EXPLORING THE CONCEPTUAL STRUCTURE OF SECURITY RATIONALE

Fredrik Karlsson[1] & Karin Hedström[2]

[1]MELAB, Swedish Business School at Örebro University, SE-701 82 Örebro, Sweden, fredrik.karlsson@oru.se

[2] MELAB, Swedish Business School at Örebro University, SE-701 82 Örebro, Sweden, karin.hedstrom@oru.se

Abstract. Working with a socio-technical view on information systems security is a challenge. Existing studies show that a great number of security incidents are caused by trusted personnel within organizations due to the tension between the design of information systems security policies, guidelines, rules and tools, and how they actually are used. This paper describes a framework for anlyzinging users' compliance with the creator's intentions that underlie an information systems security design. This framework is anchored in the concept of rationality, and the result can be used, for example, to facilitate the task of analyzing security incidents, to verify existing information systems security approaches, and to match information systems security approaches with organizational requirements. We have illustrated the use of the framework with data on health-care information systems security.

Keywords. Information Security, Value, Goal, Framework, Compliance

EXPLORING THE CONCEPTUAL STRUCTURE OF SECURITY RATIONALE

INTRODUCTION

As early as 1999 Adams et al. conclude that 'unless security departments understand how the mechanisms they design are used in practice, there will remain the danger that mechanisms that look secure on paper will fail in practice.' To date, information systems security has primarily been concerned with confidentiality, integrity and availability. For example, they are found in the ISO/IEC 27002 (ISO 2005) where information systems security is defined as the 'preservation of confidentiality, integrity and availability of information.' Consequently, technical tools, methods and standards for supporting this triad are in many aspects the centre of gravity when it comes to information systems research (Siponen et al. 2007). As Huebner et al. (2006) conclude there exist few papers that 'focus on the behavioural and social aspects of security' although the challenge is to control human behaviour (Albrechtsen 2006). Both Dhillon et al. (2000) and Sipponen et al. (2000) argue that taking information systems security issues in organizations seriously requires more than what traditional technology-centred security approaches can offer us. Therefore, Dhillon (2006) provides a broader definition of information systems security as 'the protection of information resources of a firm, where such protection could be through both technical means and by establishing adequate procedures, management controls and managing the behaviour of people.'

Information systems security is provided through information systems security mechanisms (or security mechanism for short), such as tool-based implementations, guidelines, and manuals (Albrechtsen 2006; Oscarson 2007). Oscarson (2007) defines a security mechanism as 'something that aims to achieve or maintain the confidentiality, integrity or availability of information assets.' As designed artefacts they encapsulate knowledge of good security practice. In this paper we make the case that the creators' intensions or design rationales, as part of the concept we term security rationality, inherently influence these approaches. In other words, design rationale is based on the creator's values and assumptions about security threats and information assets. Implicitly or explicitly these values and assumptions motivate the different actions that are included in the security mechanism. Today, we see that many organizations apply general standards such as the Code of Practice (ISO 2005) in formulating policies, rules and procedures. Hence, when using such standards, organizations have to rely on the design rationale of that particular standard. At the same time Halliday et al. (1997) conclude that standards are often implemented without local adaptation. As a consequence users do not always follow the security mechanisms advocated by

management and the security incidents described by Vroom et al. (2004) illustrate a tension between the information systems security approach in-concept and the security in-use. A basic condition for information systems security tools, rules and procedures to be accepted and adopted by people in organizations is that the they perceive them as appropriate and not as obstacles to the organization's operations (Dhillon 2007).

The aim of this paper is to explore the subject matter of security rationale and to investigate how the tension of security in-concept and security in-use can be analyzed. The security rationale framework (see Figure 1) can be used, for example, to facilitate the task of analyzing security incidents, to verify existing information systems security approaches, and to match information systems security approaches with organizational requirements. Consequently, the framework can assist organizations in taking informed decisions on development of information systems security. In addition, it assists in explicating otherwise tacit knowledge concerning the use situation of information systems security approaches.

