Improving the Information Security Model by using TFI

Rose-Mharie Åhlfeldt[1], Paolo Spagnoletti[2] and Guttorm Sindre[3]
1 University of Skövde, Box 408, S-542 28 Skövde, Sweden
rose-mharie.ahlfeldt@his.se
2 CeRSI – Luiss Guido Carli Unversity, Roma, Italy pspagnoletti@luiss.it
3 NTNU, Trondheim, Norway guttors@idi.ntnu.no

Abstract. In the context of information systems and information technology, information security is a concept that is becoming widely used. The European Network of Excellence INTEROP classifies information security as a non-functional aspect of interoperability and as such it is an integral part of the design process for interoperable systems. In the last decade, academics and practitioners have shown their interest in information security, for example by developing security models for evaluating products and setting up security specifications in order to safeguard the confidentiality, integrity, availability and accountability of data. Earlier research has shown that measures to achieve information security in the administrative or organisational level are missing or inadequate. Therefore, there is a need to improve information security models by including vital elements of information security. In this paper, we introduce a holistic view of information security based on a Swedish model combined with a literature survey. Furthermore we suggest extending this model using concepts based on semiotic theory and adopting the view of an information system as constituted of the technical, formal and informal (TFI) parts. The aim is to increase the understanding of the information security domain in order to develop a well-founded theoretical framework, which can be used both in the analysis and the design phase of interoperable systems. Finally, we describe and apply the Information Security (InfoSec) model to the results of three different case studies in the healthcare domain. Limits of the model will be highlighted and an extension will be proposed.

1 Introduction

In the information society, security of information plays a central role in several domains with different scopes and objectives: Privacy of personal data in healthcare; Integrity of transaction and business continuity in the business domain; Safeguard of citizens in the infrastructure domain; and Defence of democracy in the e-government

Please use the following format when citing this chapter:

Åhlfeldt, R.-M., Spagnoletti, P., and Sindre, G., 2007, in IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, eds. Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., (Boston: Springer), pp. 73–84.

domain, are some examples of such objectives. In the last decades, due to the spread of Information and Communication Technologies (ICT), governmental organisations and communities of academics and practitioners have developed security models for evaluating products, and setting up security specifications in order to prevent incidents and reducing the risk of harm.

Many different terms have been used to describe security in the IT/IS area. *Information security* has become a commonly used concept, and is a broader term than data security and IT security [1]. Information is dependent on data as a carrier and on IT as a tool to manage the information; hence, information security has an organizational focus [2].

The Swedish National Encyclopedia [3] states that information security is focused on information that the data represent, and on related protection requirements. The U.S. National Information Systems Security Glossary [4] defines information system security as: "the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats". Four characteristics of information security are: availability, confidentiality, integrity and accountability, simplified as "the right information to the right people in the right time" [5]. The Swedish Standardization of Information Technology (SIS) advocates that information security concerns the protection of information assets, aiming to maintain confidentiality, integrity, availability and accountability of information [6].

Availability concerns the expected use of resources within the desired time frame. *Confidentiality* relates to data not being accessible or revealed to unauthorized people. *Integrity* concerns protection against undesired changes. *Accountability* refers to the ability of distinctly deriving performed operations from an individual. Both technical and administrative security measures are required to achieve these four characteristics. *Administrative security* concerns the management of information security; strategies, policies, risk assessments, education etc. Planning and implementation of security requires a structured way of working. This part of the overall security is at an organizational level and concerns the business as a whole.

Technical security concerns measures to be taken in order to achieve the overall requirements, and is subdivided into physical security and IT security. *Physical security* is about physical protection of information, e.g. fire protection and alarm systems. *IT-security* refers to security for information in technical information systems and can be subdivided into computer- and communication security. *Computer Security* relates to the protection of hardware and its contents, e.g. encryption and backup techniques. *Communication Security* involves the protection of networks and other media that communicate information between computers, e.g. firewalls.

In order to provide a more understandable view of how information security characteristics and security measures relate to one another, an information security model (Fig. 1) has been created based on the common characteristics of information security and SIS classification of information security measures [6]. The aim of the model is to describe what information security represents both in terms of characteristics and measures, combining the definitions and descriptions mentioned above.

