Analyzing Value Conflicts for a Work-Friendly ISS Policy Implementation

Ella Kolkowska, Bart Decker

Analyzing value conflicts for a work-friendly ISS policy implementation

Ella Kolkowska[1], Bart De Decker[2]

[1]Örebro University School of Business, Sweden
[2]KU Leuven, Dept. of Computer Science, IBBT-DistriNet, Belgium

ella.kolkowska@oru.se, bart.dedecker@cs.kuleuven.be

Abstract. Existing research shows that the Information Systems Security policies' (ISSPs) inability to reflect current practice is a perennial problem resulting in users' non-compliant behaviors. While the existing compliance approaches are beneficial in many ways, they do not consider the complexity of Information Systems Security (ISS) management and practice where different actors adhere to different and sometimes conflicting values. The unsolved value conflicts often lead to unworkable ISS processes and users' resistance. To address this shortcoming, this paper suggests a value conflicts analysis as a starting point for implementing work-friendly ISSPs. We show that the design and implementation of a work-friendly ISSP should involve the negotiation for different values held by the different actors within an organization.

Keywords: value conflicts, ISS compliance, policy implementation

1 Introduction

Employees' poor compliance with ISS policies is a perennial problem for many organizations [1]. Previous research points out various reasons for this problem but leading amongst them are the inability of the policy to reflect current practices [2] and users' resistance to security rules [3]. Recent literature [e.g. 4] suggests that value correspondence between ISS values and employees' values might solve the problem of lack of compliance. Hence many of the suggested approaches focus on changing users' values to align them with ISS values included in the ISSP [e.g. 5]. The consequence of this narrow end-user focus is that values included in ISSP are seldom questioned and the larger context of organizational factors influencing employees' values and behaviors is not considered in the design and implementation of ISSPs [e.g. 6, 7]. We regard the lack of sufficient consideration of the current practice in the design and implementation of ISSPs as a considerable shortcoming, especially in light of the central role that ISSPs play in managing the users' ISS behaviors.

ISSPs are often expressions of management's values and beliefs about how to manage ISS in the organization [8] while employees' behaviors are often anchored in deeply held values and beliefs often related to their profession and work practices [9, 10]. Previous research shows that tensions and value conflicts are a natural part of ISS

management [9-11]. We claim that the current limited focus on changing users' values do not consider the complexity of ISS management and practice where different groups and collaborating actors adhere to different and sometimes even conflicting values. We argue that the design and implementation of a *work-friendly ISSP* should begin with the analysis of existing value conflicts and involve a negotiation of the different values held by different actors within an organization.

The purpose of this paper is to show how value conflict analysis might be used as a starting point for implementing a work-friendly ISSP. Our findings also suggest how managers can use value conflict analysis as a starting point for finding workable ISS procedures and processes.

2 ISSP Implementation and Value Conflicts

Security policies and codes of conducts are often the main and most important tool used by managers to guide and control employees' security behaviors. However little research has explored how good ISSP are designed and implemented [12]. On the contrary, previous research shows that ISSPs are often developed and implemented through a top-down approach, using international standards, without sufficient consideration for the daily work practice [13, 14], resulting in employees' resistance and non-compliance [3].

To deal with the problem, many behavioral compliance approaches emphasize the importance of value correspondence between users' values and the values included in the ISSP. According to the literature value correspondence might be achieved by cultivating a security culture [5, 15] and setting up awareness programs [16, 17]. The focus in these approaches is on making users internalize ISS values in their daily work practices [5] and in this way achieve compliance with the implemented ISSPs [14, 15].

However, if the implemented policies cannot reflect the current practice and result in unworkable security procedures, it will be difficult to achieve value correspondence and to align users' values with implemented ISS values. When forced to choose between ISS values and work values, employees will often choose to have the work done over security. Value conflicts and prioritizations are thus a natural part of security in practice.

In the context of ISS, many different actors and values are involved [10]. These different collaborating and communicating actors such as IT-technicians, management and users may adhere to different and sometimes conflicting values in the design, implementation and use of ISSPs. For example, Kolkowska [18] found that, based on the 'academic freedom' value system, university employees use their work computers for private business even if the ISSP says that the computers are to be used for work activities only. An additional example is found in Ruidhaver et al. [7]. The authors describe how account agents share usernames and passwords though it is forbidden according to the ISSP. The account agents' day-to-day operations involve maintaining customer records and they often have to share passwords to access particular customer accounts. The agents violate the ISS policy to get their job done [7]. The previous literature also illustrates various examples of value conflicts in relation to ISS in health care [10, 11] and in relation to risk management [19].

