Information Security Management: A Collaborative Approach

F. Innerhofer-Oberperfler[a] D. Bachlechner[b] R. Maier[b]
V. Hahn[a] M. Weitlaner[a] and R. Breu[a]

[a] *Research Group Quality Engineering, Institute of Computer Science, University of Innsbruck, A-6020 Innsbruck, Austria*

[b] *Information Systems I, Innsbruck University School of Management, University of Innsbruck, A-6020 Innsbruck, Austria*

Abstract

Information is a valuable asset and critical for the survival of organisations in today's globalised digital economy. To ensure adequate security of an organisation's information, rules of conduct must be established and responsibilities must be shared among the stakeholders involved in activities related to information security management. A variety of requirements – ranging from legal regulations to compliance with organisational policies to securing critical information assets – stems from numerous stakeholders with different, sometimes contradictory interests. In order to tackle this challenge, a systematic approach is needed that takes into account the inherently distributed character of information security management. In this paper, we outline our vision of collaborative information security management and discuss tasks that have to be performed in order to realise a corresponding approach in form of an information system supporting collaborative information security management. Within the scope of the discussion, we focus on organisational issues at first and then proceed to technical issues. With respect to organisational issues, we discuss activities, roles and responsibilities related to information security management as well as the information demand, supply and representation. With respect to the technical realisation of the proposed approach, we discuss the development of a security information model and the creation of consistency rules and checks. Subsequently, we describe the design of a security information lifecycle and its integration into the model.

Keywords: Information Security, Security Management, Collaboration, Information Lifecycle, Stakeholder

1 Introduction

Information assets are seen as production factor or competitive factor in organisations and thus their protection can be seen as a necessity for operative management. Security and risk management have long been recognised as integral parts of management but companies have embraced this topic only recently as consequence of various influences (e.g. dynamic environments, networked IT infrastructures, prominent bankruptcies, spectacular cases of disclosure of information and subsequent regulations). Despite the long acknowledged importance of information assets, it is only recently that information security management (ISM) has been systematically conceptualised to cover all aspects of handling information in organisations, not only limited to objects such as hardware, system software and activities of IT security performed by specialists within IT units.

ISM includes all activities and controls related to the preservation of confidentiality, integrity and availability of information and continues to be a hot topic on the agendas of executives in many organisations [24]. The standard ISO 27001 defines an information security management system (ISMS) as a *part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.* According to this widespread definition, an ISMS comprises an organisational and a technical subsystem.

According to the standard ISO 27002, ISM requires the participation of all employees in an organisation and also involves external parties such as shareholders, suppliers and customers. This participative aspect is of particular importance for the successful implementation of an ISMS [27]. From our point of view, the next major step with respect to the improvement of ISM is the move from participation to collaboration.

In this paper, we put particular emphasis on the collaborative aspect of ISM and report on the results made in an ongoing research endeavour which focuses on important issues related to this aspect. While the general goal is the analysis and development of practices, concepts, methods and tools supporting collaborative ISM, this paper presents a model-based framework for ISM that aims at bridging organisational and technical perspectives, and extends existing frameworks in order to better support the collaborative aspect of ISM.

Section 2 motivates our work and describes the state-of-the-art as well as major challenges in the field of ISM. Section 3 sketches our vision. On the basis of a collection of challenges, we develop a set of tasks to be performed in order to support collaborative ISM. Section 4 outlines our approach from an organisational and a technical perspective, respectively. In Section 5, we describe related work and in Section 6, we conclude with an outlook on future work.

2 Motivation

The Global Information Security Survey [12] published by Ernst & Young in 2008 states that information security standards are increasingly adopted by organisations. The use of the standards ISO 27001 and ISO 27002 increased by 15% and 9%, respectively, over the year 2007. These standards provide guidelines, best practices and a foundation for the certification of organisations implementing an ISMS. Also other IT related standards such as COBIT and ITIL include sections on ISM.

In many organisations, particularly in large ones, the strategic and operative responsibility for ISM lies in the hands of a Chief Information Security Officer (CISO). The Deloitte 6th Annual Global Security Survey [9] reports that in 2008, 80% of the surveyed financial institutions had at least one CISO. However, the study The Global State of Information Security [24] by PricewaterhouseCoopers claims that in other industries (e.g. consumer products and retail) the percentage of organisations with a CISO is clearly lower. According to these surveys, the activities of a CISO are generally of a cross-departmental nature and, among others, comprise the development of strategic guidelines and concrete operative specifications.

A CISO is typically dependent on many stakeholders in an organisation. The

Facilitated Risk Analysis Process (FRAP) [23] emphasises this involvement of different stakeholders. Also the OCTAVE approach [1] focuses on a series of methods to elicit the knowledge of experts and stakeholders in an organisation. Effective ISM thus requires collaboration among stakeholders such as senior managers, IT security professionals and system engineers [13].

