Value conflicts for information security management

Karin Hedström a,*, Ella Kolkowska a,1, Fredrik Karlsson a,b,1, J.P. Allen c

a Swedish Business School, Örebro University, 701 82 Örebro, Sweden
b University of Skövde, 541 28 Skövde, Sweden
c School of Business and Professional Studies, University of San Francisco, 2130 Fulton Street, MH 222, San Francisco, CA 94117-1045, USA

A R T I C L E  I N F O

Article history:
Received 18 October 2010
Received in revised form 27 June 2011
Accepted 28 June 2011
Available online 30 July 2011

Keywords:
Information systems security
Information security
Health care information systems
Values
Value conflicts
Management of information security

A B S T R A C T

A business’s information is one of its most important assets, making the protection of information a strategic issue. In this paper, we investigate the tension between information security policies and information security practice through longitudinal case studies at two health care facilities. The management of information security is traditionally informed by a control-based compliance model, which assumes that human behavior needs to be controlled and regulated. We propose a different theoretical model: the value-based compliance model, assuming that multiple forms of rationality are employed in organizational actions at one time, causing potential value conflicts. This has strong strategic implications for the management of information security. We believe health care situations can be better managed using the assumptions of a value-based compliance model.

© 2011 Elsevier B.V. All rights reserved.

1. Introduction

A business’s information is one of its most important assets. Extensive research has therefore emphasized the strategic value of information and information systems (Glazer, 1993; McFadzean et al., 2006; Nadiminti et al., 1996; VanWegen and deHoog, 1996). This together with the advance and complexity of networking technologies, which create opportunities for attacks and security breaches causing great financial losses, make information security an important strategic issue (Hu et al., 2007; Posthumus and von Solms, 2004; van Niekerk and von Solms, 2010). Indeed, the Journal of Strategic Information Systems had a special issue on security and privacy pointing at the strategic importance of information security (Dhillon et al., 2007).

While the technical parts of information security often are integrated in corporate governance, little efforts has been made to address the non-technical issues as a strategic concern (Dhillon, 2007). At the same time, previous research shows that the majority of information security breaches are caused by incidents originating inside the organization (Nash and Greenwood, 2008; Stanton et al., 2005), where internal staff are identified as the most significant threat to information security (Gaunt, 2000; Williams, 2008). The behavioral and social aspects of information security are thus seen as critical for creating secure information systems in practice (e.g., Hu et al., 2007; Siponen et al., 2008; Stanton et al., 2005).

Security policies and codes of conduct are frequently the main, or only, tool used by managers to guide and control employees’ security behaviors. The security policies and procedures of an organization embed underlying assumptions and beliefs about how to manage information security (von Solms and von Solms, 2004). In other words, security policies and regulations are expressions of values, as well as sets of instructions. Employees’ security behaviors are also expression
of values—values related to their profession. The security behavior of users is integrated in, and enacted through, the daily activities of their practice. User behavior with respect to security policies, i.e., compliance, has been recognized as an important and under-studied area for information security research (Herath and Rao, 2009; von Solms and von Solms, 2004). This research responds to this call for information security research to investigate user compliance and security practices as part of people’s everyday activities (de Paula et al., 2005). We also want to argue, based on the strategic importance of securing information assets, that the management of information security should be integrated as part of corporate governance as it is closely related to the regulatory and legal development of an organization (von Solms, 2006).

The purpose of this paper is to create new conceptual and practical tools for managing the tension between information security policies as put forward by organizations, and the daily practice of information use by its employees. Our main theoretical contribution is to offer a new value-based compliance model for information security management. We argue that the state-of-the-art in information security management is based on what we define as a control-based compliance model. The control-based compliance model relies on the enforcement of bureaucratic rules to ensure proper information security, where security is seen as the most important value enacted by users in their daily work. This control-based model views humans, and human behavior, as something to be controlled and regulated (see e.g., Bakker, 1998; Luethi and Knolmayer, 2009).