Although the notion of value conflicts in relation to ISS has been well documented in the literature, a limited number of current studies emphasize the relationship between value conflicts and the ISSP implementation. While aspects of value conflicts in relation to compliance have been touched upon in the work of Hedstrom et al. [10], they do not explicitly focus on how the analysis of value conflicts may be used in the design and implementation of work-friendly ISSPs. Our study addresses this gap showing the opportunities of systematic value conflicts analysis to attain a work-friendly ISSP implementation and ISS processes integrated in the daily work practice.

3 Theory and Methodology

Values are considered to be motivations for all human acting i.e. values decide what action is relevant to take for a person in a certain situation [20]. According to value theory [20], the value concept is unspecific and quite challenging to study. Values are subjective and often unconscious and sometimes difficult to articulate [21]. Hence, focusing on only visible and espoused values might be misleading in understanding why people behave in certain way.

Shein's model of organizational culture [21] helps to find values that exist on different levels in an organization. The model has earlier been used in studies of ISS culture [5, 14]. We chose to use Shein's model in our study because of its ability to elicit both espoused values and basic assumptions. Such distinction is important because ISS actions such as the implementation of ISSPs as well as users' ISS behaviors might differ from the values that are espoused. Focusing exclusively on users' espoused values could be misleading because, in the context of ISS, users often espouse what they are supposed to do and not what they actually do [6]. Correspondingly, values espoused in an ISSP are high level ISS values which are then implemented in actual ISS procedures [22]. The implemented procedures might fulfill other values than those espoused in the ISSP.

Schein [21] argues that in order to understand what values impact people's behaviors, values should be studied on three levels: (1) artifacts, (2) espoused values, and (3) basic assumptions. *Artifacts* in the context of ISS are related to implemented security measures and processes [5, 14] and also to employees' security behaviors. Artifacts are related to the question '*how things are done*' in an organization. *Espoused values* relate to values and norms expressed within an organization. In relation to ISS, espoused values can be found in an ISSP [14] and they can also be expressed by people in the organization. Espoused values are related to the question '*what is important in the organization*'? *Basic assumptions* are the basic underlying beliefs and values that are often subconscious. Basic assumptions directly impact the artefact level resulting in the observable behavior of employees in their daily work activities [21]. Basic assumptions are related to '*why things in an organization are done in this specific way*'.

3.1 Case Background

The case study was carried out at one of the Swedish Municipality Social Service Divisions, which is responsible for helping vulnerable children and their families. To improve ISS in the organization, the management decided to implement a computer-based IS for all communication and exchange of information. According to this decision all actor groups working in the municipality's social services were obliged to use the implemented IS. It was argued that in this way, ISS in social services would be improved since the IS realized all the prescribed ISS rules and legal requirements. Though all actor groups had to comply with the decision, it was noticed that the care providers at treatment centers did not comply with the new rules. As a result, other actor groups could not access up-to-date information and consequently, their job performance suffered and the managers were concerned about the confidentiality of information and the privacy of the clients.

3.2 Research Methodology

The study was conducted as a qualitative case study [23]. Data was collected in two phases. In the first phase, interviews and project documents from another project [24] were reviewed to create an understanding of the context for the ISS work and to identify relevant actor groups for studying value conflicts. Sixteen group interviews with eight different stakeholder groups (including management, system owners, IT-technicians and five user groups) and five project reports were reviewed. Three stakeholder groups emerged as essential to study value conflicts in relation to the ISSP implementation and use. These were (a) managers and (b) IT-technicians who enforced the new security rules and processes through the information system and (c) care providers at the treatment centers who did not comply with these rules. We also identified *'legal security'* as an important context for ISS in social services. We found that all interviewed people stressed that ISS is important in order to achieve 'legal security'. Therefore in the second phase we looked for ISS values and work values in the context of 'legal security'.

