Social action theory for understanding information security non-compliance in hospitals

The importance of user rationale

Karin Hedström, Fredrik Karlsson and Ella Kolkowska
School of Business, Örebro University, Örebro, Sweden

Abstract

Purpose – Employees’ compliance with information security policies is considered an essential component of information security management. The research aims to illustrate the usefulness of social action theory (SAT) for management of information security.

Design/methodology/approach – This research was carried out as a longitudinal case study at a Swedish hospital. Data were collected using a combination of interviews, information security documents, and observations. Data were analysed using a combination of a value-based compliance model and the taxonomy laid out in SAT to determine user rationality.

Findings – The paper argues that management of information security and design of countermeasures should be based on an understanding of users’ rationale covering both intentional and unintentional non-compliance. The findings are presented in propositions with practical and theoretical implications: P1. Employees’ non-compliance is predominantly based on means-end calculations and based on a practical rationality, P2. An information security investigation of employees’ rationality should not be based on an a priori assumption about user intent, P3. Information security management and choice of countermeasures should be based on an understanding of the use rationale, and P4. Countermeasures should target intentional as well as unintentional non-compliance.

Originality/value – This work is an extension of Hedström et al. arguing for the importance of addressing user rationale for successful management of information security. The presented propositions can form a basis for information security management, making the objectives underlying the study presented in Hedström et al. more clear.

Keywords Compliance, Information security, Social action theory, User behaviour, User rationale

1. Introduction

Information and information systems are key assets for organizations of every size. Information security breaches may cause damage that leads not only to economic losses, but also can have a negative effect on reputation, goodwill, and trust (Hoffer and Straub, 1989). Thus, information security has become a strategic issue that needs to be addressed at a corporate level (Von Solms, 2006). This view is also supported by a global state information security survey, which revealed that customer requirements have increasingly become an important factor for justifying information security.
Socio-technical analysis of information security

Expenditure PricewaterhouseCoopers (PwC, 2010, 2011). Customer requirements progressed from being factor six (out of seven) in 2007 to being the second most important factor (out of seven) in 2010. The authors of the survey concluded that “information security practices continue to take on a far more customer-facing, business-supporting, strategic value-building role” (PwC, 2011).

Sensitive and confidential information such as personal health information can, if disclosed, cause real damage to a person. The integrity and availability of such information contributes to high quality care. This makes the protection of information an important issue in health care. Indeed, it has been shown that insider security threats are much more common than security breaches caused by someone from the outside. A report by Kroll Advisory Solutions (2012) showed that 79 per cent of the security breaches at US hospitals that relate to patient data are caused by employees, with unauthorised employee access being the most common security breach.

The management of information security includes a whole range of countermeasures for information systems security and the prevention of information systems misuse (Baker and Wallace, 2007). These countermeasures are often described as technical, operational, and managerial controls (Stoneburner et al., 2002). These methods of controlling information security depend on how a potential security breach is perceived and explained. The search to find theories and frameworks for analysing non-compliance behaviour has been on the research agenda for quite some time (Herath and Rao, 2009b; Kankanhalli et al., 2003; Straub, 1990). Most of the cumulative research on information security has been technically oriented, putting forward improved technical countermeasures such as improved password protection systems, data encryption, network firewalls, and other artefacts that are aimed at protecting information resources. Among them are such countermeasures as the authentication framework proposed by Al-Muhtadi et al. (2002), and the system suggested by Myles et al. (2003), which helps users to protect information about their location in order to preserve their privacy. Information security researchers who are socially oriented tend to lean on organizational and social theories, such as deterrence theory (Lee et al., 2004) or theory of planned based behaviour (Bulgurcu et al., 2010), in order to explain non-compliance and suggest countermeasures. Such countermeasures include the IT Baseline Protection Manual and the Generally Accepted Information Security Principles (Information Systems Security Association, 2003), socio-organizational information security management systems (Harnesk and Lindström, 2011), or different types of information security awareness-raising programmes (Albrechtsen and Hovden, 2010). As can be seen from the above, information security management is, by its very nature, socio-technical (Hedström et al., 2010): the social and the technical are entangled in different administrative and tool-based forms of protection. Consequently, it is necessary to adopt a socio-technical mix of countermeasures.

Considering the socio-technical nature of information security, and the fact that actions are carried out in a social and organizational context, we propose that information security actions should be addressed as social actions, i.e. actions that are meaningful for the individual, and which relate to and are influenced by the actions of others (Weber, 1978). From this perspective, information security management should strive to understand employees’ underlying reasons for following or not following information security policies, as well as using or not using a technical solution in the way intended. This means that information security management, together with the
selection of countermeasures, should be based on an understanding of the rationality of the user. Our argument is based on an existing longitudinal case study of information security practice carried out at a Swedish hospital in which we examined users’ compliance with information security policies and guidelines (Hedström et al., 2011). In this study, we presented a value-based compliance (VBC) model for analysing value conflicts in information security. However, this study did not explain in sufficient detail the impact of such a perspective, where information security management is based on the mental process that underlies the users’ information security behaviour (Weber, 1978). In particular, it did not offer a detailed explanation of how knowledge about value-conflicts can be used as a basis for the development of a secure information environment. The purpose of this present paper is thus to illustrate the usefulness of social action theory (SAT) (Weber, 1978) as a basis for information security management within a health care setting. Furthermore, it suggests how SAT can be used to design or redesign a good mix of countermeasures for existing information security practice in health care. The result is presented as four theoretical and practical propositions based on the empirical data. To the best of our knowledge, this is one of the earliest studies to address the selection of countermeasures from a SAT perspective. We believe that it is possible to create greater information system security by basing information security management on an understanding of the mental process that underlies users’ security behaviours rather than by exclusively targeting overt behaviour (cf. with the concept of security culture (Von Solms and Von Solms, 2004; Guenther, 2004).