The organization of this paper is structured as follows. The next section describes related research. The third section is devoted to social actions and rationality in relation to information systems security while the fourth section introduces the security rationale framework. The use of this framework is then exemplified in the fifth section with an illustrative analysis of an existing information systems security approach at a Swedish hospital. The purpose of this section is to explore the usefulness of this framework in understanding the tension of security in-concept and security in-use. The paper ends with a short conclusion about the framework and further research.

SOCIO-TECHNICAL INFORMATION SYSTEMS SECURITY RESEARCH

The research on social-technical aspects related to information systems security compliance is increasing. This research can, at least, be divided into two categories: compliance studies, and frameworks for compliance studies.

In the first category, Vroom et al. (2004) as well as Doherty et al. (2005) have analyzed the compliance with information systems security policies. The latter found no statistical relationship between the application of policies and incidences, and they question dissemination strategies used. Besnard et al. (2004) as well as Albrechtsen (2006) have argued that users prioritize other work tasks instead of complying with information systems security, which means that the users prioritize between different goals. Dhillon et al. (2000), Schlarman (2001)

as well as Thomson et al. (2006a; 2006b) stress the significance of understanding organizational culture, such as beliefs, values and assumptions when working with policies and users' actions. Accordingly, both the creator's and the user's rationales are important aspects to consider when analyzing compliance in information systems security.

In the second category, frameworks for compliance studies, we find models with a scope similar to the security rationale framework. Stanton et al. (2005) provide a six-element taxonomy model to classify user behaviour in two dimensions: technical expertise and intentions. Huebner et al. (2006) have proposed a high level analysis model to capture socio-behavioural aspects of information systems security with a focus on structuration as an continuous process. Chang et al. (2007) as well as Chan et al. (2005) emphasize the importance of acknowledging the relationship between social contextual factors and information systems security. They also provide research models for studying impacts of contextual factors on information systems security. Although these models provide valuable frameworks for analyzing social factors and/or intentions in relation to compliance with information systems security they do not provide support for analyzing the relationship between designed rationale and use rationale of security mechanisms.

SOCIAL ACTIONS AND RATIONALITY IN INFORMATION SYSTEM SECURITY

Since security mechanisms represent knowledge of good security practice they also represent rationale. Regardless of the grounds, the design as well as the use is 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 (1978). First of all he makes a distinction between behaviour and actions. An action, such as designing or using a security mechanism, occurs when actors attach subjective meaning to what they do, unlike behaviour that does not involve a thought process. This leads Weber (1978) to four types of social actions: traditional, affectual, value oriented, and instrumental. Traditional actions are determined by deeply rooted habits, while affectual actions are determined by the actor's feelings or emotions. The third type, value oriented actions, is undertaken for reasons intrinsic to the actor, such as ethical reasons. 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.

As illustrated in Table 1, two of these four types of social actions – value rational and means-end rational – can be associated with Weber's types of rationality: practical, theoretical, substantive, and formal (Kalberg 1980). Practical rationality is what individuals use to carry out their daily routines and tasks. Hence, instead of basing actions on an absolute value system, individuals accept given realities and choose from preconceived means to achieve a particular end. According to Weber (1978) practical rationality is anchored in means-end calculations. An example is a user who uses the same password to several information systems. This illustrates use rationale and is based on a means-end calculation to ease the burden of remembering passwords. Of course, this rationale might or might not differ from the design rationale of not implementing single sign on.

Table 1. The relationship between social actions and rationality types

Social actions	**Mental Process**	**Types of rationality**
Traditional	Nonrational	-
Affectual	Nonrational	-
Value oriented	Decisions are anchored in a context dependent value system	Substantive
Instrumental	Means-end calculation	Practical, formal
-	Use of conceptual models	Theoretical

The second type of rationality, theoretical rationality, masters reality through conceptual models 'rather than through actions.' (Kalberg 1980) Hence, this type of rationality is based on logical deduction. This type of rationality is not directly associated with social actions; however the constructed models have the potential indirectly to shape patterns of actions. For example, the People, Policy, Technology Model (Schlarman 2001) can serve as a framework when designing a security mechanism.