In the second phase additional documents (policies, guidelines and work descriptions) were reviewed and in-depth interviews with the three stakeholders groups were conducted. Our data collection was guided by the three levels in Shein's model to values impacting the implementation and use of the ISSP. The semi-structured interviews were based on the following questions: 'how things are currently done to achieve legal security for the clients' as a way to identify artifacts, and 'what values are important to achieve legal security' in order to uncover the espoused values. Basic assumptions were derived from artifacts during the interviews and the analysis by asking 'why things in the organization are done in this specific way'. Each interview lasted approximately 1 to 2 hours. All interviews were recorded and transcribed.

The data was analyzed in four stages. In the *first stage*, espoused ISS values and work values were identified based on the documents and interviews. The analysis resulted in a long list of statements that were then categorized in clusters according to an inductive qualitative categorization [25]. Thereafter, clusters of values were labeled. The emerging clusters were further validated through discussions with other

researchers and representatives from the studied organization. During the *second stage*, security structures and processes as well as care providers' security behaviors (artifacts) were analyzed in order to identify basic assumptions. Basic assumptions could be discovered in the collected data, when the interviewees explained the reasons behind the behaviors and the reasons behind the implemented ISS processes. The identified basic assumptions were then categorized in the same way as espoused values (cfr. stage 1). In *stage three*, the identified espoused values and basic assumptions were analyzed in the context of 'legal security'. The analysis resulted in a conceptual model illustrating ISS values and social workers' values in the context of 'legal security' [see 26]. Once the conceptual model was created, an expert panel consisting of managers and social workers validated and discussed the categories and the relationships between these categories, which led to a few changes in the model. In the last and *fourth stage*, the value categories in the model were compared in order to find value conflicts explaining non-compliant behaviors.

4 Value Conflicts in Social Services

In this section, we present identified value conflicts and their implications on the ISSP use in practice. The analysis of value conflicts is based on artifacts, espoused values and basic assumptions identified in relation to the implementation and use of ISSP in social services. The last section suggests how managers can use value conflict analysis as a starting point for finding workable ISS procedures and processes.

4.1 ISS Values in the Context of Social Work

As mentioned earlier, 'legal security' was the value that had to be achieved in public social services in relation to ISS; thus, values were studied in this context. 'Legal security' is achieved by *secure work processes* and *good ISS*. Secure work processes are based on clarity, transparency, consistency and respect, which means for instance that the clients always know what happens and why, and that decisions are based on correct information that contains both facts and well founded logical interpretations. Good ISS means that information is available, and that the information is correct and protected against unauthorized disclosure (confidentiality) and change (integrity). It also means that it is possible to trace information and users in the system.

We found that *integrity* of the information was an unclear and confusing concept in social services. For managers and IT-technicians, integrity meant protection of information against unauthorized changes, while for care providers, integrity meant that the information was right, complete, not changed, detailed and dated. We found also that for managers and IT-technicians, *good ISS* was important to achieve 'legal security'. The two groups argued that the technical solutions implemented in the system would ensure confidentiality, integrity, availability and traceability and therefore also 'legal security for the clients'. For social workers, both *good ISS* and *secure work processes* were equally important in order to achieve 'legal security'. ISS values were a part of social workers' work values; however, the new processes enforced by the system come in conflict with the care providers' work processes

causing value conflicts. The identified value conflicts and their implications on ISS in practice are described in the following sections.

4.2 The Identified Areas of Value Conflicts

*Conflict regarding formality and informality (**vc_1**).* Care providers' work is based on spoken communication, conversations and meetings. Before the computer-based system was implemented, care providers had a close relationship with care officers regarding each child/teenager. The two groups frequently discussed the treatment by phone or e-mail. During these informal discussions, it was possible to communicate the emotional and interpretative dimension related to the treatment. After the system was implemented, the communication between the two groups was supposed to take place exclusively through the system. Care providers experienced such communication as insufficient and too formal because the emotional and interpretative dimension was difficult to communicate through the system. One care provider noted:

> *'We have lost the close relationship with the care officers and the possibility to communicate the emotional and interpretative dimension. We don't want the teenagers to be just dumped here. We want them to understand that the treatment is meaningful and based on cooperation between the different actors! We want them to feel that we really care.'*

Because of the conflict regarding the formality of the communicated information, care providers were still using the informal way of communication while the documentation in the system was done infrequently and resulted in a decreased availability and integrity. Also, it was impossible to trace the information and the treatment in the system.