Collaborative security and network management are increasingly embraced by organisations [14]. Deloitte's survey also claims that functional executives and business line staff are increasingly involved in every area with regard to information security strategy [9]. The survey also reports that since 2007, there has been a notable increase with respect to the adoption of a federated model for ISM.

The increasing collaboration among central security functions, organisational units and experts possessing specific know-how, indicates that ISM is distributed among different stakeholders [5]. The distribution of the activities of ISM and the implementation of a collaborative ISMS require the consideration of the following challenges. Here, we mainly discuss the challenges related to ISM that focus on communication and coordination issues. Based on them, we elaborate a set of tasks to be performed in order to realise an approach corresponding to our vision.

One of the challenges observed in the context of ISM concerns the communication difficulties arising from the collaboration of stakeholders with different backgrounds. A recent survey shows that business managers and information security professionals approach information security issues in different ways [26]. The different perspectives on information security are, among others, a matter of different levels of abstraction. A solely technical perspective is surely too narrow [11].

The coordinative efforts required for the adoption of a collaborative approach to ISM represents another important challenge. The collaboration among different stakeholders needs to be supported by a variety of coordination instruments such as frameworks, architectures and models which must be adaptable to organisation-specific characteristics [25]. Another study points out the need to support collaboration with appropriate tools [5]. Such tools have to support the collaboration among stakeholders with different levels and scopes of expertise and the supervisory control by the CISO. According to the study, this requires an entirely new class of tools which takes organisational aspects into account and provides technical solutions supporting collaborative ISM.

3 Vision

In Sections 3.1 and 3.2, we define the scope of our vision and sketch the concept behind it, respectively. In Section 3.3, a path to the realisation of our vision is pictured.

3.1 Scope

The approach presented in this paper focuses primarily on aspects of collaboration within organisations. The term collaborative security management is often used to refer to ISM that goes beyond the borders of an organisation [1]. External parties that play important roles with regard to information security are, for instance,

security consultants, auditors and other service providers. However, our primary interest lies on the collaboration within organisations (i.e. between organisational units). Within the scope of our research, we look at collaborative ISM from an organisational and a technical perspective.

3.2 Concept

A collaborative approach to ISM seeks commitment from different stakeholders and increases their involvement and contribution. To foster the effectiveness of ISM, the activities have to be distributed and coordinated. The stakeholders play different roles with respect to ISM and take over the responsibilities accruing from their roles. The stakeholders typically have diverse backgrounds and focus on different levels of abstraction. Therefore, a collaborative ISM needs to take different points of view into account and provide appropriate perspectives to cover the requirements of the stakeholders involved. Another important aspect that has to be addressed by collaborative ISM is the support of the communication among the stakeholders.

Within the scope of collaborative ISM, different stakeholders fulfil their responsibilities in parallel. For this purpose, stakeholders need to consider information from other stakeholders who are responsible for related activities. At the same time, it has to be possible to monitor the status of an organisation's information security centrally in an aggregated way but also decentrally in a disaggregated way. The information security status includes an overview of an organisation's security policies, an aggregated view on the results of risk analyses and a summary of the controls selected for implementation. In addition, the information security status reflects the performance and progress of ISM. Thus, the information security status of an organisation provides a foundation for the monitoring and supervisory control of ISM. Based on the state of security information which is processed in the information system supporting collaborative ISM, decisions with respect to current and future activities can be made. A prerequisite for the provision of an information security status is the collection and consolidation of security-related information.

3.3 Realisation

In order to realise our vision, several tasks have to be performed. The tasks can be classified into two categories (cf. Figure 1). On the one hand, the collaborative aspects of ISM have to be analysed from an organisational perspective and on the other hand, a technical point of view is needed to focus on the engineering aspects targeted to the realisation of our vision of collaborative ISM.

We have identified the following list of tasks to be performed based on a review of the literature, particularly empirical studies, as well as a series of interviews with ISM practitioners. From our point of view, engaging with them is critical in order to provide new classes of tools to support ISM as sketched recently [5]. The organisational perspective includes the following four tasks (O.1-O.4) and focuses on the delivery of models and concepts to describe collaborative ISM:

O.1: Analysis of activities An overview of activities related to ISM has to be elaborated. At the same time, the distribution of these activities among different stakeholders has to be taken into account.

O.2: Definition of roles and responsibilities In parallel with the analysis of activities, the roles of the various stakeholders and the corresponding responsibilities have to be defined.

O.3: Determination of information demand and supply Based on the analysis of activities and the definition of roles and responsibilities, it has to be determined who requests and possesses what type of information.