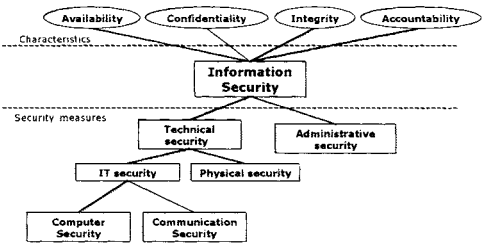

Fig. 1. Information Security Model (InfoSec model)

The main concept "information security" is presented in the middle. The four characteristics together represent information security, and are placed at the top of the figure. All requirements from the organizations concerning these characteristics must be fulfilled for information security to be achieved. The lower part of the model presents the different security measures, divided in a hierarchical order and these are gathered directly from the SIS conceptual classification [6]. Since the term "information security" includes several parts of security measures, the model has been useful both in the research and the educational area, in order to get an understanding of information security and its content. Furthermore, the model has been used as a tool in the research area to express where the problems and needs exist in the information security area [7].

In Figure 1, administrative security is not subdivided, but a case study in the distributed healthcare domain has shown that there is a need to improve the model with a more fine-grained understanding of administrative issues [7]. One way to improve the InfoSec model is to look at other security standards, methods and models in order to discover solutions to extend the InfoSec model.

The aim of the paper is to present the suggested extended InfoSec model by using concepts derived from a semiotic model (TFI) in order to increase the understanding of the information security domain and to develop a well founded theoretical framework which can be used both in the analysis and the design phase of interoperable systems. The results from three different case studies have been drawn upon in order to show the limitations of the current model and to validate the extended model.

Our contribution aims to provide a theoretically founded and empirically tested information security model for the analysis of Information Systems and its context. In this model both the IT infrastructure and the more contextual related aspects related to organizational culture and human behavior are taken in to account in order to enlarge the scope of the analysis and to select countermeasures with a holistic view on information security.

The next section presents related work, describes the TFI-model and argues for its appropriateness. In section 3 the results from three case studies are described, highlighting the limitations of the information security model. In section 4 we present a suggestion for an extended InfoSec model and the same results from the case studies are compared with the model in order to validate its extension. Finally, section 5 concludes the paper.

2 Related work

The harmonisation of the North American (TCSEC commonly known as Orange Book) and European (ITSEC) criteria for IT security evaluations led, at the end of the 1990s, to the definition of a common set of criteria (Common Criteria) for use in evaluating products and systems and for stating security requirements in a standardised way. The International Standard Organisation accepted these criteria in the ISO15408-1999. These standards define the IT product or system under evaluation as a Target of Evaluation (TOE). TOEs include, for example, operating systems, computer networks, distributed systems, and applications.

Additional standards and models were developed by other national and international organizations taking into account the abovementioned works and more context specific issues. The European Computer Manufacturers Association, ECMA, wanted to achieve a widely accepted basic security functionality class for commercial applications, defining the "Commercially Oriented Functionality Class" (COFC) and afterwards the Extended Commercially Oriented Functionality Class (E - COFC), which extends the application of ECMA's class of commercial security functions to an environment of interconnected IT systems.

These standards consider "administrative security measures" outside the scope of security evaluation criteria "because they involve specialized techniques or because they are somewhat peripheral to IT security" (CC, Introduction and general model). Despite they recognize that a significant part of the security of a TOE can often be achieved through administrative measures such as organizational, personnel, physical, and procedural controls, they chose to focus on IT security measures and they start from the assumption of a secure use of IT systems and products.

A different approach to the security of information can be found in the Code of Practice BS7799, recently accepted by the ISO in the ISO/IEC 27000 family In this case the processing of information assumes a central role and the focus is on the management of information security instead of the design of secure IT systems and products. This approach considers security of information as a quality sub-factor and provides a set of controls to be put in place in order to deploy an information security management system based on a "plan-do-check-act" cycle similar to the ISO 9000 for quality management. Another quality management based approach to information security comes from Firesmith [8] who defines taxonomy of security-related requirements based on the safety requirements of a system.