*Conflict regarding what information should be communicated (**vc_2**).* The system had been designed with 'simplicity' in mind. However, care providers argued that it was important to communicate the complete picture with all the details to ensure that the decisions are made on well grounded and logical interpretations. One care provider told us:

> *'At least two care providers have to be present at a meeting with a teenager! It is very important to document all the details … not only what the teenager says, but also how he/she says it, the body language and so on. Every detail might be important for the interpretation.'*

Care providers experienced the documentation in the system as limiting because it required formal reporting (only facts), while their work was based on interpretation and observations. Thus, to ensure sufficient richness of the information, care providers still used detailed paper-based notes to communicate the information within the group and phone conversations or meetings to communicate information to other actor groups. Consequently, data was entered in the system infrequently causing the same problems as in vc_1. Information was also documented and stored in different places (both on paper and digitally) with a significant risk for loss of integrity and confidentiality.

*Conflict about responsibility for communicated information (**vc_3**).* Before the system was implemented, care providers were responsible for presenting a rich picture of the situation, while other stakeholders were responsible for choosing the relevant information and formally document it in the records. After the system was implemented, the care providers were responsible for choosing the relevant information for other actor groups and formally document that information in the IS. One of care providers explained:

> *'I cannot take responsibility for choosing information for other stakeholders. I don't know what they need. If I miss to communicate some important details, maybe a child will not get the help he/she needs!'*

Care providers were not properly informed about what information other groups needed to take the appropriate decisions to ensure proper care and treatment. Consequently, different care providers developed different routines for documentation. As a result, other actor groups experienced that some important information was missing or was too detailed. It was also unclear what the facts were and what constitute the care providers' interpretations.

*Conflict about why the information is communicated (**vc_4**).* Before the implementation of the system, written documentation (paper notes) was mainly used as a means of communication between care providers working at a treatment center. The most important goal for the documented information was to ensure proper care and treatment. After the implementation of the system, it became unclear what the main goal of the documentation was. The documentation was not seen as part of care providers' work and they did not feel that the documentation in the new form supported their work. It was rather seen as reports to other actor groups. Because of that, documentation was experienced as extra work; social workers did not feel motivated to do it and consequently, documentation in the system was done infrequently and often paper notes were used instead. These cause the same problems as described in vc_2.

*Conflict regarding how the documentation should be done (**vc_5**).* The new work processes for documentation, enforced by the system, did not correspond to the work processes the care providers were used to. The system did not support the care providers' work and even some important templates and documents were missing in the system. As a result, confidential information was exchanged via insecure portable devices and saved as Word files on local unprotected hard drivers with a significant risk for diminished integrity and confidentiality.

4.3 Reasons for Value Conflicts and Suggested Solutions

Table 1 summarizes the identified value conflict and their implications on the ISS. Based on the analysis, we suggest possible solutions for workable ISS processes. Space limitations, however, prevent us from going into full details.

Table 1. Possible solutions for workable ISS processes

Value conflicts and implications about:	**Reasons:**	**Possible solution(s):**
(vc_1) formality versus informality; *consequences*: infrequent documentation in the system, decreased availability, integrity and traceability.	*Procedures and processes are not reflecting work processes:* the new processes for documentation do not allow communication of the emotional and interpretative dimension. *Confusion* about what integrity of information means.	*Negotiation* between implementers and users to find a way of communicating the emotional and interpretative dimension through the system. *Defining* what integrity means for the different actors.
(vc_2) what information should be communicated; consequences: infrequent documentation in the system, information stored at different places, decreased confidentiality, availability, integrity and traceability.	*Procedures and processes are not reflecting work processes:* the system requires information (only facts) while rich information (both facts and interpretations) is needed in work processes. *Procedures are unknown and/or wrongly understood:* care providers at the treatment centers are not properly educated about what information other groups need to do their job correctly. *Confusion* about integrity.	*Negotiation* between implementers and users to find a way to clearly communicate both facts and interpretations through the system. *Education* focusing on what information the other groups of social workers need and also on risks related to storage of information in different places. *Defining* what integrity means for the different actors as in vc_1.
(vc_3) responsibility for the communicated information; consequences: care providers develop different routines for documentation; information is missing or is too detailed; unclear what are facts or what are interpretations; decreased availability and integrity.	*Responsibilities unclear or wrongly understood:* care providers at the treatment centers are not properly prepared for taking the new responsibilities. They are unaware of and confused about what information other groups need. *Confusion* about integrity.	*Education* focusing on explaining the meaning of the new processes and responsibilities and also what information the other groups of social workers need. *Defining* what integrity means for the different actors as in vc_1.
(vc_4) why the information is communicated consequences: documentation in the system is done infrequently; paper notes are used instead; decreased availability, confidentiality, integrity and	*Procedures and processes are not reflecting work processes:* communication through the system does not support communication between care providers at a treatment center. *Procedures are unknown*	*Negotiation* between implementers and users to find a way to better support communication between care providers at a treatment center. *Education* focusing on how

