Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2011 Proceedings

European Conference on Information Systems (ECIS)

Summer 10-6-2011

SECURITY SUBCULTURES IN AN ORGANIZATION - EXPLORING VALUE CONFLICTS

Ella Kolkowska

SECURITY SUBCULTURES IN AN ORGANIZATION - EXPLORING VALUE CONFLICTS

Kolkowska, Ella, Swedish Business School at Örebro University, Fakultetsgatan 1, 701 82 Örebro, Sweden, ella.kolkowska@oru.se

Abstract

Security culture is considered as an important factor in overcoming the problem with employees' lack of compliance with Information Security (IS) policies. Within one organization different subcultures might transcribe to different and sometimes even conflicting, values. In this paper we study such value conflicts and their implications on IS management and practice. Shein's (1999) model of organizational culture is used as a tool supporting analysis of our empirical data. We found that value conflicts exists between different security cultures within the same organization and that users anchor their values related to IS in their professional values. Thus our empirical results highlight value conflicts as an important factor to take into account when security culture is developed in an organization. Moreover, we found Shein's model as a useful tool for analysis of value conflicts between different subcultures in an organization.

Keywords: Information Security, Security culture, Value conflicts, Shein's model.

1 Introduction

The information security (IS) literature shows that a majority of security incidents are caused by trusted personnel within organizations who intentionally or unintentionally violate IS policies (Vroom and von Solms 2004; PWC 2008; Whitman and Mattord 2008). Hence, creating work environments where employees' comply with the organization's IS policies is a key issue in the management of IS today (PWC 2008). According to the literature such environments can be established by changing the organisational culture and creating an IS culture where "proper" security behaviour is a natural part of the employees' daily work activities (Leach 2003; Thomson, von Solms et al. 2006; Knapp, Marshall et al. 2007). There are two assumptions in current research of security culture. The first is that employees are able to internalize IS values in their daily work practices (Thomson 2009). Based on this assumption a majority of current studies of security cultures focus on changing employees' basic assumptions and beliefs to align them with values implemented in IS policies (Vroom and von Solms 2004; Thomson, von Solms et al. 2006). The second assumption is that an organization's security culture can be treated as a monolithic culture (Ramachandran, Rao et al. 2008). However, these assumptions may be questioned.

Firstly, various studies show that users and managers have different views and experience of IS values and practices. These differences result in a lack of understanding for the other's point of view and lead to security approaches that are poorly aligned with the users' working situation (Albrechtsen and Hovden 2009; Kolkowska 2009). Therefore it might be difficult to align employees' values with values espoused in IS policies. Secondly, researchers in organizational culture emphasize that organizational culture may vary across different groups within organizations (Jermier, Slocum et al. 1991). Analogously, the security culture of an organization may vary across different groups such as managers, IT-professionals and employees within one organization. In this paper we make a call for better understanding of different IS values and cultures coexisting within an organization. Organizational IS policies are expressions of management's values and beliefs anchored in their profession (von Solms and von Solms 2004) while employees' behaviors might be anchored in other values and beliefs. These different values might come in conflict with each other influencing IS management and practice (Kolkowska 2009). According to organizational literature, failing to pay attention to value conflicts can lead to dysfunction within the whole organization (Dhillon 2007; Vast 2007; Guzman, Stam et al. 2008). Thus, the purpose of this paper is to understand value conflicts between different subcultures in an organization and their implications on IS management and practice. Shein's (1999) model of organizational culture is used for analysis of values and value conflicts held in the different professional subcultures. This model has earlier been used successfully in various studies conceptualizing security culture (Vroom and von Solms 2004; Thomson 2009; Da Veiga and Eloff 2010).

2 Information security culture

Today, IS is viewed in a socio-organizational perspective and the literature in this field emphasizes that the behaviors of employees, their values and beliefs have to be addressed in order to protect the information assets of an organization (Siponen 2005; Mishra and Dhillon 2006; Dhillon 2007). Various scholars (Leach 2003; Thomson, von Solms et al. 2006) recognize that an organization's security culture might be an important factor in maintaining an adequate level of IS in an organization, and argue that cultivating a security culture will establish 'proper' security related behaviors into the day-to-day activities of the employees.

Security culture is defined as 'the totality of patterns of behaviour that come together to ensure protection of information resources of an organization' (Dhillon 2007 p 221). The research on security culture can, at least, be divided into two categories: studies that propose dimensions of security culture based on frameworks from management and industrial psychology, and conceptualizations of security culture to existing models of culture (e.g Shein's (1999) model).

In the first category scholars (e.g. Chia, Maynard et al. 2002; Dhillon 2007; Ruighaver, Maynard et al. 2007) have used theory-based approaches based on Detert (2000) or Hall's (1959) taxonomies to propose dimensions for security culture. The proposed dimensions are only partially similar in all the studies indicating that the understanding of security culture is still evolving.