This brief overview of security standards shows that the focus of security models, standards and best practices, has moved from considering security as an intrinsic feature of IT systems and products towards a wider vision including the processing of information and the related management issues such as roles and responsibilities. Starting from well-known principles and standards, some authors [9] use layered models to classify security controls and to describe security models. For instance at the top level there is the organization policy with respect to security, followed by specific corporate programs to promote security and finally technical controls. A step forward with respect to these approaches can be to focus on more context-related aspects such as organizational culture and human behavior instead of technology and processes. To this end, starting from the above mentioned InfoSec model, we propose an extension based on concepts derived from a semiotic model. Adopting this view makes it possible to

better understand all those context specific aspects that can be difficult to analyze using generalized risk management techniques.

2.1 The TFI model

Adopting the view of an information system as constituted of the technical, formal and informal (TFI) parts which are in a state of continuous interaction [10], the need for an holistic approach to the study of IS security becomes apparent. Using the words of Stamper et al [11] is possible to illustrate this interrelation of abstracted layers explaining that, "Informal norms are fundamental, because formal norms can only operate by virtue of the informal norms needed to interpret them, while technical norms can play no role...unless embedded within a system of formal norm." In other words, the informal ways of managing information in organisations are critical and not always they can be replaced by rules or embedded in technical systems. With this view the informal elements (i.e. perception of risks, awareness, beliefs, culture, etc.), which are very context related, should drive the design and the selection of formal (policies, business processes, standards, procedures, etc.) and technical solutions (i.e. software and hardware platforms, network infrastructures, devices, etc.). In the context of information systems crossing the boundaries of a single organization (i.e. virtual organizations and other interoperable systems), the relationship among these three levels is even more complex and requires to address additional issues such as trust and privacy by the means of new formal and informal mechanisms (i.e. Circle of Trust, federated Identity Management Systems, etc.).

The above mentioned conceptual framework, based on semiotic theory, will be one of the assumptions behind all the subsequent discussion on IS security management. Furthermore we agree with Dhillon's [12] assumption by viewing problems as an emergent property of reflexive interaction between a system and its context, instead of considering them as a consequence of a system's function.

These premises give an idea of the complexity implicit in preventing, detecting, investigating and responding to incidents, using deterministic methods, when different organizational contexts are involved. This complexity is a serious challenge for the design phase of Information Security Management Systems (ISMS) when organizations with different security models in terms of people, rules and technology need to cooperate. Indeed information security can be considered a critical non-functional requirement when inter-organizational interoperability is pursued.

IS security is a wide field and contributions come from several disciplines such as mathematics, engineering, and social and management sciences. In this section we briefly introduce some of the contributions to the IS security literature in order to clarify the differences among the three levels [13]: *(1) technical*: automating and standardizing parts of formal systems such as computers helping in operational tasks; *(2) formal*: organizational level security mechanisms like governance, policies or processes, such as establishing controls in structure of organization and *(3) informal*: individual level security mechanisms, like shaping the norms, beliefs, values, and attitudes of employees, such as establishing normative controls.

Technical level security. From a technical perspective, the preservation of confidentiality, integrity availability and accountability requires the adoption of IT security solutions such as encryption of data and communication, physical

eavesdropping, access control systems, secure code programming, authorisation and authentication mechanisms, database security mechanisms, intrusion detection systems, firewalls, etc. At this level it is possible to introduce models and methods for the selection of the appropriate technological solution depending on the needs for a particular application.

Formal level security. The formal level of IS security is related with the set of policies, rules, controls, standards, etc. aimed to define an interface between the technological subsystem (Technical level) and the behavioural subsystem (Informal level). According with Lee's definition of an IS [14], this is the level where much of the effort of the IS management is concentrated. An interesting review of the security literature identifies a trend in information system research moving away from a narrow technical viewpoint towards a socio-organisational perspective [15]. In fact the first methods for addressing security at this level are checklist, risk analysis and evaluation. At the beginning such methods have been grounded in particular well-defined reality (i.e. military), focusing on a functionalist view of reality. However Dhillon and Backhouse [15] show that the definition of rules, standards and controls becomes more complicated than the design of technical systems.