Drawing upon the value-based compliance model, we propose a new technique for mapping complex security situations in an organization. The technique maps areas of agreement or conflict between espoused theories of information security, and the theories-in-use that guide actual user behavior. Following the call for more empirical research on the implementation and use of information security policies within healthcare (de Lusignana et al., 2007), we map areas of conflict related to the goals and values underlying security practice in a hospital setting. Using data from two longitudinal case studies of information security practice in a hospital, we map the security values underlying information security policies and regulations, the health care values held by practitioners, and the areas of conflict between the two.

By showing examples of where practitioners chose not to comply with policies and regulations, thus choosing health care values over information security values, we contribute toward a new view on the management of information security. This view is based on a value-based compliance model that acknowledges, and draws upon, the different values of the information security management and the users’ work practice. The value-based compliance model, and its specific mapping techniques, can serve as the basis for professional reflection-on-action that can improve information security in ways that respect the deeply-held values of health care professionals.

1.1. Information security and values

Values, as prioritized concepts or beliefs about end states or behaviors that transcend specific situations, are a foundational concept for organizational research (e.g., Agle and Caldwell, 1999). Values have increasingly been used within information systems (IS) research (Friedman et al., 2006; Hedström, 2007) and information security research (Dhillon and Torkzadeh, 2006; Mishra and Dhillon, 2006) to understand behavior in complex situations where actors face multiple priorities and multiple choices for action. Value conflicts have also been found in studies of health information systems (HIS) use, for example in tensions between information availability and confidentiality (Mommsens, 1999).

Although users are put forward as the most important aspect to address within information security, users are commonly viewed as a ‘people problem’ (Scheiner, 2000), and not as a resource to be drawn upon in the management of information security. Seeing users as a ‘problem’ makes it necessary to develop security measures based on a control-based compliance model, where the primary managerial concerns are user control and regulation in order to enforce policy. A control-based compliance model manages information security through the use of sanctions, controls and regulation of users (e.g., Boss et al., 2009; Herath and Rao, 2009; Straub, 1990). We argue that user violations of information security policies and regulations within health care organizations are not always best managed through a control-based compliance model. We offer an alternative model – the value-based compliance model – which assumes that groups within an organization, particularly users and managers, act based on their different values (see also Vaast, 2007). If the value-based compliance model identifies value conflicts as the fundamental driver of behavioral information security problems, this implies that creating a secure information security environment in health care will require reflecting on, and re-examining, values. This redefines the information security management problem as having a significant organizational change and development component, implying that changing peoples’ daily practice is best addressed through an understanding of the values that guide their behaviors.

1.2. A value-based compliance model – information security as mediating different rationalities

Health care professionals need to have timely access to accurate patient information. At the same time, those responsible for information security have a duty to prevent unauthorized access to health care information, and to ensure the information’s integrity, and confidentiality. Balancing these demands is a major challenge for successful information use in health care (Gaunt, 2000).

Not all groups perceive information security in the same way. Previous research suggests that information security holds different meanings for different occupational communities (Vaast, 2007). This is supported by Albrechtsen and Hovdena (2009) who argue that because users and information security managers have different responsibilities, their actions are based on different rationalities. This difference in rationalities can also be seen where demands between information...
security and direct patient care come into conflict. When forced to choose between ideal information security practice and the perception of high quality health care, health care providers will arguably often choose care over security. ‘The attitude that protection of patient information is less important than direct patient care pervades planning and provision of clinical services in general’ (Gaunt, 2000).

Considering the socio-organizational nature of information security, it is important to address the values and beliefs of practitioners (Mishra and Dhillon, 2006) in order to create an organizational culture that fosters information security behaviors (von Solms and von Solms, 2004). The argument for addressing information security as a socio-organizational information security issue has gained additional support recently (Dhillon and Torkzadeh, 2006), making information security an even more complex challenge.