traceability.	*and/or wrongly understood:* unclear what the main goal of the documentation is.	the documentation contributes to achieve 'legal security'.
(vc_5) how the documentation should be done; consequences: confidential information is exchanged via insecure portable devices and stored on local disks; decreased integrity and confidentiality.	*Procedures and processes are not reflecting work processes:* the system does not support the care providers' work.	*Negotiation* between implementers and users to find a way to change the system so that it supports the care providers' work. *Education* focusing on risks related to the storage of information on local disks and the usage of portable devices.

5 Discussion

Based on our empirical results, we will highlight four findings.

1. It is important to consider different values and value conflicts in order to design workable ISS processes. We found in our case that care providers considered ISS values as important, but equally important were other values related to their profession as social workers. They could not comply with the implemented ISS procedures because it would mean ignoring important professional values. In our case, the implemented ISSP did not reflect the current practice and resulted in unworkable security procedures. Consequently, when forced to choose between ISS values and professional values, care providers chose their professional values. The problem highlighted in the literature is that implemented ISSPs are often based on standards without considering the unique organizational context [13, 14] and most often, ISS is treated as the most important process on top of other processes and not something that should be interwoven in the existing work practice [10]. We argue that it is a significant limitation in current ISS approaches because ISS is only a small part of the users' complex reality. Lamb at. al [27] argue that users play different roles in their work context, utilize multiple applications and interact with a variety of other people often in multiple social contexts. Hence, to create workable ISS processes, we need to understand the different values that come into play in relation to ISS and influence users' ISS behaviors. Identifying value conflicts not only helps to explain many of the tensions being experienced in the ISSP implementation and use, but also clarifies the choices that have to be made in any ISSP design or implementation. Based on our empirical findings and the discussion above we conclude that understanding and analyzing value conflicts is important in order to find workable ISS processes.

2. It is important to realize that values embedded in the ISSP may differ from values guiding the ISSP implementation. As described in the case study section, the social services organization implemented ISS values included in the ISSP as part of

the computer-based information system. The managers and IT-technicians thought that implementing these values simply meant a careful design of the computer-based system. They argued that if the integrated system was used for communication and exchange of information, it would ensure compliance with the ISSP. It was assumed that employees in social services were both aware of and aligned with ISS values included in the ISSP. It was true, however, that the implementation of these values by the computer-based system clashed with the care providers' work processes and professional values. Hence, although care providers shared the ISS values included in the ISSP, they did not comply with the new ISS processes. As a consequence, the level of ISS security in the organization was decreased.

Based on our empirical findings, we argue that it is important to realize that values embedded in ISSP may differ from values guiding the ISSP implementation. ISSPs are often formulated by top managers and include high level ISS values while the ISSP implementation is performed by IT-technicians [22]. Because of that, there is a risk for a technical focus in the ISSP implementation where the largely socio-technical and organizational context is not considered [28]. This problem also occurred in the studied organization. People responsible for the implementation of the ISSP did not realize the need for establishing new responsibility structures and new process descriptions. As a result, the new procedures and responsibilities were unknown and/or wrongly understood. The findings are based on results from one case study; however, the situation described in this paper is not limited to the specific case study. Today, many organizations implement the existing security rules in form of computer-based systems. For instance, in the health care sector computer-based systems are often implemented to improve the security for medical records. Thus, lessons learned from this case study may help other organizations to avoid security problems experienced in the studied organization.