In the second category, a number of studies use existing models of organizational culture for conceptualizations of security culture. Schein's (1999) three level model of organizational culture is widely used for this purpose within the IS field. For example, Schleinger and Teufel (2003) adopt this model and give examples of security issues for each level of the model. Based on the same model, Vroom and von Solms (2004) and Thompson (2009) suggest how the organizational culture can be transformed into a security aware culture. Furthermore, Furnell and Thomson (2009) use the model to classify users' acceptance of IT security and DaVeiga and Eloff (2010) use the model as a starting point for their framework for cultivating IS culture within an organization. The common assumption in these studies is that employees' security behaviors and values should be changed so that they comply with organizational security policies and rules.

Ruighaver and Maynard et al. (2007), as well as Ramachandran and Rao et al (2008), stress that most of the studies of security culture have limited focus on end-user beliefs and behaviors without consideration of contextual factors. They argue that in the context of IS management many different actors and values are involved. These different collaborating and communicating actors, such as IT-technicians, management and users may transcribe to different values in design, implementation and use of IS measures. Therefore, the understanding of what constitutes a working security culture might differ between different groups within one organisation.

This supposition is in line with organizational research, where various scholars argue that culture within an organization is not monolithic but consists of different subcultures (Boisnier and Chatman 2002). These subcultures are usually formed around existing divisions, departments, functional or professional groups (Trice and Beyer 1993) and they can supplement or conflict with each other (Martin and Siehl 1983). Ramachandran and Rao et al. (2008) argue that to analyze security cultures in the context of the whole organization might be misleading because there might be significant differences in security cultures across different groups. They further argue that it is important to consider different professional groups in the analysis of the security culture of an organization because employees' behaviors are strongly influenced by the cultural beliefs of the profession that they belong to (Trice and Beyer 1993; Karahanna, Evaristo et al. 2005). It has for instance been argued that IT professionals who are often responsible for security issues in an organization belong to a distinct professional culture (Vast 2007; Guzman, Stam et al. 2008).

In summary, literature in the area of security shows that a majority of research on IS culture has a limited end-user perspective. This limited focus is based on the belief that the establishment of a security culture is possible simply by changing the employees' basic assumptions and beliefs in accordance with the values implemented in IS policies. Additionally, most studies examine security culture in the context of an organization without considering the complexity of IS management in organizations where different groups and collaborating actors transcribe to different and sometimes even conflicting, values. Our study addresses this gap and focuses on value conflicts based on a belief that the implementation of a successful IS involves the negotiation of different values existing in different subcultures within one organization.

3 Theory and methodology

In this section we present the theory and methodology used in the conduct of the research.

3.1 Conceptualizing Security Culture

Value conflicts in this study are studied based on Shein's model of organisational culture (Schein 1999). The main purpose of Shein's (1999) model is to increase understanding about the values that drive peoples' behaviours in an organization. Schein (1999) suggests that studies of culture should be made on three levels: (1) artefacts, (2) espoused values, and (3) basic assumptions (see figure 1).

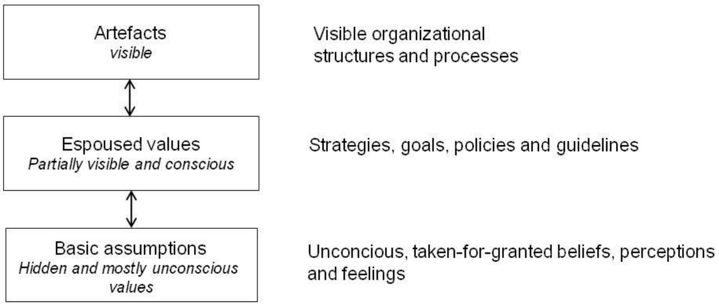
Artefacts
visible
Visible organizational structures and processes
Espoused values
Partially visible and conscious
Strategies, goals, policies and guidelines
Basic assumptions
Hidden and mostly unconscious values
Unconcious, taken-for-granted beliefs, perceptions and feelings

Figure 1. Shein's model of organizational culture (Schein 1999).

Artifacts are tangible visible behaviours, which include organisational practices and structures, i.e., what really happens in the organization (Schein 1999). In the context of IS, this level is related to implemented security measures and processes (Vroom and von Solms 2004; Thomson 2009) and also to employees' security behaviours. Artifacts are related to 'how things are done' in an organisation.