1.3. The value-based compliance model

The theoretical framework used in this paper is a further development of the concept of security rationale as laid out by Karlsson and Hedström (2008). The value-based compliance model (see Fig. 1) consists of a set of concepts, depicted as Unified Modeling Language classes: information security action (ISA) (prescribed and actual), actor, goal, and value. Between these classes we find a number of named associations. All types of ISAs are social actions, captured by the association between the actor and the actual ISA. An actual ISA is based on the actor’s goals and values, which are anchored in information security and the actor’s work practice. As we shall see below, the key associations to facilitate our analysis are ‘design rationale,’ ‘use rationale,’ and ‘value rationale.’ Hence, both designing and using ISAs are viewed as rational social actions (Weber, 1978), i.e., there is a reason behind peoples’ actions.

The value-based compliance model draws on Argyris’ and Schön’s (1996) theory on organizational learning and Weber’s (1978) notion of Social Action Theory. Argyris and Schön (1996) highlight that organizations’ explicit action strategies and goals, such as prescribed information security policies, rules, and guidelines, are enacted and realized through the practitioner actions. The situational and local character of knowing means that action strategies and goals are adapted to the current situation, and that the actor’s values determine which actions get priority when there are value conflicts. In terms of the framework, we distinguish between prescribed ISAs and actual ISAs. We assume that when ISAs are carried out we can identify a use rationale, i.e., the goals behind the action in-use. These goals are in turn anchored in one or several values, representing the value rationale. In contrast it is not possible to identify use or value rationales for non-rational actions. The same pattern can be applied to actors’ designs of prescribed ISAs. As we choose to view design as a goal-oriented process (Friedman, 2003) we see prescribed ISAs as rational. Hence, it is always possible to identify design and value rationale for a prescribed action. A prescribed ISA can also be viewed as ‘espoused theory’ – an ideal established by the organization’s policymakers ‘to explain or justify a given pattern of activity’ (Argyris and Schön, 1996). In contrast an actual ISA is a ‘theory-in-use’, or ‘the performance of that pattern of activity’ (Argyris and Schön, 1996).

Practitioners base their actions on different value rationalities when complying or not complying with information security guidelines. For example, Kolkowska (2009) found that university employees anchor their personal use of the work

![Fig. 1. UML representation of the value-based compliance model.](image-url)
computer in the ‘academic freedom’ value system. This meant that university employees sometimes prioritized goals, such as being able to listen to music, over adhering to the rationality behind university guidelines, which assume that computers are to be used for work activities only. Different rationalities can be drawn upon when employees reflect on their actions, and prioritize between different, and sometimes conflicting, strategies and goals.

2. Research design

The purpose of this study is to develop a new model for information security practices in an organization, and in this case demonstrate the model’s ability to identify areas of value conflict around information security and health care practice. We use a qualitative case study (Benbasat et al., 1987; Myers, 2009) in order to understand the rationalities drawn upon by health care professionals in their information security practice.

2.1. Case study description

This study was carried out at a small Swedish county hospital in central Sweden. The hospital serves approximately 90,000 citizens. Two clinics at the hospital were chosen as case studies based on their different degrees of computerization of patient information: clinic one has manual handling of medical records, while clinic two has used an electronic medical record (EMR) system for a number of years. This variety was important for providing us with rich data concerning information security in both light and heavy computerized settings, both of which are common in health care practice.

2.2. Research method

The value-based compliance model (Fig. 1), has guided our perspective as well as formed the basis for data collection and analysis. The focus during data collection has been on comparisons between prescribed ISAs and actual ISAs (i.e., compliance) at each clinic in order to identify which value conflicts and underlying rationalities that exist at that specific clinic. Prescribed ISAs restrict and guide the information security practice at each clinic (e.g., ‘Medical records should be handled and kept so that unauthorized people are unable access them’ or ‘Do not borrow passwords’). A prescribed ISA is a regulation on how to use, or not use, information. An actual ISA is the information security action staff carries out in their daily practice, i.e., electronically or manually use of, in this case, patient information.

Data was collected through interviews, observations, and documents (see Table 1). Prescribed ISAs were collected from the information security documents regulating the information security practice at each clinic (e.g., information security policy, IT strategy, routines for handling medical records). We wanted to study prescribed ISAs on the county council level as well as the hospital level and identified official documents used as the basis for management of information security. From the beginning we chose the information security policy as a document for finding prescribed ISA. The other documents were suggested during interviews with information security managers and also during interviews with health care staff. The health care staff suggested documents that were used to manage information and information security at the clinic.