The paper is structured as follows. In the following section, we review earlier research on non-compliance and the misuse of information systems. The subsequent sections describe first SAT and then the research method used. Next, we describe our analysis and exemplify our use of SAT for understanding user non-compliance. We then go on to discuss the impact of a SAT analysis on the selection of countermeasures, present our propositions, and address the limitations of our study. Finally, this paper offers a short conclusion.

2. Employee non-compliance and information systems misuse
Non-compliance with information security policies and misuse of information systems are closely related. Policies, guidelines and security awareness-raising programmes rely on the users’ willingness and ability to follow them; non-compliance means that users deliberately or accidentally fail to follow these guidelines and rules. This often leads to information systems misuse, which may cause serious security breaches. Employees’ misuse of information systems is often defined as “unauthorized, deliberate, and internally recognizable misuse of assets of the local organizational information system” (Straub, 1990). The same one-sided focus on intentional actions can be found in existing research on the effectiveness of countermeasures. D’Arcy and Hovav (2007), for instance, carried out a quantitative study to investigate the effectiveness of security policies, the SETA program, and computer monitoring for five different scenarios of information systems misuse (inappropriate e-mail, password sharing, software piracy, unauthorized access, and unauthorized modification). Their study was based on general deterrence theory, which argues that users’ misbehaviour is intentional, based on users’ judgement as to whether or not the risk of sanctions when engaging in computer abuse is worth the gain: “It posits that individuals with an
instrumental intent to commit antisocial acts can be dissuaded by the administration of strong disincentives and sanctions relevant to these acts” (Straub and Welke, 1998).

Studies that seek to explain users’ misuse of information systems or non-compliance have relied heavily on deterrence theory (Straub, 1990; Kankanhalli et al., 2003; Lee et al., 2004; D’Arcy et al., 2009), although its capacity to explain such behaviours is open to debate. These studies focus on the severity, certainty and celerity of sanctions for achieving high information security. For example, Kankanhalli et al. (2003) found that deterrent severity did not have a strong impact on the effectiveness of information security. On the other hand, D’Arcy et al. (2009) found that employees’ misuse of information systems was only influenced by the perceived severity of sanctions; their perceived certainty was not found to be important. Other common approaches used to explain users’ non-compliance with information security polices are neutralization theory (Siponen and Vance, 2010), theory of planned behaviour (Bulgurcu et al., 2010), agency theory (Herath and Rao, 2009a) and protection motivation theory (Herath and Rao, 2009b; Pahnila et al., 2007). Myyry et al. (2009) suggested a combination of cognitive moral development theory and the theory of motivational types of values. However, these approaches are limited because of their focus on deliberate actions and the countermeasures used to address such actions. Hedström et al. (2011) put forward the VBC model, which takes into consideration both deliberate and accidental information security actions. The framework draws on SAT as well as theory on organizational learning (Argyris and Schön, 1996; Schön, 1991). However, Hedström et al. (2011) did not use SAT to its full potential. They concluded that employees’ information security actions are anchored in goals and values, which are important to understand when it comes to non-compliance. However, they did not differentiate between different types of social actions, the mental process and the type of rationale behind these actions, and how these aspects affect the choice of countermeasures.

In accordance with Magklaras and Furnell (2002), we believe it is necessary to include accidental actions when analysing information systems misuse. It is, for instance, estimated that about half of all security breaches are accidental (Vroom and Von Solms, 2004). This illustrates that the behaviour which causes security breaches is both intentional and unintentional. It is important to acknowledge and work with accidental misuse as well as intentional misuse, as it is impossible for management to foresee in advance all incidents that can occur within an organization (Thomson and Nierkerk, 2012). Misuse should be seen as an unauthorized use of the organization’s information systems, which can be caused by intentional or accidental non-compliance with security policies and regulations. Intentional misuse can include, for instance, data theft or purposeful access to sensitive data, while accidental or unintentional misuse might include users who involuntarily send an e-mail with sensitive content to the wrong person or accidentally install computer software with malware content. Magklaras and Furnell (2002) classified insiders’ accidental misuse as an effect of inadequate systems knowledge. Intentional misuse by insiders can also be the result of stress or a genuine lack of knowledge of the rules: examples include data theft, personal differences and deliberate ignorance of the rules. In another study, Magklaras and Furnell (2004) reported that the most common misuse by legitimate users is the storage and dissemination of pornographic material. The second most common misuse is theft or alteration of commercially sensitive information; this was reported in
24 per cent of the cases, whilst e-mail abuse accounted for 16 per cent of the cases. The authors based their results on a survey of 50 IT professionals across Europe. A recent study on non-compliance with The Health Insurance Portability and Accountability Act (HIPAA) showed that the work environment and organizational limitations are important factors for users’ non-compliance (Liginlal et al., 2012).

3. Information system security as social actions

Since security countermeasures represent knowledge of good security practice they also represent rationale. Regardless of the grounds, the design and use of countermeasures is often rational from the actor’s point of view. The design is based on the creator’s design rationale, while the use is based on the user’s use rationale. Both these concepts can be approached through Weber’s (1978) theory of social action (SAT). He suggested that four types of social actions exist: traditional, affectual, value oriented, and instrumental, as shown in Table I. Traditional actions are determined by deeply rooted habits, while affectual actions are determined by the actor’s feelings or emotions. Value-oriented actions are undertaken for reasons that are intrinsic to the actor, such as ethics. Finally, instrumental actions involve consideration of the behaviour of other human beings and objects, and the relative importance of different ends. Hence, there is no objective meaning of optimal means and ends; we have to take into account the value base upon which we make the judgement.

According to Weber (1978), two of the four types of social actions are anchored in rationality: value-oriented and instrumental actions. Here, the action involves a mental process where the actor bases the action on conscious and clearly formulated goals and/or values, and uses, to his or her knowledge, the best means available to attain these goals and/or values. Consequently, rational social actions are meaningful for the actor. Traditional and affectual actions are, however, non-rational social actions; thus, they do not involve mental processes when carried out. Traditional actions are “automatic” and are based on deeply rooted habits, where the actor does not reflect on or even remember why the action is carried out. Affective actions are a direct consequence of the actor’s emotional condition; for example, a person may act in a certain way when feeling intimidated by an alarm.