Espoused values relate to values and norms expressed within an organisation. These espoused values and norms might be formalized in different documents, but they can also exist informally. In relation to IS, espoused values can be found in IS strategy, policy, and guidelines (Vroom and von Solms 2004) and they can also be expressed by people in the organisation. Espoused values are those values that people would mention if someone asks them what they consider as important in their work. Espoused values are related to the question 'what is important in the organisation'?

Basic assumptions are the third and most hidden level of values in organizational culture. These assumptions are the basic underlying beliefs and values that are transferred to new members by the processes of socialisation. At this level, values are often unconscious. Basic assumptions directly impact the artefact level by deciding the observable behaviour of employees in their daily work activities (Schein 1999). Basic assumptions explain why people in an organization behave in a certain way. In the context of IS, basic assumptions explain the rationality behind implemented security structures and processes, as well as the rationality behind employees' security behaviours. Therefore basic assumptions are related to 'why things in an organisation are done in this specific way'. Because basic assumptions are hidden and unconscious, people can usually not express them clearly.

Schein (1999) stresses that people do not always act according to what they say; in other words, their actions do not always fulfil their espoused values. For example people can express that cooperation is important in their work, but if we study how they work we find that they usually work behind closed doors and they do not exchange experiences or information. In other words there are no structures or processes that support the value of cooperation. This means that another value (an unconscious basic assumption) drive the processes. It is important to find basic assumptions to understand why people behave in certain way. Sometimes, the visible processes fulfil the espoused values and, in these cases, the espoused values can be said to explain people's behaviours and is the same as the underlying basic assumptions, but sometimes the visible processes do not comply with espoused values and this means that other values lie behind people's behaviours. Shein's model was chosen for this study because it makes it possible to distinguish between espoused values and basic assumptions. Such distinction is emphasized as important in the domain of IS because security actions in the real world might be different from the espoused values (e.g. Vroom and von Solms 2004; Ramachandran, Rao et al. 2008).

3.2 Research method

The study was conducted as a qualitative case study (Benbasat, Goldstein et al. 1987; Myers 2009) at one of the Swedish universities. Various studies show that security threats and attacks against higher education institutions are growing (Marks 2007). At the same implementation of security measures are often more problematic in this environment than in other corporate environments (Drevin, Kruger et al. 2007).

Data was collected through both interviews and documents at two departments. The two departments, that differed considerably concerning IS management and practice were chosen in consultation with the IS manager at the university. At each department we studied two subcultures: IT-professionals, who were responsible for management of IS at the departments, and users (faculty members) who were suppose to follow the implemented security rules. Our data collection was guided by the three levels in Shein's model to identify artifacts, espoused values and basic assumptions related to IS. We conducted semi-structured interviews based on the following questions: 'how things are done here in relation to information handling' as a way to identify artifacts, and 'what is important in work with IS in order to uncover the espoused values. Basic assumptions were derived from artifacts during the analysis. Policies, guidelines and work descriptions were studied at each department. Those documents were complemented with semi-structured interviews with IT-professionals and users. Lecturers, researchers and PhD students were selected, including both long-term employees as well as new staff members in order to achieve a comprehensive group of respondents. All in all twelve users were interviewed at department one, seven at department two, and four members of IT-professionals at each department. The number of respondents was not pre-determined, but we stopped the interviews when a saturation level was achieved. Each interview took between one and two hours and was recorded. The recorded interviews were transcribed in order to facilitate the analysis and to enable the values to be supported and demonstrated through citations.

The data was analysed in four stages. Each department was analysed individually, meaning that we did not use the analysis from the first department as an input to the analysis at the second department. This was important to ensure the integrity of each case. The two departments were compared in the last stage of the analysis. In the *first stage* espoused security values for each group were identified based on the documents and interviews. The analysis resulted in a long list of statements, e.g., 'Academic freedom is very important in my job', 'sensitive data must be protected against disclosure'. The statements were then categorized in clusters dealing with a similar issue. Thereafter clusters of values were labelled. The initial clusters were refined, renamed, and reanalyzed several times. The emerging clusters were validated through discussions with other researchers during several seminars and also through two meetings with the IS manager at the university. Espoused values for each subculture were analyzed in the same way but separately. During *the second stage*, structures and processes as well as security behaviours (artefacts) at each department were analysed in order to identify basic assumptions. Some basic assumptions could be found in the collected data, when the interviewees explained the reasons behind the behaviours, however most of basic assumptions were derived by the researches from the identified structures, and processes (artifacts) using Kluckhohn's (1951) recommendation of identifying values from actions and words. According to the Kluckhohn (1951) values are exposed in: 1) actions or words that express approval or disapproval, and 2) actions intending to achieve a certain goal or result. The identified basic assumptions were then categorised in the same way as espoused values (stage 1). *In stage three*, value conflicts at each department were identified. Firstly espoused values and basic assumptions per each subculture were compared to find value conflicts (vertical comparison in Shein's model). Secondly espoused values as well as basic assumptions were compared between the two groups at each department (horizontal comparison in Shein's model). In the last and *fourth stage*, value conflicts identified at the two departments were compared in order to find similarities and differences between the two departments.

