems*. Vol. 12, No. 2, pp. 174-207.
22. Pearsall, J. (1998) The New Oxford Dictionary of English, Clarendon Press, Oxford.
23. Robbins, P. S. and Barnwell, N. (2002) Organisation theory. Concepts and cases, Prentice Hall, Australia.
24. Schein E., H. (1999) The corporate culture survival guide, Jossey-Bas, San Francisco.
25. Shaw, M. L. G. (1980) On becoming a personal scientist: Interactive computer elicitation of personal models of the world, Academic Press, New York.
26. 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.
27. Straub, D. and Nance, W. (1990) Discovering and Disciplining Computer Abuse in Organisations: A Field Study, *MIS Quarterly* 14 (1): 45-60.
28. Straub, D. W. and Welke, R. J. (1998) Coping with systems risks: security planning models for management decision making, MIS Quarterly, 22, 441-469.
29. Strauss, A. & Corbin, J. (1998) Basics of Qualitative Research Techniques and Procedures for Developing Grounded Theory (2 ed.). Thousand Oaks, USA, Sage Publications.
30. Von Solms, S. (2000) Information Security – the Third Wave?, *Journal of Computers & Security*, 9 615-620.
31. Walsham, G. (1995) Interpretive case studies in IS research: nature and method. *European Journal of Information Systems*. 4, 74-81.
32. Yin, R.K. (1994) Case Study Research-Design and Methods. USA, Thousand Oaks: SAGE Publications.