Value-oriented and instrumental actions can be associated with Weber’s types of rationality, whereby mental processes can be categorized as: practical, theoretical, substantive, or formal (Kalberg, 1980). Individuals use the first type of rationality, practical rationality, to carry out their daily routines and tasks. Hence, instead of basing actions on an absolute value system, individuals accept given realities and

<table>
<thead>
<tr>
<th>Social actions</th>
<th>Mental process</th>
<th>Types of rationality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional</td>
<td>Nonrational</td>
<td>–</td>
</tr>
<tr>
<td>Affectual</td>
<td>Nonrational</td>
<td>–</td>
</tr>
<tr>
<td>Value oriented</td>
<td>Decisions are anchored in a context</td>
<td>Substantive</td>
</tr>
<tr>
<td></td>
<td>dependent value system</td>
<td></td>
</tr>
<tr>
<td>Instrumental</td>
<td>Means-end calculation</td>
<td>Practical, formal</td>
</tr>
<tr>
<td></td>
<td>Use of conceptual models</td>
<td>Theoretical</td>
</tr>
</tbody>
</table>

Table I.
The relationship between Weber’s (1978) social actions, mental processes and rationality types
choose a preconceived means to achieving a particular end. According to Weber (1978), practical rationality is anchored in the mental process of means-end calculation; one such example is an employee who uses the same password to access several information systems. This illustrates the employee’s use rationale, which is based on a means-end calculation to ease the burden of remembering passwords. Of course, this rationale may or may not differ from the design rationale of the security manager who implemented password protection. The second type of rationality, theoretical rationality, is used by individuals to master reality through conceptual models “rather than through actions” (Kalberg, 1980). Hence, this type of rationality is based on the mental process of logical deduction and is not directly associated with social actions. However, constructed models or theories have the potential to indirectly shape patterns of actions: for example, deterrence theory (Lee et al., 2004) can serve as a framework when designing a security mechanism, such as an information security policy. Based on this theory, security managers should include punishment in policy design in order to deter people from violating security policy. Substantive rationality is the third of Weber’s (1978) rationality types. This rationality type is similar to practical rationality in that it directly affects actions and involves a mental process. However, instead of accepting given realities and choosing from preconceived means, these decisions are anchored in specific value systems that vary “in comprehensiveness, internal consistency and content” (Kalberg, 1980). One example of such a value system is that of “scientific freedom”. University employees may, for example, anchor their “right” to freely install software on their computers in these values. This type of rationality may organize some part of life, and an actor can change value systems depending on context. Thus, these actions are important to the actors themselves, irrespective of the consequences (Weber, 1978). Finally, formal rationality is often associated with organizations, such as bureaucracies. In the same way as practical rationality, it directly orders actions into patterns by using the mental process of means-end calculations. In this case, the calculations are anchored in universal rules, laws or regulations. Hence, the resulting actions are made without reference to people. One example of formal rationality in security mechanisms and health care is the implementation of the Swedish Personal Data Act (Ministry of Justice, 2008). The aim of this law is “to prevent the violation of personal integrity in the processing of personal data”.

4. Research method
We carried out a longitudinal case study (Yin, 1994) between 2008 and 2010 at a regional Swedish hospital to illustrate the rationale and mental processes behind employees’ non-compliance with information security polices. The hospital employs about 750 people, has 142 places of treatment and serves around 90,000 citizens. The degree of computerization varies within the hospital; some clinics use electronic medical records (EMR), whilst others do not. Two clinics at the hospital were chosen as cases based on their different degrees of computerization of patient information: one clinic uses manual handling of medical records, whilst the other has used an 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.
4.1 Data collection

Qualitative data was collected from the information security documents that regulate information security practice at each clinic (e.g. information security policy, IT strategy, routines for handling medical records), as well as information security documents found at a county council level (Table II). The findings in these documents were complemented with interviews with three high-level information security managers. The interviews gave us a more in-depth knowledge of the county council’s information security policies and strategies. In other words, they provided us with insights into the designers’ rationale. Each interview lasted approximately two hours, and 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 each of the clinics. 24 semi-structured interviews were carried out with health care staff. Each interview lasted between one and two hours. The questions asked during the interviews related to how information security was enacted and carried out in practice, together with the reasons for information security actions. This empirical data gave us a sense of the employees’ use rationale. The interviews were based on an analysis of the rules of information security found in the documents and voiced by the security managers; together, these constituted an initial interview guide (Patton, 1990). Examples of questions include: “What kinds of passwords do you use for the systems?”, “How do you remember the passwords?”, and “Can you describe how the paper medical records are retrieved from the archive?”. The interviews were tape recorded and transcribed. In addition to the interviews, observations of information security practice were carried out at the respective clinics over a period of 28 h. We also observed daily health care work at the clinics over a period of seven days (at a rate of four hours of observation per day). Note-taking was used as the method of recording these observations, and photographs were taken, when appropriate. This gave us a more in-depth knowledge of the way in which information security is carried out and integrated

<table>
<thead>
<tr>
<th>Type of data collection</th>
<th>Interviews</th>
<th>Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clinic 1</td>
<td>Licensed practicing nurses (four), assistant nurse (one), physician (one), administrative staff (five)</td>
<td>Three observations, each lasting four hours (12 h of observation in total)</td>
</tr>
<tr>
<td>Clinic 2</td>
<td>Licensed practicing nurses (four), assistant nurse (one), physician (one), administrative staff (five), counselors (two)</td>
<td>Four observations, each lasting four hours (16 h of observation in total)</td>
</tr>
<tr>
<td>Hospital-wide</td>
<td>Information security manager (one), IT manager (one), quality manager (one)</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>
in health care practice. During our observations, we focused on the same categories as during the semi-structured interviews, i.e. areas that regulate information security practice. This resulted in employees being re-interviewed and further questioned about the reasons for their actions.