4 Value conflicts in the university's security culture

This section presents value conflicts found in the case study. The findings from the two departments are presented separately. The analysis of value conflicts are based on artifacts, espoused values and basic assumptions identified at each department.

4.1 Value conflicts identified at department 1

A number of value conflicts were identified at department one. Generally both users and IT-professionals espouse similar values in relation to IS; therefore we did not find any value conflict on this level. The conflicts were found between basic assumptions held by IT-professionals and users and also between IT-professionals' espoused values and their basic assumptions. The two categories of conflicts are presented below.

Conflict 1: different assumptions about responsibility

Both IT-professionals and users emphasized the value of responsibility as important in work with IS at the department; however their basic assumptions about this value were different. IT-professionals advocated that user need to be active and take responsibility for protecting information, finding IS information, looking for relevant rules and guidelines and so on. IT-professionals argued: 'it is a part of the culture that people look for the information by themselves', and 'as users know best what information that is sensitive at their computers they should be responsible for protecting it'. Users on the other hand considered IT-professionals responsible for protecting networks and information at the department, and also for providing users with relevant information about IS. Users also thought that it was the responsibility of the IT-professionals to increase IS awareness among users. The users stressed: 'We are responsible for giving courses and carrying out our research but management has to supply us with the necessary information about the laws and regulations we have to follow', 'IT security is the IT-department's issue. We don't know anything about security'.

Conflict 2: different assumptions about freedom

Both IT-professionals and users emphasized the value of freedom as important in work with IS at the department, but they understood this value differently. IT-professionals supported freedom in an open and free IT-environment. The users at the department had maximized rights in the networks and on the computers and they could download and install software on their computers. IT-professionals argue that such a strategy support creativity and flexibility needed in the work in an academic environment. However, IT-professionals emphasized the value of freedom in relation to using the computer at work, 'we have a lot of problems with the laptops because people use them as toys. It causes a lot of extra work for us and the computers are inefficient when there is a lot of rubbish on them.' They stressed that some private use of university's resources is allowed, but it should be restricted by ethical principles and general guidelines. Users on the other hand, seemed to believe that the freedom in using work recourses should not be limited 'The boundaries between private life and work are diffuse here. It is common that people use work resources to do private things, but it is also common to use private resources to do work. I think that the only thing we should think about is not to disturb co-workers in their work'.

Conflict 3: different assumptions about protection of information

Both users and IT-professionals stressed that it was important to protect information. Users emphasized the importance of protecting information and IT resources. They stressed that information assets should be effectively protected because information is the most important part of their job. 'I am most scared that somebody could delete or change my information…I would be upset…most of my work exists in digital form and is saved on my computer so it would be impossible to get the information from my paper notes.'

IT professionals also emphasized the importance of protecting information and resources; however we did not find any visible processes or structures how they implemented this value. IT-professionals pointed out that sensitive information handled by IT should be handled according to the same rules as sensitive information that is handled manually and the users should be aware about them. They also stressed that users are responsible for confidential information handled on their computers and in their work. 'If people know that they handle very sensitive information they should ensure the right security level, for example by cryptography. But it is not something we do generally'. It was obvious that IT-professionals at department one consider protection of information to be users' responsibility; however they did not create any prerequisites for the users to take such responsibility. We did not find any responsibility descriptions clarifying users' responsibilities, or any guidelines explaining how users can protect their computers and information. There were no courses, brochures or other means aiming to increase users' IS awareness. Consequently we did not find any efforts from the IT-professionals to help users protect information at the department.

Conflict 4: protection of information (IT-professionals espoused values and basic assumptions)

IT-professionals at department one espoused values of confidentiality and integrity, and stressed that it was important to protect information at the department. However, as described in the previous section we did not find any visible structures or processes (artifacts) supporting these values. In other words, basic assumptions lay behind structures and processes related to IS at the department. We found that basic assumptions held by IT-professionals were: that information handled at the department is not confidential and for that reason, there is very little risk of the information being a target for intentional or direct attacks. IT-professionals considered users to be capable to take care of IS issues in this environment and saw themselves as a resource in IS work, i.e., their role was to encourage users' initiatives related to IS and support users' attempts.

4.2 Value conflicts identified at department 2

We identified a number of value conflicts at department two. The conflicts were related to both espoused values and basic assumptions held by IT-professionals and users and also to IT-professionals' espoused values and their basic assumptions. First we present value conflicts between basic assumptions and espoused values held by IT-professionals and then value conflicts between IT-professionals and users.