3 Value conflict analyses may direct management's attention to new security solutions. The studied organization experienced a problem of care providers' non-compliance with the new ISS rules. This lack of compliance decreased the ISS in the organization and also exposed the organization to significant liabilities, which could potentially have an impact on the viability of the enterprise. The most popular approach suggested in the literature on ISS compliance is based on the deterrence theory and emphasizes the use of sanctions to control employees' non-compliant behaviors [29, 30]. In our case, applying this approach would mean that management enforces the new ISS processes by using sanctions. This would create an environment where the care providers would be forced to work according to unworkable ISS processes and violate their professional values or to act according to their professional values with the risk of the ISS rules being ignored. Another stream of security compliance research suggests value correspondence by making users' to internalize ISS values in their daily work practices [5, 15]. Value correspondence can be achieved by cultivating a security culture and setting up awareness programs [16, 17]. In our case, such approach would solve some of the experienced compliance problems. According to our analysis (see section 4.3) some of the new procedures and mechanisms were unknown or wrongly understood. In this case, management needs to create an understanding for the new processes and change some of the care providers' values by education and suitable awareness programs. We argue that value conflicts analysis may direct management's attention to *why* concordance between

ISS rules and ISS practice is not achieved and point at other security solutions that possibly both improve compliance and consider the current practice. The possible solutions that emerged from our analysis were: education, negotiation and definition of the main ISS concepts. We suggest education in cases where ISS procedures and responsibilities are unknown and/or wrongly understood. Our contribution in relation to the earlier awareness studies is that value conflicts analysis directs attention to specific areas that should be focused on in education and awareness programs. Further, we suggest negotiations in cases where ISS procedures and processes do not reflect work processes. Negotiation means finding the middle ground between implementers and users and in this way find better ways to achieve the same result. Lastly, we suggest defining of key ISS concepts in cases when different actors give different meanings to these concepts.

4 Negotiation involves users in the ISS design and implementation process. The view of the users' ISS compliance is formed by the longstanding technical tradition and the use of traditional technically oriented models and methods [31]. In the technical tradition, people are considered as the biggest threat and for that reason, their behaviors have to be restricted and controlled in order to achieve a high level of ISS. Users are viewed as the 'weakest link' or 'the enemy inside', and they usually have a passive role in the ISS design and implementation process [31]. Users' knowledge about the current practice, their responsibility-taking and intentional actions are not utilized in ISS management. The lack of involvement in the ISS design and implementation process is considered as a problem and often results in users' resistance to implemented ISS rules [3]. We argue that, suggested in this study, negotiation between ISS implementers and users in order to find work-friendly ISS processes is an opportunity to involve users in the ISS design and implementation process and consequently decreases their resistance to implemented ISS rules.

6 Conclusion and Future Research

In this paper we have analyzed value conflicts between ISS values and work values existing in a social services organization. In our case study, new ISS processes were approved by management and were implemented without considering the consequences on the users' daily work. The poor implementation resulted in non-compliance behaviors and a decreased level of ISS security. Based on the analysis of value conflicts that emerged in relation to the implementation and use of the ISSP, we suggest solutions that should result in more work-friendly ISS processes and an ISSP implementation that both improve compliance with ISS rules and consider the current practice.

In summary, the paper offers four key findings: 1) it is important to consider different values and value conflicts in order to find workable ISS processes; 2) it is important to realize that values embedded in the ISSP may differ from values guiding the ISSP implementation; 3) value conflict analyses can direct management's attention to new security solutions; 4) negotiation involves users in the ISS design and implementation process.

Findings presented in this paper are useful for expressing an ISS policy in an informal way. Future research needs to investigate more thoroughly how to map an

informal specification into a formal policy, part of which has to be declared by means of the underlying information system and then automatically enforced in the organization. More studies are also needed about which features of modern security enforcement systems could be appropriate in this case.