The findings in the documents were complemented with interviews with three high-level information security managers. The interviews gave us deeper knowledge about the county council’s information security policies and strategies, and

<table>
<thead>
<tr>
<th>Clinics</th>
<th>Interviews</th>
<th>Observations</th>
<th>Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clinic 1</td>
<td>Licensed practicing nurses (4) Assistant nurse (1) Physician (1) Administrative staff (5)</td>
<td>Three observations for 4 h</td>
<td>Routines for handling manual medical records</td>
</tr>
<tr>
<td>Clinic 2</td>
<td>Licensed practicing nurses (4) Assistant nurse (1) Physician (1) Administrative staff (5) Counselors (2)</td>
<td>Four observations for 4 h</td>
<td>Routines for using the electronic medical record Routines for using Infomedix – an IS for communication between municipalities and the clinic</td>
</tr>
<tr>
<td>Hospital-wide</td>
<td>Information security manager IT manager Quality manager</td>
<td></td>
<td>Information security policy IT strategy Information to county council staff about information security Security instructions for county council IT users IT policy Policy for information and communication</td>
</tr>
</tbody>
</table>
questions were based on the prescribed ISAs found in the information security document. The purpose of the interviews was to identify the underlying goals and values driving management of information security, as well as rule out uncertainties regarding the prescribed ISAs. The security managers were asked to explain the prescribed ISAs, what they wanted to achieve with a specific ISA, and why they had chosen to work with that specific ISA. Each interview lasted approximately 2 h, was tape recorded, and subsequently transcribed.

We also interviewed health care staff (e.g., nurses, physicians, administrators) to collect data on how information security is carried out at the specific clinic (actual ISAs). Twenty-four semi-structured interviews, lasting between 1 and 2 h, were carried out with health care staff. The questions concerned how ISAs were enacted and carried out in practice, together with the reasons for the information security actions. The interviews were based on the analysis of the prescribed ISAs. We asked for instance ‘what passwords do you use for the systems?’, or ‘can you describe how the paper medical records are retrieved from the archive?’ The interviews were tape recorded and transcribed. The interviews were complemented by observations of the information security practice at respective clinic. We followed daily health care work at the clinics during 7 days of observations (4 h observation/day). The observations were documented by note-taking and, when appropriate, by photographs. This gave us deeper knowledge about how information security is carried out and integrated in the health care practice. During observations we focused on the same categories as during the semi-structured interviews, i.e., areas that were regulated by the prescribed ISAs. This resulted in re-interviewing and further questioning about the reasons for their actions.

We became aware of inconsistencies between the information security practice as described in the interviews and the information security practice as it was observed. For example, we observed that the staff developed routines for handling of patient information which sometimes came in conflict with information security as prescribed in the policies and routine descriptions. In these cases, we asked the staff to explain why they had developed this routine, and how it was carried out in practice.

Once the results of our preliminary analysis were written up, we used three expert panels to further validate our findings. Two of the expert panels consisted of administrative staff, physicians, and nurses from each clinic (five experts from Clinic 1, eight experts from Clinic 2), and a third expert panel consisted of four high-level managers at the county council level.

The data was analyzed in four stages, using the value-based compliance model described in Fig. 1 as an organizing framework. In the first stage, we identified prescribed and actual security actions, resulting in approximately 400 ISAs per clinic. The prescribed ISAs were based on the documents, while actual ISAs were based on observations and interviews. During the second stage, we categorized the ISAs according to type of actual or prescribed ISA as well as eliminated duplicates. The second stage resulted in approximately 140 ISAs (approximately 70 prescribed and 70 actual ISAs) per clinic. During the third stage we derived values from the reasons behind the types of prescribed and actual ISAs. The values related to actual ISAs were identified from reading through staff interview transcripts and notes from the observations at the clinics. The prescribed values were identified by reading through the interview transcripts with security managers. The values were validated during the three, abovementioned, expert panels with staff from each clinic as well as senior management and information security managers. The analysis resulted in eight different values at each clinic. The analysis ended (stage four) with comparisons between actual and prescribed ISAs at each clinic in order to identify value conflicts at that specific clinic. This meant analyzing whether a specific information security action as described in the information security steering documents was followed or not by staff working at the clinic (i.e., compliance). We matched the specific prescribed ISA, as it was written in the information security documents, with the equivalent information security action as it was carried out in practice. We have not compared data from the two clinics, since the purpose of this study was to create a new conceptual tool for managing the tension between information security policies and users’ behavior. We found in total seventeen areas of value conflicts (covering both clinics).