4.2 Data analysis

Data analysis was carried out in five steps using the VBC framework and the taxonomy of SAT presented in Table I. The VBC framework highlights the following concepts: the actor, the information system action (prescribed and actual), the goal and the value. These concepts are shown in Figure 1 using a unified modeling language class diagram. Between these concepts, a number of associations are used to capture compliance and non-compliance, and the rationality upon which the different actions are based. As is shown in Figure 1, all types of information security actions, both actual and prescribed, are social actions associated with an actor. Information security managers design prescribed information security actions, while users carry out actual information security actions when they handle information/information assets in their daily work. Both actual and prescribed information security actions are based on the actor’s goals and values, which are anchored in the actor’s work practice (as a user or designer). Different levels of compliance can be identified:

- compliance at the activity level;
- compliance at the goal level; and/or
- compliance at the value level.

![The VBC framework](image)

**Source:** Hedström *et al.* (2011)
Our analysis was carried out with a specific interest in the rationale for actual information security actions. We used the type of mental process laid out in SAT to determine the type of social actions and the type of rationality involved.

The first step was to identify a set of prescribed and/or prohibited actions based on the hospital’s information security policy, guidelines, and routines. We eliminated duplicates during this step in order to reduce the amount of data that needed to be analysed in later steps. Second, we used the data gathered from the employees to elicit a list of actual information security actions. It was decided that when the users described the same information security action with different levels of abstractions, these should be grouped together. Again, this was done in order to reduce the number of action statements that needed to be worked on during the on-going analysis. In our third step, we categorized instances of compliance and non-compliance by comparing the set of prescribed/prohibited actions with the users’ actual actions. The non-compliance actions are presented in Table III, where they are grouped into four main categories.

In the fourth step, we analysed the rationale behind the non-compliance actions using the SAT taxonomy. We used the transcribed interviews and observation protocols as input for the analysis. First, we asked “Why is this action performed in this context?” in order to identify which type of mental process, if any, was behind the actual information security actions. If the answer described an intentional effort, we had identified a goal related to either an instrumental or a value-oriented action. When we could not trace any effort towards achieving an intention, such an action was classified as traditional or affectual, i.e. these non-rational actions are based on what caused the action. Second, we classified the identified rationality behind instrumental and value-oriented actions using SAT’s four types of rationality (substantive, practical, formal, theoretical).

During the fifth and last step, we classified the identified non-compliance actions based on the type of users’ non-compliance during the routine handling of patient information. This resulted in four types of non-compliant actions: non-compliance regarding password routines, non-compliance regarding information routines, non-compliance regarding documentation routines, and non-compliance regarding illicit use of systems.

During our analysis, we continuously used three expert panels to further validate our findings. Two of the expert panels consisted of administrative staff, physicians,

<table>
<thead>
<tr>
<th>Categories of non-compliance</th>
<th>Non-compliance action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password routines</td>
<td>Password sharing</td>
</tr>
<tr>
<td></td>
<td>A system for password creation</td>
</tr>
<tr>
<td></td>
<td>Same password for all systems</td>
</tr>
<tr>
<td></td>
<td>Not logging out</td>
</tr>
<tr>
<td>Information sharing routines</td>
<td>Writing sensitive patient information on paper notes</td>
</tr>
<tr>
<td></td>
<td>Lists of patients are written on the wall in view of incoming patients</td>
</tr>
<tr>
<td></td>
<td>Store sensitive information in unauthorized places</td>
</tr>
<tr>
<td>Documentation routines</td>
<td>Summarizing patient data</td>
</tr>
<tr>
<td></td>
<td>Censuring extra sensitive patient information</td>
</tr>
<tr>
<td></td>
<td>Not all physicians verify journal information</td>
</tr>
<tr>
<td>Illicit use of systems</td>
<td>Private, not healthcare-related, internet browsing</td>
</tr>
</tbody>
</table>

Table III.
Identified types of non-compliance
5. Non-compliance in a Swedish hospital

The overall purpose of information security policy at the studied hospital is to ensure that the “correct person has access to the correct information when needed and where needed” (County Council, 2001). We encountered four types of information security non-compliance at the two clinics (Table III). The first type of information security non-compliance is associated with users not following the routines regarding passwords. The second type illustrates how users develop different routines for managing and sharing patient data that goes against information security policies. The third type concerns documentation of patient information that does not follow protocol. Finally, the fourth relates to illicit use of systems.

5.1 Password routines

Most of the examples of non-compliance in Table III are associated with instrumental social actions, i.e. actions based on means-end calculations. They are deliberate and carried out for a reason. The nurses state that the reason for sharing passwords is that “it would be too cumbersome to log in and out all the time”. This means that the nurses intentionally choose to use the same password and refrain from logging out from the system. This is done when they access, in their view, less sensitive information. In this case, the nurses’ non-compliance their use of the cash register. Another example of non-compliance with the rules for password management is when users write the password on a piece of paper, which they stick on the wall so that it is easily accessible by all. This is also a clear example of an instrumental social action, as it is deliberate and based on the need to make password management easier. It is a case of practical rationality because the users judge the need to have easy access to passwords to be more important than following information security routines. Hence, it is an intentional action that is based on the need for efficient work practices. It is also possible that this way of managing passwords is based on tradition, where the habits of password management have, to some degree, become institutionalized to the extent that it is now taken for granted (Berger and Luckmann, 1967). The nurses work in teams, making the team an important social group in which traditions can easily evolve.

The same explanation, in which social actions are instrumental, is also valid for situations when users use the same password for all systems or when they choose passwords that are not complex enough to be secure. One of the users explained to us that “Normally, I use the same password [for all systems] in order to remember them. You have to do that in order to remember them”. Another user explained that:

I usually have one word and then I add a number, which becomes a running sequence of numbers in new versions of the password. But I don’t know if it is safe.
The reason why these users have developed password systems that lead to weak passwords, and have used the same password for all systems is based on practical rationality. Thus, users avoid having to remember many different passwords as a means to an end.