Conflict 1: management of information security

Most of the espoused values expressed by IT-professionals at department two correspond to implemented structures and processes. However, we did not find any processes supporting the espoused values respect, dialogue, cooperation and communication. These four values were espoused by IT-professionals in relation to how management of IS should be carried out at the department. IT-professionals emphasized the importance of respect, cooperation, communication and dialogue between IT-professionals and users in deciding IS solutions. IT-professionals also emphasized that their mission is to support users in their work and that security requirements should come from the organisation. However, we found that IS at the department was managed top-down. This meant that the IT-professionals "know best" what was important to do to ensure security and they also decided the security requirements without consulting the users. This view resulted in, users sometimes being forced to change their way of working due to implemented solutions and requirements. Users were considered the greatest barriers to an effective IS and consequently, the users had to be controlled and directed. Therefore the values visible in structures and processes related to IS were control, standardization and planning.

Conflict 2: standardisation and control vs creativity and flexibility

This conflict arose because IT-professionals and users espoused and held different values in relation to standardization, control, creativity and flexibility. IT-professionals advocated control and standardization of the IT environment in the department. This meant that users' rights in the networks were minimized and IT-professionals were responsible for all installations and changes, and that networks were systematically monitored. Standardization meant that computers were similar in terms of installed hardware and software. Standardization made support easier and more effective. It was also less expensive and less time-consuming. On the other hand, users emphasized the value flexibility and creativity in their work. Flexibility means that there is the potential for different solutions; changes can be implemented quickly, depending on users' needs. It was argued that different users have different software and hardware needs related to their education and research. Creativity meant the possibility to test and try new software that could improve the quality of the work. 'In my work I have to download and test different software. It is unacceptable that we are not allowed to do it. The problem is even worse because we cannot get help from the IT personnel quickly enough'.

Conflicts 3: control vs freedom

IT-professionals stated that the environment should be controlled and for that reasons users' rights in the networks had to be limited. Users on the other hand argued that they should have more freedom in the networks so they can carry out high quality work. Still users' rights in the department's networks were limited in order achieve control over the IT environment, and consequently users did not have administrative rights on their computers and were not allowed to install software by themselves. These restrictions irritated users and reduced the quality of their work, 'because we do not have rights on the lab's computers, I had to skip the part of the lesson that needed administrative rights'.

Conflict 4: planning vs flexibility

This conflict is related to IT professionals' and users' different ideas about values of planning and flexibility. IT professional stressed that users should better plan their work and their need for support. According to the IT professionals, this would make support more effective. 'I think that they are able to plan their work! The whole organization is planned, for example the budget has to be planned, and students and courses and so on… so it should not be a problem to plan other tasks in a more detailed way either'. The users, on the other hand, emphasized the need for flexibility. They state that it is not always possible to plan the work in detail because the work is flexible, creative and constantly changing. They explain that especially in relation to research project needs could change quickly and they need IT-professionals to help them with updates, installations, and purchases and so on. The problem at the department was that unplanned requests were not prioritized and this resulted in decreased availability to information and resources for some users.

Conflict 5: technical perspective vs trust

IT-professionals believed that users should have a passive role in relation to IS and that security can be achieved by implementing technical solutions and controls. 'it is technical solutions that minimize security risks…awareness is maybe useful, but more for the reason that the users can recognize when a computer does not work properly or when something is strange…in that case they should contact us'. Moreover, IT-professionals considered users to be the greatest threat for effective IS and consequently, the users had to be controlled and directed. Users on the other hand believed that they can improve IS because of their knowledge about computers and their high IS awareness. The users consider their knowledge and experience to be sufficient to carry out some IS related and computer related tasks. They believed that they should be less controlled and more trusted in the work with IS. 'I think it is important with trust. The organization benefits a lot and people are treated with trust and respect. People have then more motivation to work and work better.' The users at the department did not feel that they were trusted, appreciated or respected for their knowledge.

Conflict 6: Different assumptions about availability

Both IT-professionals and users emphasized availability, but they had different basic assumptions regarding the scope of this value. IT professionals' efforts to ensure availability were mostly related to information and resources in the department's 'secure network', as well as the standard set of software and hardware. Structures and processes aiming to achieve availability were related to efforts made to ensure a stable and trustworthy network. The consequence of this approach was that the network was closed and information resources were available only at the university. It was a problem for users, who often needed to access information from outside the university. 'This work means an environment where people can exchange knowledge and experiences with both colleagues and students and other researchers around the world. Availability is important'

Conflicts 7: different assumptions about users' involvement in information security

This value conflict is related to different basic assumptions related to users' involvement with IS at the department. Top-down steering and the technical focus in working with IS at the department meant that decisions and security measures were implemented without dialogue with the users. Users stated that they should have the right to influence their work environment. They wanted to have an opportunity to influence the work environment by participating in decision making related to their work; for example, when an IS strategy is formulated and implemented. Users at the department felt ignored when decisions were made without their knowledge and participation. An IS strategy was implemented in the department without dialogue with the users and complaints made by users did not have any effect on the strategy and implemented security controls. This resulted in the development of a negative attitude towards implemented security controls. The users stressed: 'The implemented IS strategy is not suitable for our work and not accepted among users. It was not discussed with us, but just implemented.' 'We have collected all complaints and presented them to IT personnel, but they do not have time to change the implemented rules and/or to examine new possibilities.'