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. These actions are not purely based on choosing means to ends and acting upon these decisions. These decisions are anchored in 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 might anchor their 'right' to freely install software on their computers in these values. Hence, this type of rationality may organize some part of life, and an actor can change value clusters depending on context.

Finally, we have the fourth, and formal, type of rationality. This type of rationality is often associated with organizations, such as bureaucracies. In the same way as practical and substantive rationality it directly orders actions into

patterns based on means-end calculations. In this case the calculations are anchored in universal rules, laws or regulations. Hence, the resulting actions are made without regard to people. One example of formal rationality in security mechanisms is 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.'

THE SECURITY RATIONALE FRAMEWORK

Our analytical framework is illustrated as UML classes in Figure 1. In total the framework consists of the following classes: security mechanism (in-concept and in-use), actor (creator and user), goal and value. Between these classes we find a number of associations. Our analytical framework is anchored in the concept of security mechanism. Oscarson (2007) divided them into manual protections or tool-based protections. Manual protections are administrative processes such as processes, standards, policies, laws and rules, as well as knowledge based protections such as collective or individual knowledge of information systems security. In addition he divides tool-based protections into information technology based (e.g., hardware and software), and non-information technology based protections (e.g., fire distinguishers, paper-shredders, doors and locks). This means that a security mechanism can be on different levels and of different types. The former is illustrated by the 'part of' association in Figure 1. We see a specific security mechanism as ranging from a guideline, an implemented tool-based solution to methods and sets of tool-based solutions.

A security mechanism is usually introduced by management in order prevent, avert, or recover an incident. In Figure 1, we chose to term this 'in-concept.' Management in their role as leaders legitimates the security mechanisms in organizations (Berger et al. 1967). These security mechanisms are, or are suppose to be, used by people in the organization to improve their work practice in terms of information systems security. We term this security mechanism 'in-use', which is the user's interpretation and adapted version of the security mechanism.

In the framework we acknowledge the possibility of three different relationships between the security mechanism in-concept and in-use. First, we have the ideal situation when there is a correspondence between the security mechanism in-use and in-concept; in other words, the security mechanism is used as intended. Second, the security mechanism in-concept might not have a practical equivalence in-use. Hence, in this situation there is a difference between the security mechanism in-concept and in-use. This can happen when management fails to communicate the security mechanism, or when users do not agree with its importance. Third, a security mechanism can exist in-use only, without a

corresponding legitimized in-concept mechanism. This is the case when users develop their own security mechanisms, based on their understanding of the every-day work practice and view on important information systems security approaches.

Figure 1. Security rationale framework

Weber's (1978) view on social actions and rationality helps us explaining the tension between in-concept mechanism and a security mechanism in-use. It shows that the design rationale of security mechanisms as well as the use rationale is anchored in the actors' goals (see Figure 1). For example, how formal rationality, such as the goals with the Personal Data Act, can be used as part of the creator's rationale when designing a security mechanism. In our framework this type of goals are related to each other. We have identified two types of association: goal achievements and goal contradictions. In the first case goals support each other and in the second case they are in conflict. For example, goals from two different acts can be in conflict with each other. Furthermore, the goals are, in turn, manifestations of the actor's value base. When anchoring a security mechanism in the Personal Data Act the creator also adheres to the values of that act, such as privacy values. In a set of values we acknowledge two types of associations; values can support or contradict each other. This is in line with previous work on goal-oriented research in for example requirements engineering (e.g. Braesciani et al. 2004; Mylopoulos et al. 2001) and method engineering (e.g. Karlsson et al. 2006; Ågerfalk et al. 2006). Hence, it is possible to depict two different types of rationale that illustrates the tension between security mechanisms in-concept and in-use. First, the security mechanisms' designs are anchored in one or more goals that the creator wants to fulfil. We chose to define this as the security mechanism's design rationale. Second, we have the user's goal with using the security mechanism. This might or might not be anchored in another set of goals than the creator wants to fulfil. We term the user's goals for using the security mechanism use rationale. The discrepancy between the design rationale and the use rationale for a given security mechanisms illustrates the tension between information systems security in-concept and in-use.