7 References

1. Ernst & Young: Moving beyond compliance, Global Information Security survey, (2008)
2. Mattia, A., Dhillon, G.: Applying Double Loop Learning to Interpret Implications for Information Systems Security Design. In: the IEEE Systems, Man & Cybernetics Conference October 5-8, Washington DC (2003)
3. Lapke, M., Dhillon, G.: Power relationships in information systems security policy formulation and implementation. In the 16th Annual European Conference on Information Systems (ECIS), Galway, Ireland (2008)
4. Mishra, S., Dhillon, G.: Information systems security governance research: a behavioral perspective. In the 1st Annual Symposium on Information Assurance, academic track of 9th annual NYS cyber security conference, New York, USA (2006)
5. Thomson, K.L.: Information Security Conscience: a precondition to an Information Security Culture. In: 8th Annual Security Conference, Las Vegas, NV, USA April 15-16 (2009)
6. Ramachandran, S., Rao, V.S., Goles, T.: Information Security Cultures of Four Professions: A Comparative Study. In Proceedings of the Forty First Hawaii International Conference on System Sciences' 2008, Big Island, Hawaii, (2008)
7. Ruighaver, A.B., Maynard, S.B., Chang, S.: Organisational security culture: Extending the end-user perspective. Computers & Security 26(1), 56—62 (2007)
8. von Solms, R., von Solms, B.: From policies to culture. Computers & Security 23(4), 275--279 (2004)
9. Albrechtsen, E., Hovden, J.: The information security digital divide between information security managers and users. Computers Security 28(6), 476--490 (2009)
10. Hedström, K., Kolkowska, E., Karlsson, F., Allan, J., P.: Value conflicts for information security management. The Journal of Strategic Information Systems 20(4), 373-384 (2011)
11. Vast, E.: Danger is in the eye of the beholders: Social representations of Information Systems security in healthcare. Journal of Strategic Information Systems 16, 130—152 (2007)
12. Baskerville, R., Siponen, M.: An information security meta-policy for emergent organizations. Logistics Information Management 15(5/6), 337—346 (2002)
13. Siponen, M., Wilson, R.: Information security management standards: Problems and solutions. Information and Management 46, 267--270 (2009)
14. Vroom, C., von Solms, R.: Towards information security behavioural compliance. Computers & Security 23(3), 191--198 (2004)
15. Thomson, K.L., von Solms, R., Louw, L.: Cultivating an organizational information security culture. Computer Fraud and Security (10), 7--11 (2006)
16. Siponen, M.: A Conceptual Foundation for Organizational Information Security Awareness. Information Management & Computer Security 8(1), 31--41 (2000)
17. Furnell, S.M., Gennatou, M., Dowland, P.S.: A prototype tool for information security awareness and training. Logistics Information Management 15(5), 352--357 (2002)
18. Kolkowska, E.: A Value Perspective on Information System Security - Exploring IS security objectives, problems and value conflicts. Orebro University, Orebro (2009)

19. Sasaki R., Hidaka, T., Moriya, M., Taniyama, H., Yajima, K., Yaegashi, Y., Kawashima Y., Yoshiura, H.: Development and applications of a multiple risk communicator. In: Sixth International Conference on RISK ANALYSIS, pp. 241--249. WIT Press (2008)
20. Mumford, E.: Values, Technology and Work. The Hague Martinus Nijhoff Publishers (1981)
21. Schein, E.: The corporate culture survival guide. Jossey-Bass Publishers, San Francisco (1999)
22. Dhillon, G.: Principles of information systems security: text and cases. Wiley Inc., Hoboken, NJ (2007)
23. Myers, M.D.: Qualitative research in business & management. Sage Publications, London, UK (2009)
24. Lagsten, J.: Utvärdera Informationssystem: Pragmatiskt perspektiv och metod, Linköping University, Linköping (2009)
25. Silverman, D.: Interpreting qualitative data. Methods for analyzing talk, text and interaction (2nd ed.). Sage, London (2001)
26. Kolkowska, E.: Lack of compliance with IS security rules: value conflicts in Social Services in Sweden. In: 8^th Annual Security Conference 15-16 April, Las Vegas, USA. (2009)
27. Lamb, R., Kling, R.: Reconceptualizing users as social actors in information systems research. MIS Quarterly 27(2), 197--235 (2003)
28. Hedström, K., Dhillon, G., Karlsson, F.: Using Actor Network Theory to Understand Information Security Management. In the 25th Annual IFIP TC 11, 20-23 September Brisbane, Australia (2010)
29. Straub, D., Nance, W.: Discovering and Disciplining Computer Abuse in Organizations: A Field Study. MIS Quarterly 14(1), 45--60 (1990)
30. Kankanhalli, A., Teo, H.H., Tan, B.C., Wei, K.K.: An Integrative Study of Information Systems Security Effectiveness. International Journal of Information Management 23(2), 139--154 (2003)
31. Siponen, M.: An analysis of the traditional IS security approaches: implications for research and practice. European Journal of Information Systems 14, 303—315 (2005)