Informal level security. In the domain of the informal level of IS security, the unit of analysis is individual and the research is concerned about behavioural issues like values, attitude, beliefs, and norms that are dominant, and influencing an individual employee regarding security practices in an organization. The solutions suggested in this domain are more descriptive than prescriptive in nature and the findings at this level need to be effectively implemented through other levels (i.e. formal and technical). An interesting review of research papers in the behavioural domain, looking at used theories, suggested solutions, current challenges, and future research has been presented by Harris and Mishra [13].

This approach helps in the management of insider threats. Numerous studies [16-20] have indicated that there is a problem in managing information security especially with respect to controlling the behavior of internal employees. Research has also shown that many times internal employees subvert existing controls in order to gain undue advantage essentially because either an opportunity exists to do so or they are disgruntled [21]. The problem gets compounded even further when an organization is geographically dispersed and it becomes difficult to institute the necessary formal controls [22].

Also the prevention of social engineering attacks deals with the informal level of information security. According with Jones [23], while the typical hacker "takes more advantage of holes in security," the social engineer manipulates personnel to gain information that would not normally be available, such as passwords, user IDs, or even corporate directories. In effect, social engineering is typically employed by hackers as a means to acquire information that would be extremely difficult to obtain through strictly technical means. Unlike hacking, social engineering taps into the psychology of what people expect from others and their natural tendency to be helpful. Therefore technical barriers and rigid rules are not sufficient to contrast these threats if people are not aware of the security risks.

3 Extended InfoSec model based on TFI

One way to extend the InfoSec model in its administrative part is to use the elements of the TFI-model; formal and informal. Administrative security concerns information security management, which can be both formal and informal. According to chapter 2, the formal element includes policies, rules controls, standards etc aimed to define an interface between the technological subsystems while the informal element includes the aspects related to the human behaviour. This seems to be in conjunction with the security area too. Also Björck [24] has declared this division of information security when he classifies some written papers from the security areas. He divides them into technical, formal and informal parts. He also concludes that information security papers mostly concern technical aspects while there is a further need of research in the formal level but above all, the informal level has been neglected. One important element in this level is to make the users security aware. Concerning the formal part it seems to be natural to subdivide this part into external and internal levels. Each organisation is subject to external regulations concerning security issues, for instance, laws, regulations and agreements with other companies. Furthermore, there is internal formalism for information security management, such as IT-strategies, security polices, educational programs etc. According to Lee [14] this is the level where much of the effort of the information security management is concentrated. Hence, we have extended the InfoSec model as depicted in Figure 2.

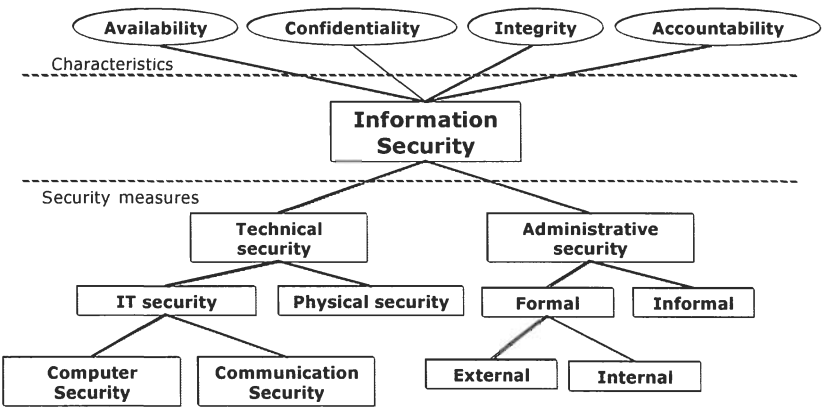

Fig. 2. Suggestion for an extended InfoSec model

4 Evaluating the new InfoSec Model

In this section we present the case studies and apply a summary of the results to the new extended model in order to illustrate its usefulness. It is beyond the scope of this paper to describe the specific case studies in huge detail, this can be found in referenced papers. However, a brief description is presented in this section.