On several occasions, we also noticed that different types of information systems were left logged on, even though no one was sitting at the computer. This was the case even with the EMR, which contains very sensitive patient information. A failure to log out can also be classified as an affectual action, without any rationality or underlying intention. For instance, in the case of an emergency, the person sitting at the computer may have to rush off to attend to a patient. One user said:

You don’t always have time to log out from the computer. An alarm sounds, and then you have to run and don’t have time to log out from all the systems.

We also found cases where the physician’s failure to log out of EMR was intentional, because “I would not be away for a long time”. Consequently, it was not considered worth the effort to log out, which is a means-end calculation (practical rationality).

5.2 Information sharing routines

Another instance of non-compliance concerns the widespread use of paper notes containing summaries of patient information taken from the medical records. These notes include such information as the patient’s name, room, reason for admittance, and need for support. The nurses write these notes for the benefit of the next team of nurses that takes over patient care. The users say that these notes are important:

The same information is partly in the electronic medical record, but this way is much quicker, it’s about efficiency. We don’t have time to sit by a computer and read about every patient when you have ten patients to take care of. We also have to attend to new patients and new prescriptions, so we don’t have time to read through everything.

This routine is clearly an instrumental social action that is meant to save time when communicating information about patients. Yet again, this is an example of practical rationality.

We have seen many examples of the risks associated with showing sensitive patient information to, for example, other patients and unauthorized staff. Such information includes transcripts from the medical records. This is clearly not in line with the information security policy, which states that “Medical records shall be kept locked or in a box”, and “Every piece of a medical record shall be handled and stored in a way that prevents unauthorized access”. One example of non-compliance is when physicians take medical records away with them, and accidentally leave them in their office. This is an example of a non-rational, affectual social action.

The secretaries fetch medical records for the coming day from document storage. These medical records are later placed on the reception desk, where they are not securely stored. Not only is there a risk that unauthorized persons can gain access to them, but also this way of handling medical records does not follow confidentiality rules. The hospital’s information security policy states, for example, that it is important to offer “protection against events or actions that, intentionally or unintentionally, lead to the disclosure of information”. In this example, the secretaries’ decision not to follow this ruling is clearly based on practical rationality, and means and effect. This is an instrumental social action, where the aim is to achieve greater efficiency and save time.
in the morning. By doing this the night before, the medical records are easily available for the next day. When the staff arrive in the morning, they can concentrate on incoming patients rather than having to bother about fetching documents.

5.3 Documentation routines
The hospital’s quality manager stressed the importance of “taking notes as soon as you are with a patient”, and that “everything important shall be registered in the medical record”. Nevertheless, the physicians do summarize or censor patient information in the medical records, because:

[...] if the information doesn’t lead to anything, not to any action or if no one has any need for the information, I think one can wait to write it [in the medical record] as it generates extra work for the secretaries, without coming to any use.

The physicians also summarize patient information for patients who stay in hospital over the weekend: “if the patients stay a little longer and over the week-end I usually summarize [dictate] on Thursday”. The physicians estimate that the usefulness of keeping timely and detailed record-keeping is not worth the time it takes. Thus, this is an instrumental social action that is based on practical rationality.

The decision to censor patient information is also common in counsellors’ work:

One is extra careful about what you write in the records, and you write in a more general manner so you make sure that you do not disclose any patients by writing something offensive or sensitive. You know that other people can read the information. You write “family-problem” instead of writing the exact nature of the problem.

The way that counsellors deal with extra sensitive patient information clearly shows that they think it is more important to protect the patient’s privacy than to strictly follow the rules of information security. For them, it was very important to keep and cultivate the patient’s confidence. This is an example of a value-oriented social action and substantive rationality. Counsellors in Sweden maintain strict confidentiality, which is deemed to be an important value in counsellor education. What ever emerges in the conversation between the patient and the counsellor is not to be disclosed (with a few exceptions regulated by law).

Another important routine is related to physicians’ verification of patient data in the medical records, such as medical transcripts or test results. One reason physicians have to sign test results is to verify that they have read the information. Chief physicians are, however, excluded from this because, as one user stated, they do not have the time to sign such transcripts. Chief physicians have a limited amount of time at their disposal, which is seen as being more important than other physicians’ time. This is another example of an instrumental social action that is anchored in practical rationality in order to make better use of chief physicians’ time.

5.4 Illicit use of system
According to one of the nurses, they had been informed that they “shouldn’t use the internet for private matters as for instance looking for houses for sale, and that Internet usage should only be related to work”. Irrespective of this, they did use the internet for private matters during night shifts: “I guess we all are on the Net, it helps us not to fall asleep”. This is clearly an example of a traditional social action, which is carried out because everyone else is doing it.
6. Discussion

6.1 Non-compliance as social actions

The examples of non-compliance actions found at the hospital are based on our data from the two clinics. We gathered a good mix of actions, which relate both to manual and electronic handling of patient data, because the two clinics use computerization to varying degrees. It is clear from the examples we have given that these differences affect the ways in which patient information is handled.

Instrumental actions, which are anchored in practical rationality, are the most common, as illustrated in Table IV. These actions are based on an intention to achieve an end, such as being able to remember the passwords, or create more efficient routines for information access and sharing. This is not surprising as many of the reasons for users’ failure to comply with information security polices were based on a need to work efficiently. Sometimes, the hospital staff found the information security routines to be too cumbersome and time-consuming (for a more thorough discussion on value conflicts see Hedström et al. (2011)). However, it is worth noting that we did not find any instrumental non-compliance actions that were anchored in formal rationality. In other words, we did not find any cases where the hospital staff argued that existing information security policies were in conflict with other formal documents, such as those relating to the law. Moreover, we found no evidence that users’ non-compliance was based on theoretical rationality.