O.4: Representation of information and means of communication The representation of information and means of communication have to be adapted to the stakeholders' preferences and points of view.

The following four tasks (T.1-T.4) are associated with the technical perspective and focus on the delivery of technical solutions which foster the implementation of the developed models and concepts of collaborative ISM:

T.1: Creation of a security information model The security information which is generated, collected and processed as part of ongoing ISM activities has to be consolidated in form of a model.

T.2: Development of consistency rules and checks To keep the model consistent, sets of rules and checks have to be developed. Such mechanisms are of particular importance in collaborative environments.

T.3: Design of a security information lifecycle The information held in the security information model undergoes several transitions. Therefore, an individual lifecycle has to be designed for every type of information.

T.4: Analysis of lifecycle phases The lifecycle phase of a piece of information is interrelated with the values of the corresponding model element's status attributes. The aggregation of such status attributes provides a foundation for the supervision, control and distribution of ISM activities.

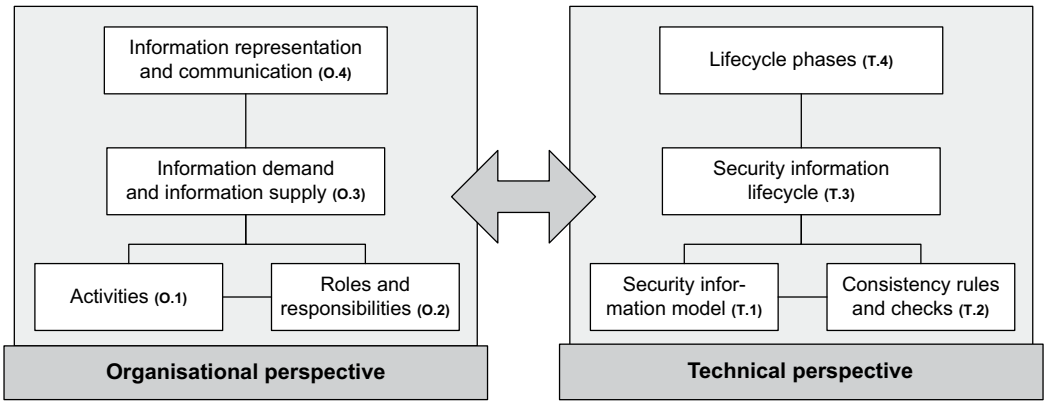

Fig. 1. Relationships among the tasks assigned to the organisational and the technical perspective, respectively

4 Approach

In Section 4.1, we describe the analysis of activities related to ISM (O.1) as well as the definition of roles and responsibilities (O.2). The determination of information

demand and supply (O.3), the representation of information, and means of communication (both O.4) are discussed in Section 4.2. In Section 4.3, the creation of a security information model (T.1) and the development of consistency rules and checks (T.2) are presented. Finally, in Section 4.4, we describe the design of security information lifecycles (T.3) and the analysis of their respective phases (T.4).

4.1 Activities, roles and responsibilities

It is quite obvious that in order to support collaborative ISM, it is necessary to understand the core activities associated with ISM (O.1). Within the scope of international and national information security standards and guidelines, experts from academia and practitioners classified the core processes related to ISM and identified the underlying activities. Based on the analysis of the activities related to ISM as well as other sources, the roles and responsibilities in the context of ISM were investigated.

The standard ISO 13335 includes a set of guidelines for the management of IT security, focusing primarily on technical security control measures. The ISO 27000 family of standards includes ISM standards derived from British Standard BS 7799. We identified the essential activities related to ISM primarily on the basis of those two standards. A classification into five categories seems to be well-suited for further analyses:

Development of a corporate information security policy Organisations can hardly assure a corporate level of information security, if they lack a corporate information security policy. The objective of the information security policy is to provide decision makers direction and support with respect to ISM in accordance with organisational requirements and relevant laws and regulations. Respective activities predominantly relate to the compilation, communication and revision of the information security policy.

Implementation of risk analyses The set of activities associated with the implementation of risk analyses depends on the adapted risk analysis strategy. However, organisations typically follow a strategy combining the baseline security approach with the implementation of elaborate risk analyses in selected cases. Activities associated with this category concentrate on the security requirements analysis, the actual risk analyses and the acceptance of individual residual risks.

Compilation of a security plan A security plan helps to mitigate risks to an acceptable level. Essential activities relate to the selection of controls that make the associated residual risks acceptable. Besides that, respective activities predominantly relate to the compilation and revision of security policies and the security plan. While security policies concretise the rather abstract corporate information security policy with respect to particular information security areas (e.g. a data storage policy), a security plan regulates certain aspects with respect to the implementation of controls (e.g. priorities, resources).