3. Results – value conflicts between information security and health care practice

The Section 3 illustrates a number of value conflicts based on the value-based compliance model as outlined in Fig. 1. These value conflicts show how health care staff and information security managers view information security practice differently, and how, under certain circumstances, health care professional choose to prioritize health care values over information security values.

We use graphs (Figs. 2–4) to illustrate how prescribed ISAs, developed by information security management, are conflicting with information security as it is carried out by health care staff (actual ISAs). We have chosen examples illustrating value conflicts based on the CIA-triad (confidentiality, integrity, and availability) (Harris, 2002) which is commonly used for developing information security measures. We have also included accountability, as it has been suggested as a complement to CIA (Harris, 2002; Oscarson, 2007) especially for health care organizations (Åhlfeldt, 2006). We have chosen examples that in a very clear way illustrate value conflicts between prescribed and actual ISAs. We want to stress that these are examples taken from the clinical practice for the purpose of illustrating the use and results of the model.

3.1. Protected and secure passwords

Fig. 2 illustrates how hospital staff actions conflict (a1–a3) with the prescribed rules designed to manage a secure password system. We observed how an HIS for patient registration was kept logged on at the same account, but used by different
users. This meant that health care staff did not need to log on and log off the HIS to access information (a4), making the registration procedure more efficient. In practice, the presiding nurse took care of patient registration. As a consequence, different users used the same account, which is in conflict with prescribed rules (p1 and p2). The goal of a secure password protection system is to ensure that only authorized people can access the information (g1) and make it possible to keep track of who is responsible for information in the medical record (g2). The prescribed actions related to secure passwords state that passwords are individual, and cannot be shared (p1). Passwords should immediately be changed if there is a suspicion that someone else knows the password (p2), and passwords should be constructed carefully in order to avoid passwords that are easy to guess (p3).

In their daily work, health care professionals in our case studies use many different HISs and every system has a specific password. Consequently, users have to remember many different passwords. One respondent told us that she writes the passwords on notes she keeps in her wallet (a3), and that she also creates passwords based on attributes related to her as a person (a2). This makes it easier to remember her many passwords. However, such a solution is in conflict with prescribed actions (p3). The user’s actions are conflicting with the prescribed rule because for her it is more important to have a usable password system (g4) giving her easy access to necessary information (g3). Another solution related to easy access to information (g3) is to write passwords on the wall in the consulting room (a1), making them easily accessible for all (g3). This action comes into conflict with the rules regulating the confidentiality of passwords (p1 and p2).

At the hospital, it is very important to protect sensitive patient information in order to ensure the integrity (v3) of the information, making sure that only authorized people can access the information (v1), and that there is someone responsible for the information (v2).
for the information (v2). These prescribed rules are based on values from the CIA-standard: confidentiality (v1), and integrity (v3) together with accountability (v2). For the health care staff, accessibility to information (v5) and as much time with patients as possible (v4) are important values. Because the password protection system is neither usable nor time efficient from the point of view of the users, they feel justified in developing their own information security routines. The examples illustrate how information security values, based on the rationality of information security management, come into conflict with health care values, based on the rationality of the health care practice as seen by the health care staff.