<table>
<thead>
<tr>
<th>Type of non-compliance action</th>
<th>Non-compliance action</th>
<th>Social action</th>
<th>Mental process</th>
<th>Type of rationality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password routines</td>
<td>Password sharing</td>
<td>Instrumental</td>
<td>Means-end calculation</td>
<td>Practical</td>
</tr>
<tr>
<td></td>
<td>A system for password creation</td>
<td>Instrumental</td>
<td>Means-end calculation</td>
<td>Practical</td>
</tr>
<tr>
<td></td>
<td>The same password is used for all systems</td>
<td>Instrumental</td>
<td>Means-end calculation</td>
<td>Practical</td>
</tr>
<tr>
<td></td>
<td>Not logging out</td>
<td>Instrumental/ affectual</td>
<td>Means-end calculation/ non-rational</td>
<td>Practical/-</td>
</tr>
<tr>
<td>Information routines</td>
<td>Writing sensitive patient information on paper notes</td>
<td>Instrumental</td>
<td>Means-end calculation</td>
<td>Practical</td>
</tr>
<tr>
<td></td>
<td>Lists of patients are written on the wall in view of incoming patients</td>
<td>Instrumental</td>
<td>Means-end calculation</td>
<td>Practical</td>
</tr>
<tr>
<td></td>
<td>Store sensitive information in unauthorized places</td>
<td>Instrumental/ affectual</td>
<td>Means-end calculation/ non-rational</td>
<td>Practical/-</td>
</tr>
<tr>
<td>Documentation routines</td>
<td>Summarizing patient data</td>
<td>Instrumental</td>
<td>Means-end calculation</td>
<td>Practical</td>
</tr>
<tr>
<td></td>
<td>Censuring extra sensitive patient information</td>
<td>Value oriented</td>
<td>Decision based on a value system</td>
<td>Substansive</td>
</tr>
<tr>
<td>Illicit use of systems</td>
<td>Chief physicians do not verify journal information</td>
<td>Instrumental</td>
<td>Means-end calculation</td>
<td>Practical</td>
</tr>
<tr>
<td></td>
<td>Internet browsing</td>
<td>Traditional</td>
<td>Non-rational</td>
<td>–</td>
</tr>
</tbody>
</table>

Table IV. Examples of non-compliance actions, social actions, the underlying mental process and type of rationality.
We encountered two examples of affectual non-compliant actions. The first example was when nurses sat in front of the computer, and had to rush off to attend to an alarm without logging out. The other related to the physicians who accidentally left medical records in their offices. We only found one clear example of traditional social actions: the case where the night nurses use the internet for private matters, because “everyone else is doing it”. Finally, we encountered only one value-oriented social action: the case when the counsellor chose patient privacy over documentation routines.

Four propositions can be put forward, based on empirical findings and the purpose of this paper, which is to evaluate the usefulness of SAT in information security management:

**P1.** Employees’ non-compliance is predominantly based on means-end calculations and practical rationality.

This proposition complements previous knowledge that suggests that about half of all security breaches caused by insiders are accidental (Vroom and Von Solms, 2004). Our research has shown that only a limited number of cases of non-compliance with security policies and regulations can be classified as non-rational actions. Our data comes from one hospital in Sweden, which might reflect the specifics of the health care sector and the particular context of that hospital. However, the study cited by Vroom and Von Solms (2004) used data taken from a variety of industries.

The rationality type that drives this behaviour is practical. This means that the reasons for users’ non-compliance are based on a need to carry out a specific task. If non-compliance is an effect of a rational choice, then we need to understand why users make this choice. Previous research has addressed user rationality from the perspective of general deterrence theory (Kankanhalli et al., 2003; D’Arcy and Hovav, 2009). Thus, it has been assumed that user non-compliance is predominantly based on malicious intent. Consequently, we suggest propositions **P2-P4**, shown below:

**P2.** An investigation of information security and employees’ rationality should not be based on an a priori assumption about user intent.

Although it should be noted that our study was not structured to target malicious actions per se, our results show that it was not possible to know in advance why employees chose not to follow a specific information security rule. Consequently, we should not have any a priori assumptions about their reasons for non-compliance. A previous study has shown that more than 90 per cent of known HIPAA breaches are both non-malicious and unintentional (Liginlal et al., 2012). For example, if we base our countermeasures solely on an assumption of malicious intent (as in general deterrence theory), there is a risk that these measures might be less efficient. We did not find any evidence of malicious misuse in our case, although many non-compliance actions were intentional. When we asked employees in our case why they did not follow protocol, they mostly could not account for their non-compliance. More often than not, their decision was based on competing goals and values, such as a need to adopt a usable password system, or a need to access patient data quickly and efficiently while on the go (for more details cf Hedström et al., 2011):

**P3.** Information security management and choice of countermeasures should be based on an understanding of the use rationale.
Our research is in line with that of Thomson and Nierkerk (2012), who stressed the importance of working towards common information security goals in order to cultivate a culture of information security. We were also influenced by existing work in this area, including the management-driven model of value-focused thinking (Dhillon and Torkzadeh, 2006), although in our study we take a clear user perspective. In this paper, we extend our research of user rationale by proposing a taxonomy for structuring an analysis. Such research is based on earlier work on value-conflicts presented by Hedström et al. (2011). Providing a high-level structure for analysis may help identify similarities in rich empirical data sets, thus making it possible to target design solutions towards these broader categories. This paper can also be related to work by Magklaras and Furnell (2002), who stated that it is important to understand the reasons for misuse. Thus, we focus on the importance of understanding users’ values, i.e. the rationality behind users’ actions. We take their argument further, and suggest a way forward for analysing the underlying reasons for users’ actions. We suggest that information security management and the choice of a mix of countermeasures should be based on an understanding of user rationale, where using SAT helps us to understand the type of rationality. With this as a basis we can develop countermeasures that target the specific type of rationality behind a user’s behaviour. For instance, it is necessary to develop countermeasures that address non-compliant acts based on practical rationality with a good understanding as to why these non-compliant acts have occurred:

\[P4.\] Countermeasures should target intentional as well as unintentional non-compliance actions.