RESEARCH APPROACH

The security rationale framework is illustrated by empirical data from a interpretative case study (Walsham 1995; Yin 1994) carried out at the hospital of Karlskoga – a small county hospital in central Sweden. The hospital serves approximately 90 000 citizens. The hospital is situated in the County of Örebro, responsible for healthcare for 274 000 inhabitants. The vision of the information

systems security work in the County of Örebro is to provide ‘correct information to the right people, right on time, and to the right place.’ In addition, it is important to acknowledge that the information systems security analysis has been carried out with a focus on patient information. Following the National Health Service Act (Department of Health 2008) patient information was defined as ‘(a) information (however recorded) which relates to the physical or mental health or condition of an individual, to the diagnosis of his condition or to his care or treatment, and (b) information (however recorded) which is to any extent derived, directly or indirectly, from such information, whether or not the identity of the individual in question is ascertainable from the information.’

Data Collection

We used the security rationale framework to compare security mechanisms in-concept with security mechanisms in-use. The comparison is illustrated using data from a case study, which consists of two parts. The first part focused on in-concept security mechanisms, while the second part focused on the in-use security mechanisms. The in-concept security mechanisms were identified by carefully analyzing the county’s official documents related to information systems security objectives. The following documents were included in the analysis:

a. County council information security policy
b. County council IT strategy
c. 11 commandments on information security
d. Security instructions for county council IT users
e. IT policy for the county council
f. County council policy for information and communication
g. Routine descriptions regarding the handling of medical journals

To identify in-use security mechanisms we used interviews. Interviews were made with middle management, physicians, nurses, and medical secretaries. In this paper we chose to exemplify the use of the security rationale framework with a middle manager working at the surgery clinic responsible for personnel and surgery planning. We have chosen the example for two reasons. First, this role is central at the clinic when it comes to information handling. Second, this interview provides good examples of situations where the security mechanisms in-concept and in-use match as well as when they do not match, and, finally, situations where security mechanisms exist in-use but not in-concept. The interview focused questions such as how the information systems security work was carried out, how patient information was handled, and what the interviewee considered important in relation to information systems security.

Data Analysis

The security mechanisms were given unique numbers, which later were used in order to relate one specific in-concept security mechanism with a comparable security mechanisms identified in-use from the interview. The security mechanisms were carefully analyzed row by row, and direct citations were used to describe their content.

The purpose of the analysis was to identify a) the practical use of security guidelines, policies, instructions and/or tools in the clinic's work practice, and b) if there are security mechanisms developed and used in the work practice, without having any counterparts in the security guidelines, policy or instructions. The analysis therefore describes three situations, 1) in-concept and in-use, 3) in-concept but not in-use, and 3) not in-concept but in-use. The first situation is the ideal one from an information systems security point of view, where the work carried out corresponds to the prescribed actions. Hence, in this situation we find a match between design rationale and use rationale. The second situation, when the staff deliberately or unintentionally fails to comply with a security mechanism, might indicate lack of knowledge, or that they do not agree with the design rationale of that security mechanism. The last situation illustrates the case when the work practice has developed a security mechanism not found in the guidelines, policies, or tools prescribed by the management. This might indicate that the governing management routines and policies need to be up-dated, or that the people working in the organization have a different view on information systems security. The two last situations indicate potential goal and value conflicts, which need to be further investigated in order to reduce the tension between information systems security in-concept and in-use.