### 3.2. Updated and available patient information

Another important goal at the hospital, based on the Patient Data Act (SFS, 2008, p. 355) is to keep a medical record for each patient (g1) (see Fig. 3). This means that every important piece of patient information must be documented in the medical record (p1). Having a medical record is important for providing secure and high quality health care. In order to be able to follow the patient’s medical history (g2), a prescribed action is that ‘patient information has to be documented at once when medical staff is with the patient’ (p2). The assessment of what information to document and how soon is done by the physician, licensed practical nurses (LPNs), or counselor at the hospital. Fig. 3 below illustrates how a physician waits to...
document patient information if he decides that the information is not needed immediately (a1). A similar assessment is made by the counselor, who sometimes decides not to enter sensitive information in a patient’s medical record due to respect for the patient’s privacy (a2). The counselor explained that the patients communicate sensitive information to her in a trusted situation, while the medical records can be read by other groups of users.

The prescribed rules are based on the integrity (v1) value, i.e., that it is important with complete and updated information in the medical records, and the availability (v2) value, i.e., that it is important to have information available for authorized users at any time they need it. Both integrity and availability are part of the CIA-triad. The medical staff bases their actions on efficiency (v4) and privacy (v3) values. The physician, who describes how he wants to spare the secretaries unnecessary work, prioritizes efficiency over integrity and availability. The counselor is most of all concerned about her patient’s privacy and prioritizes this value over availability and integrity.

### 3.3. Protecting patient information

The protection of patient’s information against disclosure (g1) is mandated by Sweden’s Patient Data Act (Fig. 4). In order to protect patient’s information, it is prescribed that information concerning patient’s social, medical and other sensitive information must be carefully protected against disclosure (p2), and that '[paper-based] medical records should be handled

---

**Prescribed ISAs:**
- p1. ‘[Paper-based] medical records should be handled and kept so that unauthorized people cannot access them’
- p2. ‘Information concerning patient’s social, medical and other sensitive information must be carefully protected against disclosure’
- p3. ‘Medical journals shall be kept in a locked box or document cabin. Documents in use can be kept in a binder at the nurses’ office’

**Prescribed ISA goals:**
- g1. To protect patients information against disclose

**Prescribed ISA values:**
- v1. It is important that patient information is confidential (confidentiality)

---

**Actual ISAs:**
- a1. ‘We have new patients and new ordinations so we don’t [have time] to read all information, because of that we use paper-notes’.
- a2. In the evening, before closing, medical records for patients coming for consultation the next day are put on the desk
- a3. Lists containing information [names and social security numbers] about patients who are coming for consultation during the day are put up on the wall
- a4. ‘We put the medical records at a special place close to the fax-machine. It isn’t possible to lock this room.’

**Actual ISA goals:**
- g2. To have easy access to information
- g3. To be efficient

**Actual ISA values:**
- v2. It is important to have easy access to information (easy availability)
- v3. It is important to be efficient (efficiency)

---

**Fig. 4.** Value conflicts regarding protecting patient information.
and kept so that unauthorized people cannot access them’ (p1), and also that the ‘[paper-based] medical records must be kept in a locked box or document cabin’ (p3). However, our data analysis revealed that hospital staff does not always comply with prescribed practice. For example, we observed that medical [paper] records for patients coming for consultation the following day were put on the desk in plain view in the consulting room the evening before the consultation (a2).

We learned that by preparing medical records in this way, nurses could save time for preparing in the morning and be more efficient. For the same reason, ‘to be efficient’ (g3), the nurses use paper-notes with concise information about patients staying at the hospital (a1). The paper-notes are short versions of information registered in digital medical records. Nurses use the short versions because they do not see themselves as having time to log on and read digital medical records when they need the information. According to the nurses, using paper-notes is more time efficient. We also observed that during the day paper-based medical records were placed in unlocked locations where they could be easy accessible when the medical staff needed them (a4). Another practice for facilitating easy access to patient’s information (g2) was to use paper lists of patients coming for consultation during the day (a3). The lists, containing patients’ names and patients’ social security numbers, were in plain view on the wall in the consulting room. There was one list for each physician. Patients in the waiting room, and patients arriving for their consultations, were able to see the information on the lists.