4.3 Value conflicts identified at the university – a summary

The table below (table 1) presents a summary of all value conflicts identified at the university. In the first column we see the department at which the conflict was identified. The second column describes the conflict. The third column shows what actor groups experienced the conflict (IT means IT-professionals and U means users) and the last column shows what types of values that are in conflict (BA basic assumptions resp EV espoused values).

Department	Conflict	Actors	Values
D1	C1 Different assumptions about responsibility	IT-U	BA
	C2 Different assumptions about freedom	IT-U	BA
	C3 Different assumptions about protection of information	IT-U	BA
	C4 Protection of information	IT	Between EV-BA
D2	C1 Management of information security	IT	Between EV-BA
	C2 Standardisation and control vs creativity and flexibility	IT-U	Both EV and BA
	C3 Control vs freedom	IT-U	Both EV and BA
	C4 Planning vs flexibility	IT-U	Both EV and BA
	C5 Technical perspective vs trust	IT-U	Both EV and BA
	C6 Different assumptions about availability	IT-U	BA
	C7 Different assumptions about users involvement in IS	IT-U	BA

Table 1. Value conflicts identified at the university

5 Discussion and contributions

Based on our empirical results, we will highlight four findings. We would like to point out that the first three findings presented in this section are context-specific and related to this particular case study in an academic domain, thus the findings might be different from an industry setting.

First we found that different groups emphasize different values in relation to IS. We found that employees at the university anchor their IS values in their professional values. Employees at the two departments emphasized similar values that were in agreement with professional values of their academic profession. For instance we found that university employees anchor their use of the work computer for private business in the 'academic freedom' value system. This finding is in line with other studies showing that security cultures differ between professions (Vast 2007; Guzman, Stam et al. 2008; Ramachandran, Rao et al. 2008). Based on our findings showing that professional values influence the view of IS, we argue that professional values should be considered when security culture is cultivated in an organization. On the other hand, we found that IT-professionals at the different departments held different values in relation to IS. Therefore we cannot conclude that IT-professionals at the investigated university belong to a homogenous professional group sharing similar values. This finding is inconsistent with earlier studies that show that IT-professionals belonging to the same profession share the same values even if they do not work for the same organization (Guzman, Stam et al. 2008). We think that this inconsistence depends on the type of organization we study. In an academic environment values of freedom and autonomy are emphasized as important and these values influence even IT-professionals work in this environment (Kolkowska 2006). According to the university's IS Manager, the differences between IT environments at the university - in terms of variation and decentralization, and the difference in IS strategies and goals - are due to different cultures within the departments. Hence this study found that different security subcultures exist within the very same organization. 1) We found different security subcultures at the two studied departments due to a decentralized and diversified organization where different departments have different security requirements. 2) We found also different security cultures between different groups at the same department. We therefore conclude by arguing that it is meaningful to cultivate different security cultures within the same organization even though the majority of literature on security culture argues for the development of a strong security culture at the organizational level.

Second we found value conflicts between values related to IS in between different subcultures in an organization. The consequence of the identified value conflicts was an insufficient level of IS at both departments. Two different IS management styles were found at the two departments and for that reason the value conflicts identified at the two departments differed.

IS management at department two had a technical focus. Such focus has been criticized in the IS literature and termed as 'technically skewed' for a largely socio-technical problem (Hedström, Dhillon et al. 2010). Value conflicts identified at the department were found both between the espoused values and between basic assumptions. IT-professionals' values and beliefs grounded in the technical perspective and related to how IS should be handled at the department came in conflict with users' professional values and basic assumptions. This resulted in dissatisfaction among users and also in conscious violation of IS policies and measures. In a free and uncontrolled organization such as the university there were many such possibilities. IS management at department one is in line with socio-organizational perspective (Dhillon and Backhouse 2000). We did not identify any value conflicts between espoused values. It was probably because IT-professionals at this department emphasized that IS management should support the organisational values. The users at this department were satisfied and willing to cooperate in IS issues. However, we found value conflicts between basic assumptions held by IT-professionals and users. These value conflicts led to insufficient level of security at the department and to unrealized expectations between these two groups. Based on this finding we argue that it is important to make basic assumptions visible and to highlight value conflicts between different groups. We suggest that these value conflicts can be used as a starting point for development of an IS culture that brings together expectations of different groups within an organization.