ILLUSTRATING SECURITY RATIONALE IN A SWEDISH HOSPITAL

The following analysis is used as an illustration of the framework. We present two security mechanisms per situation. Consequently, this analysis is not to be seen as a complete analysis of security rationale at Karlskoga hospital. In this analysis we have related goals and values to the identified security mechanisms in the cases as they have been explicitly expressed by the interviewee or found in the analyzed documents.

In-concept and in-use

We found several statements when an in-use security mechanism is in accordance with its in-concept counterpart. Table 2 illustrates two security mechanisms related to the confidentiality of patient information. The first in-use statement (SM-H16) states that the staff never writes down patient information on papers,

thus minimizing the risk for disclosure due to papers lying about available for unauthorized persons. This statement is in the table compared with a similar declaration in the information security policy (SM-94), where the importance of being careful about patient information is stressed.

Table 2. In-use and in-concept

In-use	**In-concept**
SM-H16: 'We never write down information about the patient on a separate paper.' Goal: - Value: -	SM-94: 'Information related to an individual's social, medical, and personal affairs, has to be carefully protected against disclosure' (County council information security policy) Goal: 'The care taker shall protect the privacy of the patient' (11 commandments on information security), 'Patients should be confident that sensitive information will not be disclosed to unauthorized people.' (11 commandments on information security) Value: Confidentiality
SM-H120 'One is not allowed to discuss patients with people in the staff unless it is beneficial for the patient.' Goal: 'It is very important with professional secrecy.' Value: -	SM-106: 'A patient's condition and personal affairs is only to be discussed with people within the work team, and only if it is necessary for the treatment of the patient.' (County council policy for information and communication) Goal: 'The user will only have access to information needed for the work.' (11 commandments on information security) Value: -

The second in-use statement (SM-H120) concerns the habit or need to discuss patients with one's peers. The interviewee clearly states that one is only allowed to discuss patients, even with staff, when it is deemed as helpful for the patient in some way. This statement can be related to the declaration SM-106 found in the policy for information and communication which states that one has to be careful when discussing patients, and that it can only be done with people from the same work team, and only when it is seen as beneficial for the treatment of the patient.

In-concept but not in-use

We also found security mechanisms that where in-concept in the various documents, but not used in the work practice. One such example, in Table 3, is the question about information systems security training. The interviewee states that they, at her work place, have not received any special training regarding how to handle sensitive information such as medical journals (SM-H44). This can be compared to the declaration expressed in the IT strategy where the importance of

training for all staff in information systems security is stressed (SM-40). It is problematic if not all staff has received the training put forward as important, as training is important for raising the security level and preventing incidents due to information systems security breaches.

Table 3. In-concept but not in-use

In-use	**In-concept**
SM-H44: 'We haven't received any special training [about how to handle medical journals], instead it is something which is discussed.' Goal: - Value: -	SM-40. 'The county shall offer all employed IT-education on different levels…With a special emphasis on information systems security.' (County council IT strategy) Goal: 'All staff shall have knowledge about the county's information security policy, guidelines, rules, and instructions' (IT policy for the county council) Value: -
SM-H15: 'We put the medical journals at a special place close to the fax-machine. It is not possible to lock this room.' Goal: - Value:	SM-85: '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' Goal: 'Medical journals shall never be kept unsupervised in a room which is not locked' (Routine description regarding the handling of medical journals)

Another example of a security mechanism that is emphasized in the documents, but handled a bit different in the work practice, is the question about how to keep medical journals for patients staying at the clinic. The documents state very clearly that medical journals shall be kept in a locked room unless they are supervised by someone from the staff (SM-85). The people working at the clinic with the everyday practice place the medical journals in an unlocked room, easily available for the staff (SM-H15). These two security mechanisms clearly illustrates the clash between availability and confidentiality, where the staff needs to be able to efficiently access important documents, while the routine description is more concerned with following the formal rationality of the Swedish Patient Record Act (Ministry of Health and Social Affairs 2008).