Protecting patient information against disclosure is very important in a hospital setting. If unauthorized people can access patients’ sensitive information, their privacy can be violated. The prescribe rules related to patient information protection are based on confidentiality (v1), as found in the CIA-triad, while maximizing patient time (v3) and accessibility to information (v2) are values prioritized in daily health care practice. In the examples above, we can see how users at the hospital modify or ignore the prescribed rules in their daily work, calling upon important values such as efficiency and accessibility in order to justify their actions.

4. Discussion

In this research, we seek to move the literature on the behavioral aspects of security management beyond its rather limited role of finding new ways to ensure conformity with established rules and policies (as in e.g., Mishra and Dhillon, 2006). We argue that the predominant control-based compliance model is not likely to be successful when there are conflicts between actual and espoused security practices based on deeply-held professional values such as high quality health care, maximizing time with patients and, ironically, patient privacy. Management of information security and compliance should view users of information security measures as competent and rational actors, and see non-compliance as an action based on an underlying rationality which could form the basis for improving the information security management at the organization. Today, most efforts to establish a successful information security practice, is devoted to developing rules regulating expected use of information systems, and making the users understand how to follow the prescribed information security rules and policies.

The practice of information security would definitely improve if there was more continues feedback between information security managers and users. Success is more likely if we assume that staff is one of the best sources of security practice innovations. Information security management has to more clearly involve users in the design and implementation of information security controls. Indeed, we can envision a future where the information security management process might be seen as defective if there are not regular, systematic efforts to involve staff in the design and implementation of controls. Here it is important to identify areas of conflict between security procedures and legitimate professional work values, and involve professionals in reconciling these conflicts. An information security practice involves the entire organization, from top management and Board of Directors, to staff using the organization’s different information systems. Modern information security management has to move beyond its current role as a cost and control center on the side of the organization, and instead include information security as an integral part of corporate government, acknowledging the important strategic role of information security management (for a discussion on corporate information security governance see von Solms, 2006). Even in cases where it is necessary to enforce security policies and rules based on legal requirements, we believe that professional reflection-on-action has a vital role to play in finding specific implementations of prescribed ISAs that respect professional work values, and in more deeply engaging users in the values and rationality of information security management. A value-based approach therefore makes it easier for users to develop an understanding for the necessity of complying with information security policies. The information security management will also have better knowledge about the users’ values, which will improve their competence in relating and designing the prescribed ISAs aligned with users’ rationality.

Information security management is often built on a top-down-approach, where information security managers develop security measures (i.e., administrative routines or technical controls) based on international standards such as ISO 27000-series (ISO/IEC, 2005), without sufficient consideration for the daily work practice. As we have shown, in a highly time-competitive practice where staff (i.e., physicians, LPNs, etc.) holds strong professional values, such as health care, this creates an environment where information security measures are at the risk of being ignored, or that staff creates their own, not always safe, procedures for dealing with the demands of the daily work practice. The control-based compliance model builds on a view on humans as needing restrictions or controls (e.g., Boss et al., 2009; Herath and Rao, 2009), and would see this lack of compliance as user ignorance or misconduct. The solution would thus be to implement more specific rules or educate users through information security education. The value-based compliance model, would instead, see users’ non-compliance as rational actions, based on reflection-in-action (Schön, 1991), explaining the ‘gap’ with a lack of understanding of the multiple
Our research has not only practical implications, but also implications for research and how we as researchers address and understand the practice of information security. A better understanding of the rationality of users' actions would be helpful in designing and implementing different security controls. Successful compliance research needs to move from the current and rather limited focus on expected use and misuse of information systems, to a focus on actual use and misuse. The idea that it is enough to address expected use, without addressing actual use, is an obstruction in the design and implementation of information security controls. If we, as researchers, assume that knowledge about compliance and non-compliance can be developed exclusively from asking managers and users about expected use or misuse of information systems, we will forever stay in the dark. These accounts about compliance have to be complemented and contrasted with studies of actual use, as the possibility to describe actual use is limited due to the difficulty to remember every detail of one's actions, as well as influenced by the user's idea of how things should be done. This way of viewing knowledge, where the study of the meaning of language and actions is in focus, has methodological implications. Research on compliance, with this...
view, needs to rely on multiple data sources, where observations of actions are analyzed in interplay with documentations and interviews. This means that we advocate an interpretative approach where we also can reveal underlying interests and values, as we believe that it is important to understand the reasons for actions, if we want to develop a contribute to change, and the development of a successful information security practice.