Different countermeasures target different situations; thus, it is important to have a good mix of countermeasures (e.g. security policies, training, awareness-raising programmes, access controls, filtering) as a strategy for ensuring secure information use. Many of the theories used for understanding employee non-compliance fail to include unintentional misuse (Da Veiga and Eloff, 2007; McCarthy and Campbell, 2001). We believe that if we focus on users’ reasons for their actions, including both intentional and unintentional misuse, we can create a better understanding of users’ non-compliance, thus paving the way for sounder and more robust information security frameworks.

### 6.2 Implications for the choice of countermeasures

A mix of countermeasures is necessary in order to target and address different types of social actions. Table V shows a number of examples of countermeasures that address different types of social actions and their underlying rationality types. In the first column from the left we have exemplified non-compliance actions that originate from the combination of different types of social action and rationality. Although these examples are based on our empirical work, they are not entirely realistic, because we did not come across the full range of social action-rationality combinations during our empirical work. The second and third columns show the types of social action and types of rationality that the non-compliance action represents. The fourth column shows suggested implications of the choice of countermeasures. The table and the discussion given below are by no means an exhaustive review of how countermeasures can be related to different types of social actions and their rationality types; it just
serves as an example to show the breadth and variety of countermeasures that are more or less suitable for targeting different scenarios. Moreover, we used three broad types of countermeasures in our discussion: technical solutions, administrative routines, and awareness-raising programmes, which correspond to technical, formal, and informal information security (Dhillon, 1999).

Starting at the top of Table V we find an example of a traditional social action: private use of internet resources at work, which was based on the argument that everybody else does it and has always done it. As discussed earlier this type of social action does not involve any mental processes and is not associated with any type of rationality. Rather, it is rooted in old habits and, therefore, it might be difficult to find suitable technical countermeasures. For example, in this case, the employees frequently need to use the internet for a wide variety of work-related tasks; thus, it is not possible to block internet access. Instead, it is more appropriate to educate the employees on the current information security policy, which states that internet resources shall not be used for private purposes. In addition, it must be made clear to the employees why this regulation exists. For example, this type of internet usage competes for bandwidth resources that are needed for work-related tasks; thus, it is not possible to block internet access. Instead, it is more appropriate to educate the employees on the current information security policy, which states that internet resources shall not be used for private purposes. In addition, it must be made clear to the employees why this regulation exists. For example, this type of internet usage competes for bandwidth resources that are needed for work-related tasks; thus, it is not possible to block internet access. Instead, it is more appropriate to educate the employees on the current information security policy, which states that internet resources shall not be used for private purposes. In addition, it must be made clear to the employees why this regulation exists.

A failure to log out from an IT system when there is a need to rush off to an emergency situation is another type of non-rational social action (affectual) that does not involve a mental process. However, in contrast with traditional actions, it is difficult to introduce mental processes in situations of affection. Thus, awareness-raising programmes or administrative routines would have little or limited effect on these types of non-compliant actions. Technical solutions are expected to be more efficient, either by

<table>
<thead>
<tr>
<th>Example of non compliance action</th>
<th>Types of social action</th>
<th>Type of rationality</th>
<th>Countermeasure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private use of internet resources at work</td>
<td>Traditional</td>
<td>Value oriented</td>
<td>Awareness programme</td>
</tr>
<tr>
<td>Not logging out when rushing off to take care of an emergency alarm</td>
<td>Affectual</td>
<td>Substantive</td>
<td>Technical solution</td>
</tr>
<tr>
<td>Censuring extra sensitive patient information when documenting patient information</td>
<td>Substantive</td>
<td>Practical</td>
<td>Awareness programme</td>
</tr>
<tr>
<td>The same password is used for all systems</td>
<td>Instrumental</td>
<td>Formal</td>
<td>Administrative routines/technical countermeasures</td>
</tr>
<tr>
<td>Employee has to choose between conflicting administrative routines</td>
<td>Instrumental</td>
<td>Formal</td>
<td>Administrative routines, awareness programme</td>
</tr>
<tr>
<td>Employee stores own summaries of patient information, using liberal-intuitive theory to argue that actions not explicitly prohibited are allowed</td>
<td>Instrumental</td>
<td>Theoretical</td>
<td>Awareness programme</td>
</tr>
</tbody>
</table>

Table V. Examples of examples countermeasures that address different types of social actions and their underlying rationality types
solving the problem or reminding the employee to carry out certain actions. In the case of not logging out from the system, a technical solution can be implemented which logs out inactive users, automatically protecting sensitive information.

The third type of non-compliance actions shown in Table V are value-oriented social actions, which are based on substantive rationality. One such example is the counsellor who does not document all information about patients. This action is anchored in the value systems of the counsellor’s earlier education which stressed the great importance of building counsellor-client trust. Since these types of social actions are based on value systems that are different to those promoted by the organization, they must be targeted using education that aims to change an employee’s value systems. Implementing technical solutions or administrative routines will only result in an employee trying to find new ways to work around the system, because the employee believes he/she is doing the right thing.

As shown in Table V, instrumental actions can be anchored in three different types of rationality: practical, formal, or theoretical (indirectly). Practical rationality means that an employee carries out a means-end calculation that is based on available options to solve a problem, such as having to deal with a complicated password system. With regard to this type of rationality, the solution can be found in any of the three types of countermeasures or a combination of them. It must be determined by the underlying reasons that an employee chooses a particular option; in this specific case, the decision to reuse a password across multiple IT systems. Technical or administrative changes can give the employee other available options that better fit their work situation, whilst awareness-raising programmes can make an employee aware of which of the available options are good and bad choices, thus changing the means-end calculation. For example, implementing a single log-on for some or all of the IT systems may be one possible solution to this specific problem.

Instrumental social actions are based on means-end calculations and where the available options are specified by bureaucratic regulations such as laws or administrative routines. Consequently, non-compliance actions are anchored in formal rationality, which means that different types of laws and/or administrative routines may come into conflict with each other, or the employee may interpret it in this way. Hence, the employee uses a law or an administrative routine to argue for his/her actions. Depending on whether conflict between bureaucratic regulations is actual or perceived, the solution can be to either change the bureaucratic regulations (administrative routines) or make the employee aware of how to interpret existing bureaucratic regulations (awareness-raising programme).