Not in-concept but in-use

The work practice stresses the importance of availability of information and reliable information. These two issues are not mentioned in the documents as frequently. The interviewee stated, for instance, that 'It is important that the

medical journals are in alphabetical order. If they are in a mess it is difficult to find the correct information.' (SM-H14 in Table 4). There is no statement in the documents mentioning the importance of putting the medical journals, or any information for that matter, in a specific order. This illustrates that it is important for the work practice to have efficient and safe access to patient information. If not there is a risk that the patient might receive the wrong treatment.

Table 4. Not in-concept but in-use

In-use	**In-concept**
SM-H14: 'It is important that the medical journals are in alphabetical order.' Goal: - Value: -	Security mechanism: - Goal: - Value: -
SM-H17: 'Everyone has access. This is important as one sometimes has to read a last note about e.g., which kidney the operation concerns, then one looks at the x-rays, and on the operation announcement and on the patient. So this is really an extra check that the operation is performed on the correct side. It is important as it has fatal consequences for the patient. We need to be able to access the medical journal before surgery.' Goal: - Value: -	Security mechanism: - Goal: - Value: -

Another statement (SM-H17) expressed by the interviewee is that it is important for them that everyone at the clinic has access to the medical journals of every patient's that are at the clinic. This concern about availability, and the need for accessing all medical journals, is not at all mentioned in the documents, which are more concerned with restrictions and controls when discussing authorization.

CONCLUSIONS

In this paper we have presented a security rationale framework for developing a better understanding of the differences between information systems security in-concept and in-use. The framework makes it possible to distinguish between situations (a) where the introduced security mechanism is used as intended, (b) where the introduced security mechanism is not used as intended or not used at all, and (c) when there is a security mechanism in-use which has not been introduced by management and hence it does not exist in-concept. In addition,

through the use of the security rationale framework it is possible to identify the differences in the design and use rationale for these three situations. Consequently, based on the analytical results it is possible (a) to verify existing information systems security approaches by analyzing the overlap between use and design rationale of security mechanism, (b) better match information systems security approaches with organizational requirements by paying attention to use rationale during design of security mechanism, and (c) to facilitate the task of analyzing security incidents through analysis of difference between the use and design rationale. Hence, all three situations aim at reducing the tension between informations security in-concept and in-use.

In this paper we have, when possible, provided associated goals and values for the identified security mechanism. The reason is that we only have based the analysis on explicit statements from the actors (creators or users). However, it is possible to interpret the rationale behind different statements as put forward by Dhillon et al. (2006) in their work on values on information systems security. This might be a more fruitful way of analyzing. However, it calls for method development together with the framework in future studies.

ACKNOWLEDGMENTS

We want to thank the Swedish Emergency Management Agency for providing the funding for this research. We also want to show our gratitude to Örebro County Council, and the staff at the hospital of Karlskoga, who so generously has given us their valuable time and invited us to take part of their every-day work.

REFERENCES

Albrechtsen, E. "A qualitative study of user's view on information security," *Computers and Security* (26:4) 2006, pp 276-289.

Berger, P.L., and Luckmann, T. *The social construction of reality. A treatis in the sociology of knowledge* Anchor Books, New York, USA, 1967.

Besnard, D., and Arief, B. "Computer security impaired by legitimate users " *Computers & Security* (23:3) 2004, pp 253-264.

Braesciani, P., Perini, A., Giorgini, P., Guiunchiglia, F., and Mylopoulos, J. "Tropos: An Agent-Oriented Software Development Methodology," *Autonomous Agents and Multi-Agent Systems* (8:3) 2004, pp 203-236.

Chan, M., Woon, I., and Kankanhalli, A. "Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior," *Journal of Information Privacy & Security* (1:3) 2005, pp 18-41.