5. Limitations and future research

We believe that a value-based compliance model has the potential to offer a way to a better information security practice. But so far we can only determine that it has been useful for identifying and understanding value conflicts. We have not studied how organizations can develop their information security practice, through a value-based approach, which is a limitation of our study. The extensive literature on ‘reflection-on-action’ has shown the potential benefits of having professionals learn and improve by confronting conflicts between values and actions. It can also be a challenging and time-consuming path, calling upon managerial skills that might not be explicitly developed or rewarded in the information security profession. Our proposed value-based approach for management of information security takes a different perspective on user and user compliance than the prevalent control-based compliance model (e.g., Boss et al., 2009; Herath and Rao, 2009; Straub, 1990). This tradition to manage information security with sanctions and controls, rather than working with peoples’ values, could be a challenge when accepting a managerial model building on a more value-based approach, as it is difficult to change an organization’s corporate culture and view on management.

Other limitations concern the use of the model – which has been evaluated in one organization. This model was further developed in a Swedish context, and although we believe that the model as such is possible to transfer to other national settings, the use and results of the model, will of course depend on the specific culturally context where it is used. Consequently, this compliance model opens up future research opportunities. First we would like to further evaluate the value-based compliance model as a vehicle for the management of information security. This would suggest using the model to develop an information security practice within a healthcare organization, in order to assess its usefulness for the management of information security. Second, we want to compare the results from this health care study with analysis of value conflicts in other types of health care organizations. This would not only give us interesting results concerning the use of the model, but also comparative results concerning types of value conflicts, which would be of interest for developing our understanding of the different rationalities of information security practice within health care. Another interesting way forward, is of course, to do a comparative study within another type of organization. This would give as the opportunity to evaluate the usefulness of the model outside a health care organization. For future research it would also be interesting to use this model for analysis of information security practices in other countries. Another limitation concerning the use of the model is intentional and malicious information security behavior (see e.g., Stanton et al., 2005), which we did not find any evidence of at the clinics. This does not mean, however, that this type of behavior does not exist; only that we did not uncover any ISAs that were carried out with the intention to harm. The value-based model (see Fig. 1) supports the disclosure of different types of rationalities, meaning that also harmful intentions can be covered.

6. Conclusion and strategic implications

The view underlying the control-based compliance model, of users as needing sanctions, control and regulations, has a long tradition within information security practice and research. We offer another perspective (see Fig. 1) of management of information security, taking managers and employees’ different rationalities as a starting point for information security management and compliance. The value-based compliance model acknowledge the inherent nature of value conflicts in complex organizational work, where multiple forms of rationality are employed in organizational actions at any one time. This changed view of management of information security and compliance has strong strategic implications for research as well as practice. For practice this means that management of information security should not only focus compliance with standards, but view information security as contextual and see users as resources instead of as problems. It also means viewing information security as a strategic issue that should be integrated with corporate management. For research it means developing and evaluating models, processes, and tools supporting a value-based perspective on the management of information security. Knowledge about compliance, is with this perspective, developed through the study of the meaning of what people say and what they do, e.g., the interplay between language and action. This means that the methodologies we use should support multiply data sources where observations of actual use are an important part of the empirical material. It also means that the theories we use needs to help us reveal the rationality behind what people say and do. An understanding of the interests and values influencing the practice of information security is an important piece of knowledge for development and use of secure information systems.

Acknowledgments

Sincere thanks to the Swedish Civil Contingency Agency for financial support for researching and writing this article. And many thanks to the staff at the hospital who so kindly let us to share their work practice. We also want to extend our thanks to the reviewer and editor, who, with encouraging and insightful comments helped us develop our thoughts further.
References