4.1 The applied case studies

The first case study [25] was conducted in the home healthcare of two municipalities. The focus in this case study was patient privacy and information from the Swedish Data Inspection Board (DIB) was used as a basis for the interviews with the responsible persons and the healthcare staff working in home healthcare. Observations were also carried out in order to obtain an idea of how personal data is managed by following the healthcare staff in their work.

The second case study [26] includes observations and interviews with healthcare staff at a hospital in the western region of Sweden. The aim of the study was to determine how users of EHR are affected by the requirements of information security, as well as how the users themselves affect information security and in what way they follow the recommendations and advice of the Swedish DIB.

The third case study was performed as part of the VITA Nova Hemma research project [27]. In this research project different healthcare providers participated in order to investigate how a process manager can be used to support a leg ulcer process. This process connects different healthcare actors: primary care, secondary care and municipalities [28, 29]. Part of the case study included a system analysis of different security aspects for the involved healthcare systems. Interviews were held with administrators for the respective healthcare systems. A second part included further studies of the healthcare organizations' systems and networks. The suppliers of the patient record systems and the people responsible for the communication networks in the included healthcare organizations were interviewed. The basis for the questions in the security analysis was the ISO-standard ISO/IEC 17799 Information Security Management [30].

The results are briefly summarized: *IT-security* - inadequate logon functions in both systems and networks. *Computer Security* - inadequate access profiles levels. *Communication security* - facsimiles as a communication transmitter, interruptions in the networks, inadequate authentications techniques and security measures concerning mobility. *Administrative security* - missing IT-strategies and information security polices, inadequate education in information security, no compliance and follow up, inadequate security awareness and attitudes, inadequate security routines, and missing security requirements.

The results from the case studies are presented in Figure 3a and show a number of problems and needs in the different levels of security. The symbols refer to the results for specific case studies, for instance, 1a refers to case study 1 and the results noted a in that particular case. It is out of the scope of this paper to analyse the particular result. Instead we focus on the structure of the problems and needs. The results show that there is a cluster of problems and needs in the administrative security area. In comparison with the technical security this part will be hard to express in more detail, and there is no balance concerning the graphical illustration between the technical and administrative level. One reason could be that technical measures have got higher priority and have been in focus for a longer period of time. Therefore it is necessary to further detail the administrative part of the information security model as well, and thus get an improved view of where problems and needs are located within administrative security.

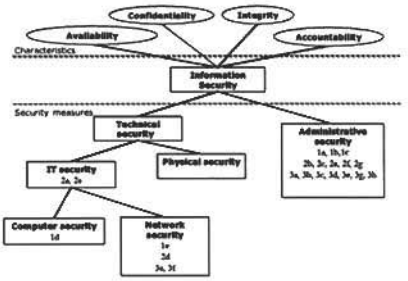

Fig. 3a: Needs in healthcare. extended InfoSec model

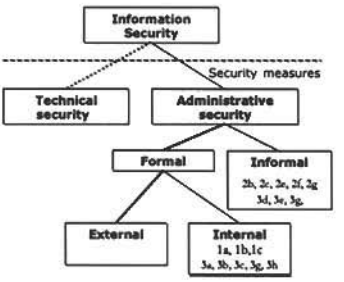

Fig. 3b: Corresponding results in the

One approach is to apply the results shown in Figure 3a to the extended InfoSec model. The result at the administrative security level has been classified according to the new levels of administrative security: formal and informal. The formal issues have been further classified as external and internal. The result of this classification is shown in Figure 3b and should be compared with results from Figure 3a.

The result shows that our case studies exhibit both formal and informal problems and needs. However, in the formal part, there are no reported problems in the formal external level. This does not imply that there are no problems in this area, however. Other investigations reveal problems at this level, concerning for instance legislation contradiction [31]. It is reasonable to assume that the problem was not mentioned in our case studies since other more internal problems impact the respondents' daily work more directly. Another formal external problem could be e-contracting. In the healthcare area, no such contracting is applied yet, and therefore no such problems have been identified. In the future when different healthcare performers will exchange patient information, some kind of contracting may very well be implemented, and may hence also become a security problem in this level.