The third finding is that basic assumptions do not always support espoused values. This means that implemented security structures and processes are not in line with security values emphasized in relation to IS. We found such inconsistencies at both the studied departments. We argue that it is important that values espoused by people responsible for IS are in agreement with their basic assumptions for two reasons. First users get confused if implemented IS initiatives are not in line with IS values that are emphasized as important. Second it is important that IS managers are aware of what values guide their work with IS. It is stressed in the literature that management's values and beliefs are important in designing and implementing IS policies and rules (Hsu 2009). If managers do not understand the reasons behind an IS policy or do not fully support the rationale behind the strategy they are unlikely to engage in its development and implementation and they do not adhere to it later causing confusion among the users (Hirsch and Ezingeard 2008).

Four, we found our theoretical model based on Shein's model is useful analysis of values and value conflicts in context of security culture. The model gave us a good support in data collection and analysis. According to the literature, the study of values within an organization can be complicated by the fact that some values are hidden and unconscious (Kluckhohn 1951; Mumford 1981). Shein's model supports identification of both espoused values and unconscious values (basic assumptions). Basic assumptions are identified by focusing on behaviours and visible structures and processes (artifacts). Because the model is divided in three distinct levels it is possible to make comparisons between different cultures on these three levels. In our case study it was helpful to understand if value conflicts appeared on espoused value level or on basic assumptions level. A study which only looks at espoused values can be misleading because people do not always act according to what they say (Schein 1999). In our study we used the model for two kinds of comparisons 1) espoused values and basic assumptions within the same subculture (vertical comparison in Shein's model) and 2) espoused values as well as basic assumptions were compared between different subcultures (horizontal comparison in Shein's model). We found the model helpful in finding value conflicts in these two kinds of analysis. The limitation of the model is that it does not really support how the basic assumptions can be derived from the identified artefacts. In our study we have complement the model for this purpose with Kluckhohn's (1951) recommendation of identifying values from actions and words. Based on this recommendation in our analysis we focused on 1) actions or words that express approval or disapproval 2) actions intending to achieve a certain goal or result. We argue that Klouckholm's theory is a valuable complement to shein's model.

6 Conclusion

Users' lack of compliance with IS policies and rules is considered a major problem within this area today. According to the literature developing an organizational security culture might contribute to improvement of compliance with IS policies. This study suggests that analysis of value conflicts can be used as a starting point for development of IS culture that is aligned with organizational and professional values and brings together expectations of different stakeholders within an organization. In this article we highlighted and analysed value conflicts related to IS between users and IT professionals within an academic environment. We found that employees at the university anchor their values related to IS in their professional values and also that there are different security subcultures within the same organization.

We would like to point out that the value conflicts identified in this study are context-specific and cannot be generalized beyond the academic domain. Value conflicts found in this specific context might be different from an industry setting. Therefore the key limitation of this study is that the findings are based on one case study in an academic environment. However, the study was of explorative character and our purpose was to bring to light the importance of understanding value conflicts between different groups in creating of an information security culture. We believe that our empirical results highlight value conflicts as an important factor to take into account when security culture is cultivated in an organization.

References

Albrechtsen, E. and J. Hovden (2009). The information security digital divide between information security managers and users. Computer & Security, 28(6), 476-490.

Benbasat, I., D. K. Goldstein, et al. (1987). The case research strategy in studies of information systems. MIS Quarterly, 11(3), 369-388.

Boisnier, A. and J. A. Chatman, Eds. (2002). Cultures and Subcultures. Dynamic Organizations: The Dynamic Organization. Lawrence Erlbaum Associates, NJ.

Chia, P. A., S. B. Maynard, et al. (2002). Exploring Organisational Security Culture. Sixth Pacific Asia Conference on Information Systems, Tokyo, Japan, 2-3 September 2002

Da Veiga, A. and J. H. P. Eloff (2010). A fremework and assessment instrument for information security culture. Computer & Security, 29(2), 196-207.

Detert, J. R. (2000). A Framework for Linking Culture and Improvement Initiatives in Organizations. Academy of Management Review, 25(4), 850-863.

Dhillon, G. (2007). Principles of information systems security: text and cases Hoboken. Wiley Inc., NJ.

Dhillon, G. and J. Backhouse (2000). Information system security management in the new millennium. Communications of the ACM, 43(7), 125-128.

Drevin, L., H. A. Kruger, et al. (2007). Value-focused assessment of ICT security awareness in an academic environment. Computers & Security, 26(1), 36-43.