Finally, instrumental actions can be based on theoretical models. For example, an employee who stores summaries of patient information in a local archive may use liberal-intuitive theory to argue that this action is allowable since information security policy does not explicitly state that local storage of patient information is forbidden. Instrumental actions are similar to value-oriented social actions in that the employee questions the fundamental workings of the organization’s information security practice. Implementing technical solutions or administrative routines that only deal with the immediate problem means that other types of non-compliance, which are anchored in the same theoretical rationality, can occur; in this case, liberal-intuitive theory. Hence, an employee needs to be educated as to why his/her theoretical rationality is in conflict with the organization’s existing information security practice.
The above discussion of information security measures covers all three broad categories. In practice, however, countermeasures need to be more specific; a specific type of technical countermeasure or an awareness-raising programme must target a specific area. Information security management and the introduction of any specific countermeasures should of course rely on previous knowledge and best practice. The findings of a study by Kroll Advisory Solutions (2012), also carried out in a hospital setting, have shown that unauthorized access is the most common security breach caused by employees. Thus, it must be considered an important input in devising countermeasures. However, using rationality types taken from SAT means that certain types of countermeasures can be ruled out since they do not target the actual cause of non-compliance action.

Magklaras et al. (2002) argued the importance of developing a security culture in order to achieve greater user compliance. Also of interest is a study by Pieters and Coles-Kemp (2011), who argued the importance of identifying conflicts between the security policy and cultural norms within an organization. We have complemented these studies with an approach that addresses non-compliance through an analysis of the rationale that underlies users’ actions. It is important to apply a multi-stakeholder perspective when designing information security measures, because managers and different groups of users have different views on information security and potential breaches (Von Solms and Von Solms, 2006).

6.3 Limitations of this study
This study was carried out at two clinics within one hospital; hence, it is limited both in terms of size and context. However, our aim was to illustrate the usefulness of SAT, and, clearly, the study was large enough to reveal examples that could be related to different types of social actions. What may have impacted on our results is the choice of context, and types of non-compliance. Further research could thus broaden the study’s scope to investigate other contexts. In addition, the result should be valid for other settings in which strong professional values are prevalent. These values influence the rationality of some employees, such as social workers (Banks, 1998), and psychiatric clinicians (Salomon et al., 2010). The resources available will, of course, heavily affect the chosen mix of countermeasures. In our discussion of countermeasures, we have not taken into account how such available resources as competence, time, and financial means would influence the management of information security.

Other limitations relate to data collection. We did not capture any malicious non-compliance (Stanton et al., 2005), which may be due to the research design itself. Our data collection relied on interview and observation techniques. Consequently, it may be reasonable to assume that the users’ behaviour and/or arguments, to some extent, changed in the presence of the research team. However, it was obvious during our observations that the hospital staff carried out actions that were not in-line with information security policies. Our data triangulation between interviews and observation allowed us to validate users’ descriptions of the kind of actions they carry out and the way in which they go about this. It may also be reasonable to assume that users may attempt to present their behaviour as rational during interviews, in order to defend their actions or even to “hide” malicious intent. This does not mean,
however, that malicious actions do not exist; only that we did not uncover any such information security actions.

7. Conclusion
Our research illustrates the usefulness of SAT for the management of information security. SAT and its taxonomy directs attention to the rationality of the actor in order to clarify and reveal the meaning of the action. By viewing information security actions as social actions, it is possible to gain awareness of the underlying reasons for users’ compliance and non-compliance without any a priori assumptions about user intent. We suggest that SAT can help to create a better foundation for the management of information security and support the selection of a good mix of countermeasures that focus on users’ rationality without any a priori assumptions about user intent. We believe that it is possible to reduce the number of non-compliant acts and create a more secure environment by developing countermeasures that address the underlying rationale for a specific non-compliant behaviour rather than overt behaviour. We present our findings in relation to four propositions, together with practical and theoretical implications. These four propositions can form the basis for information security management, and clarify the underlying objectives regarding user rationale presented in Hedström et al. (2011).

In our study, it was most common to find examples of instrumental non-compliant social actions, i.e. non-compliant as a means-end calculation, where the user sees the action as a means to an end. We found only one example of a value-oriented social action, two examples of affectual social actions, and one example of a traditional social action. The latter two types of actions lack rationale, and are not meaningful for the user; they are also difficult to predict. As non-compliance is frequently based on means-end calculations it becomes very important to base the design of information security countermeasures on a sound understanding of user rationale. In order to construct efficient countermeasures we first need to understand the reasons for both user compliance and non-compliance. We have also found that it is important to take into account non-compliant acts that are accidental or based on tradition. Even though not many of these can be found in our case, such misuse needs to be considered, because it can lead to serious security breaches. In the context of a hospital, non-compliant acts can cause serious harm, both for the patient and the organization, itself.

References


Patton, M.Q. (1990), Qualitative Evaluation and Research Methods, Sage, Newbury Park, CA.


**About the authors**

Karin Hedström is an Associate Professor of information systems at Örebro University as well as visiting Associate Professor of information systems at Linköping University. She holds a PhD in information systems development from Linköping University. Her research interests concern the ethics of information systems and information security. Dr Hedström has published in numerous international journals and conferences proceedings. Karin Hedström is the corresponding author and can be contacted at: karin.hedstrom@oru.se

Fredrik Karlsson is a Professor of information systems at Örebro University. He received his a PhD in information systems development from Linköping University. His research is about information security, compliance, tailoring of systems development methods, system development methods as reusable assets, and CAME-tools have appeared in a number of IS journals and conferences.

Ella Kolkowska is a Lecturer and PhD student at Örebro University. Her research is about social and organizational aspects in information security, value conflicts as well as compliance with information security policies.

To purchase reprints of this article please e-mail: reprints@emeraldinsight.com
Or visit our web site for further details: www.emeraldinsight.com/reprints