An interesting finding is that if the InfoSec model had included external administrative security from the beginning, the interviewer could have asked more direct questions for the formal external purposes. Instead, the administrative part alone was in focus, causing the questions to be rather abstract. This also shows that the extended model could be of great use in order to emphasize the whole of the information security area, and the administrative security level in particular.

In the informal part we find problems like inadequate security awareness and attitudes but also missing measures for compliance and follow up activities. Technical solutions are quite easy to implement. Formal administrative solutions can be considered a rigid task to perform but is in fact attainable. The main challenge for information security in the future is to implement useful methods to achieve security awareness in organisations. According to Valentine: "Employee security awareness programs need to begin growing out of their infancy and be treated with as much attention to detail as any other information security engagement" [32].

5 Discussion and Conclusion

We have shown how the InfoSec model can be extended by using elements from the TFI model. The administrative part in the InfoSec model has been subdivided into formal and informal security. The formal part has been further subdivided into external and internal parts. Our main contributions include showing how the extended InfoSec model can be of great use in order to emphasize a more holistic view of the information security area, and the administrative security level in particular. The model also visualises more specifically within what areas information security measures need to be taken into account.

The case studies presented in this paper, indicated no external problems and needs in the formal part of information security. We do not claim that all external regulations and legalisation issues have been taken to account or that there are no problems concerning the external part. This investigation of external issues has just not been in focus. In the internal formal part, there is a need for information strategies and information security policies strongly related to context or the type of domains such as healthcare, military and business sectors. The internal rules, instructions and education should emerge after defining the policies. In the informal part there is also a need for measures to support the organisation in implementing information security awareness. This is not a simple task, but is very important in order to reach sufficient information security within the whole organisation.

One weakness in this paper is that only one single investigation has been used to evaluate the extended InfoSec model. Future work must evaluate the model in other studies as well, both theoretically and practically, in order to establish its usefulness.

Furthermore, we need to investigate how to construct context-related strategies and polices. A risk management methodology which takes behaviour and cultural aspects into account is needed to improve security awareness. The extended Info Sec model has a holistic approach and can therefore be a helpful tool to bring informal issues into account, why such a risk management methodology should be based on our model, especially in the asset identification phase (physical asset but also value of information for the stakeholders) and also in the control selection phase.

The need for formalisation in the design phase of information systems development is moving towards the use of semantic technologies and ontologies. Future research should therefore evaluate the extended model in other domains. In the INTEROP project and the task group of non-functional aspects in particular, some related work is on-going which may enable a broader evaluation. The extended model should be seen as a semantic model in order to be a useful support in different areas to include the information security issues.

References

1. Björck, F., 2005a. Knowledge Security [on line]. Available from: http://www.bjorck.com/3.htm [Accessed 1 November, 2005].
2. Oscarsson, P., 2002. Information Security, Data Security, IT Security, Computer Security, IS Security ... - What Makes the Difference? In Proceedings of Promote IT, pp. 649-655. Skövde, Sweden. 22-24 April 2002.