Furnell, S. and K.-L. Thomson (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. Computer Fraud & Security, (2), 5-10.

Guzman, I. R., K. R. Stam, et al. (2008). The Occupational Culture of IS/IT Personnel within Organizations. The Data base for Advances in Information Systems, 39(1), 33-50.

Hall, E. T. (1959). The Silent Language. Anchor Books, Garden City, NY.

Hedström, K., G. Dhillon, et al. (2010). Using Actor Network Theory to Understand Information Security Management. the 25th Annual IFIP TC 11. Brisbane, Australia, 2010, 20-23 September.

Hirsch, C. and J.-N. Ezingeard (2008). Perceptual and Cultural Aspects of Risk Management Alignment: a case study. Journal of Information System Security, 4(1), 3-20.

Hsu, C. W. (2009). Frame misalignment: interpreting the implementation of information systems security certification in an organization. European Journal of Information Systems, 18, 140-150.

Jermier, J. M., J. J. W. Slocum, et al. (1991). Organizational Subcultures in a soft Bureaucracy: Resistance Behind the Myth and Facade of an Official Culture. Organization Science, 2(2), 170-194.

Karahanna, E., J. R. Evaristo, et al. (2005). Levels of Culture and Individual Behavior: An Integrative Perspective. Journal of Global Information Management, 13(2), 1-20.

Kluckhohn, C. (1951). Values and value-orientations in the theory of action: an exploration in definition and classification. Harper & Row, New York.

Knapp, K. J., T. E. Marshall, et al. (2007). Information security: management's effect on culture and policy. Information Management & Computer Security 14(1), 24-36.

Kolkowska, E. (2006). Values for Information System Security in an academic environment - a pilot study. Published in the Proceedings of the 12th Americas Conference On Information Systems (AMCIS), Acapulco, Mexico August 4-6, 2006.

Kolkowska, E. (2009). A Value Perspective on Information System Security - Exploring IS security objectives, problems and value conflicts, Orebro University, Orebro, lic thesis.

Leach, J. (2003). Improving user security behaviour. Computers & Security, 22(8), 685-692.

Marks, A. (2007). Exploring universities' information systems security awareness in a changing higher education environment: a comparative case study research, Universities of Salford. PhD thesis.

Martin, J. and Siehl (1983). Organizational Culture and Counterculture: An Uneasy Symbiosis. Organizational Dynamics, 12(2), 52-65.

Mishra, S. and G. Dhillon (2006). Information systems security governance research: a behavioral perspective. 9th annual NYS cyber security conference, New York, USA.

Mumford, E. (1981). Values, Technology and Work, The Hague Martinus Nijhoff Publishers.

Myers, M. D. (2009). Qualitative research in business & management. Sage Publications, London, UK.

PWC (2008). Security Breaches Survey 2008. Enterprise and Regulatory Reform (BERR), PricewaterhouseCoopers on behalf of the UK Department of Business, www.pwc.co.uk.

Ramachandran, S., V. S. Rao, et al. (2008). Information Security Cultures of Four Professions: A Comparative Study. Proceedings of the Forty First Hawaii International Conference on System Sciences' 2008, Big Island, Hawaii, January 7-10.

Ruighaver, A. B., S. B. Maynard, et al. (2007). Organisational security culture: Extending the end-user perspective. Computers & Security, 26(1), 56.

Schein, E. (1999). The corporate culture survival guide. Jossey-Bass Publishers, San Francisco.

Schlienger, T. and S. Teufel (2003). Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture. 14th International Workshop on Database and Expert Systems Applications.

Siponen, M. (2005). An analysis of the traditional IS security approaches: implications for research and practice. European Journal of Information Systems, 14(3), 303-315.

Thomson, K. L. (2009). Information Security Conscience: a precondition to an Information Security Culture. 8th Annual Security Conference Las Vegas, NV, USA April 15-16.

Thomson, K. L., R. von Solms, et al. (2006). Cultivating an organizational information security culture. Computer Fraud and Security, (10), 7-11.

Trice, H. and J. M. Beyer (1993). The Culture of Work Organizations. New York, Englewood Cliffs, NJ: Prentice-Hall.

Vast, E. (2007). Danger is in the eye of the beholders: Social representations of Information Systems security in healthcare. Journal of Strategic Information Systems, 16(2), 130-152.

Whitman, M. E. and H. Mattord (2008). Principles of Information Security. Course Technology, Boston.

von Solms, R. and B. von Solms (2004). From policies to culture. Computers and Security, 23(4), 275-279.

Vroom, C. and R. von Solms (2004). Towards information security behavioural compliance. Computers and Security, 23(3), 191-198.