Chang, S.E., and Lin, C.-S. "Exploring organizational culture for information security management," *Industrial Management & Data Systems* (107:3) 2007, pp 438-458.
Department of Health *Health and Social Care Act 2008* Department of Health, London, 2008.
Dhillon, G. *Principles of information systems security: text and cases.* Wiley Inc, Hoboken, NJ, 2007.
Dhillon, G., and Backhouse, J. "Information security management in the new millenium," *Communication of the ACM* (43:125) 2000.
Dhillon, G., and Torkzadeh, G. "Value-focused assessment of information security in organizations," *Information Systems Journal* (16:3) 2006, pp 293-314.
Doherty, N.F., and Fulford, H. "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis," *Information Resources Management Journal* (18:4) 2005, pp 21-39.
Halliday, J., and von Solms, R. *Effective information security policies* Port Elizabeth Technikon, Port Elizabeth, 1997.
Huebner, R.A., and Britt, M.B. "Analyzing Enterprise Secuirty Using Social Networks and Structuration Theory," *The Journal of Applied Management and Entrepreneurship* (11:3) 2006, pp 68-77.
ISO "ISO/IEC 27002:2005, Information Technology - Secuirty Techniques - Code of Practice for Information Management Systems - Requirements."
Kalberg, S. "Max Weber's Types of Rationality: Cornerstones for the Analysis of Rationalization Processes in History," *American Journal of Sociology* (85:5) 1980, pp 1145–1179.
Karlsson, F., and Wistrand, K. "Combining method engineering with activity theory: theoretical grounding of the method component concept," *European Journal of Information Systems* (15:1) 2006, pp 82-90.
Ministry of Health and Social Affairs "Patient Record Act (SFS 1985:562)," Ministry of Health and Social Affairs, 2008.
Ministry of Justice "Personal Data Act (SFS 1998:204)," Ministry of Justice, 2008.
Mylopoulos, J., Chung, L., Liao, S., Wang, H., and Yu, E. "Exploring Alternatives during Requirements Analysis," *IEEE Software* (18:1) 2001, pp 92-96.
Oscarson, P. "Actual and perceived information systems security," in: *Linköping University*, Linköping, Linköping, Sweden, 2007.
Schlarman, S. "The People, Policy, Technology (PPT) Model: Core Elements of the Security Process," *Information Systems Security* (10:5) 2001, pp 36-42.
Siponen, M. "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management & Computer Security* (8:1) 2000.
Siponen, M.T., and Oinas-Kukkonen, H. "A Review of Information Security Issues and Respective Research Contributions," *Database for Advances in Information Systems* (38:1) 2007, pp 60-80.

Stanton, J.M., Stam, K.R., Mastrangelo, P., and Jolton, J. "Analysis of end user security behaviors," *Computers & Security* (24:2) 2005, pp 124-133.
Thomson, K.-L., and von Solms, R. "Towards an Information Security Competence Maturity Model," *Compter Fraud & Security* (2006:5) 2006a, pp 11-15.
Thomson, K.-L., von Solms, R., and Louw, L. "Cultivating an organizational information security culture," *Compter Fraud & Security* (2006:10) 2006b, pp 7-11.
Walsham, G. "The Emergence of Interpretivism in IS Research," *Information Systems Research* (6:4) 1995, pp 376–394.
Weber, M. *Economy and society* University of California Press, Berkeley, CA, 1978.
Vroom, C., and von Solms, R. "Towards information security behavioural compliance," *Computers and Security* (23:3) 2004, pp 191-198.
Yin, R.K. *Case study research: design and methods*, (2nd ed. ed.) SAGE, Thousand Oaks, CA, 1994, pp. xi, 171.
Ågerfalk, P.J., and Fitzgerald, B. "Towards Better Understanding of Agile Values in Global Software Development," Eleventh International Workshop on Exploring Modeling Methods in Systems Analysis and Design (EMMSAD'06), Luxembourg, 2006.