3. NE 2005. National Encyclopedia [on-line]. Available from: http://www.ne.se [Accessed 28 October 2005].
4. U.S. National Information Systems Security Glossary, 2006. Available from: http://security.isu.edu/pdf/4009.pdf [Accessed 25 October 2006].
5. Wikipedia, 2006. Information Security. Available from: http://www.wikipedia.com [Accessed 29 May, 2006].
6. SIS, 2003. SIS Handbok 550. Terminologi för informationssäkerhet. SIS Förlag AB. Stockholm (in Swedish).
7. Åhlfeldt, R-M., 2006. Information Security in a Distributed Healthcare Domain – Exploring the Problems and Needs of Different Healthcare Providers. Licentiate Dissertation. Report series No. 06-003. ISSN 1101-8526.
8. Firesmith D.G., 2005. "Analyzing the Security Significance of System Requirements," Requirements Engineering'2005 (RE'05) Symposium on Requirements Engineering for Information Security (SREIS), IEEE Computer Society, Washington, D.C., September 2005.
9. Jain, A. & Raja, M K 2006. An Exploratory Assessment of Information Security Principles & Practices: An Insight from a Financial Services company, Proceedings of the 5th Security Conference, Las Vegas.
10. Liebenau and Backhouse 1990 Understanding Information: an Introduction, Macmillan, London
11. Stamper R., Liu K., Hafkamp M. and Ades Y. 2000 Understanding the Roles of Signs and Norms in Organisations - A semiotic approach to information systems design. Journal of Behaviour & Information Technology, vol. 19 (1), pp 15-27.
12. Dhillon, G. 1997. Managing information system security. London: Macmillan.
13. Harris, M. & Mishra, S. 2006 Human Behavior Aspects in Information Systems Security. Proceedings of the 5th Security Conference, Las Vegas.
14. Lee, A.S. (1999). Inaugural Editor's Comments, MIS Quarterly, 23(1), v-xi.
15. Dhillon, G. and Backhouse J. 2001 Current Directions in IS Security Research: Toward Socio-Organisational Perspectives. Information Systems Journal 11(2): 127-153.
16. Siponen M.T. 2000 "A Conceptual Foundation for Organizational Information Security Awareness", Information Management & Computer Security, 11 (1), pp. 31-41.
17. Whitman, M. 2003. "Enemy at the Gate: Threats to Information Security." Communications of the ACM 46(8): 91-95.
18. Bottom, N. 2000. "The human face of information loss." Security Management 44(6):50-56.
19. Magklaras, G. and S. Furnell 2005. "A preliminary model of end user sophistication for insider threat prediction in IT systems." Computers & Security 24: 371-380.
20. Schultz, E. 2002. A framework for understanding and predicting insider attacks. Compsec, London.
21. Dhillon, G., & Backhouse, J. 1997. Managing for secure organizations: a review of information systems security research approaches. In D. Avison (Ed.), Key issues in information systems: McGraw Hill.
22. Dhillon, G. 2000 Challenges in Managing IS Security in the new Millennium, Chapter 1 of Challenges in Managing Information Security, Idea Group Publishing.

23. Jones, C. 2003 The Social Engineering: Understanding and Auditing [Online]. SANS Institute. Available from: http://www.sans.org/rr/whitepapers/engineering/1332.php [Accessed Nov 01 2005].
24. Björck, F. 2005b Discovering Information Security Management. PhD Dissertation. University of Stockholm. Report series No. 05-010, Stockholm.
25. Åhlfeldt, R. 2002. Information Security in Home Healthcare: A Case Study, In the *Conference Proceedings of the Third International Conference of the Australian Institute of Computer Ethics (AiCE) 2002*. Sydney, Australia, 30 September 2002, pp. 1-10. Eds. M. Warren and J. Barlow. Australian Institute of Computer Ethics. ISBN 0-7300-2560-8.
26. Åhlfeldt, R. and Ask, L. 2004. Information Security in Electronic Medical Records: A case study with the user in focus. In *Proceedings of the 2004 Information Resources Management Association International Conference*, New Orleans, USA, May, pp 345 – 347.
27. Åhlfeldt, R. and Nohlberg, M. 2005. System and Network Security in a Heterogeneous Healthcare Domain: A Case Study. In *CD-ROM Proceedings of the 4th Security Conference, Las Vegas, USA, 30–31 March 2005*. ISBN 0-9729562-5-5.
28. Perjons, E., Wangler, B., Wäyrynen, J. and Åhlfeldt, R. 2005a. Introducing a process manager in healthcare: an experience report, *Health Informatics Journal*, Vol 11(1), 45-61, March 2005. ISSN 1460-4582.
29. Johannesson, P., Perjons, E., Wangler, B. and Åhlfeldt, R-M. 2005. Design Solutions for Interoperability using a Process Manager. In Proceedings of the 1th International Conference on Interoperability of Enterprise Software and Applications (INTEROP-ESA'2005), Geneva, Switzerland, 23 – 25 February 2005, pp 397-408. ISBN 13-978-1-84628-151-8
30. ISO/IEC 17799 Part 1: Code of practice for information security management.
31. Nationell IT-strategi för vård och omsorg. 2006. ISBN 91-631-8541-5 (in Swedish).
32. Valentine, A., 2006 "Enhancing the employee security awareness model", Computer Fraud & Security, June 2006, pp 17-19.