Implementation of the security plan When implementing the security plan, particular emphasis has to be put on awareness and training programmes. Related activities also include the measurement of the effectiveness of the implemented controls. Finally, when new IT systems are acquired, it has to be verified that

they meet the corporate information security policy as well as the more specific security policies.

Maintenance of information security over time In order to keep a specified level of information security, changes with respect to the information security requirements of the organisation (e.g. changes of regulatory frameworks) as well as changes in the organisation itself (e.g. changes of the IT infrastructure or the development of new operational segments) have to be identified and treated. Furthermore, activities related to the handling of actual incidents also belong to this category of activities.

The results of the analysis of information security standards and guidelines are currently being reviewed for their practical appropriateness by means of a series of expert interviews. The preliminary results of the study not only confirm the relevance of the identified activities but also allow drawing conclusions on aspects such as relative importance, stakeholders involved and tools applied.

A collaborative execution and delegation of the types of activities outlined above requires the identification of involved stakeholders and the assignment of them to specific roles according to their responsibilities. To perform this task (O.2), the involved stakeholders are identified in a first step. This is done by reviewing literature, existing role models and organisational ISM models. So far, we have identified the following basic types of stakeholders participating in ISM:

Organisational units ISM happens in a distributed way and effects organisational units all over the organisation [8]. The organisational unit that supervises ISM needs active contribution from other units such as Human Resources, the legal or the financial department.

Persons Business managers who are knowledgeable about IT can provide value to an organisation and they can give impetus to ISM [8]. For effective ISM, the specific know-how of several persons such as security specialists, technical specialists and functional specialists in an organisation needs to be tapped.

Technical components Examples of technical components are infrastructure monitoring solutions, firewalls, access control systems and intrusion detection systems. These technical components are stakeholders in the sense that they provide a wealth of useful security information for ISM. At the same time, they also require configuration parameters as input to fulfil the tasks assigned to them.

In a second step, the final results of the literature review focusing on the identification of different types of stakeholders will be compared with the results of the expert interviews which provide an overview of the roles and responsibilities in practice. For an effective delegation of responsibilities and the assignment of roles to the stakeholders, suitable criteria need to be developed. So far, we have identified the following criteria based on recent literature [5,30,8]: responsibilities, interactions with other stakeholders, reporting relationships and the position within the organisation.

The preliminary results indicate that the benefits of information security need to be communicated to the involved stakeholders in order to ensure cooperation. This clearly supports approaches that require the establishment of direct links between

ISM and operative business processes. Another critical success factor is related to organisational culture and revolves around the handling of errors as well as the communication between hierarchical levels.

4.2 Information demand, supply and representation

After the analysis of the activities related to ISM (O.1) and the exploration of roles and responsibilities (O.2), it is necessary to investigate the relations among the identified roles involved in particular activities. The objective of this task (O.3) is to provide a clear picture with respect to information demand and information supply. Aspects such as availability, ownership and usage are of particular interest.

This meant that we had to identify the pieces of information that play a role in ISM. Again, the information security standards and guidelines seemed to be a good starting point for our investigations. With respect to information demand and information supply, we took the Standards Australia and Standards New Zealand AS/NZS 4360, the OCTAVE approach, the related standards ISO 27001 and BS 7799-3, the NIST Risk Management Guide for Information Technology Systems and the ProSecO approach [16] into account.

We classified the identified pieces of information (e.g. risk treatment options, valuation scale for assets, goals and objectives) into five categories: contextual information, information related to security requirements as well as information on assets, information on risks and information on controls. On top of this, we identified the sources of the various pieces of information. Information sources are mainly organisational documents (e.g. an organisational manual) and IT systems (e.g. a vulnerability scanner).

For all information sources, we defined an information owner. The information owners are directly linked to the roles and responsibilities explored in task O.2. The pieces of information that play a role in ISM stem from the standards and guidelines. Thus, every piece of information is linked to at least one activity from the standards and guidelines mentioned above and elaborated in task O.1.

The results of the analysis of information demand and information supply (i.e. the pieces of processed information and their sources) provide the starting point for the analysis of the communicative aspects of ISM (O.4). In this task, we focus on the representation of information and on the means of communication by which they are distributed among the different stakeholders. The intention of this analysis is to understand how different pieces of information have to be delivered to stakeholders. Typical representations of information include risk inventory tables, written policies and guidelines, graphical representations like process models and network topologies, and informal unstructured collections of other pieces of information.

4.3 Security information model, consistency rules and checks

To provide a common ground for collecting and processing the information pieces identified in task O.3, we defined meta-models describing the relevant information types (T.1). These meta-models are based on and extend previous works in the area of model-based security analysis [6] and have already been applied successfully in a case study which focused on the security analysis of service-oriented systems [7].

An important aspect is the provision of a security model containing concepts and relations for different types of information and their relations resulting from task O.3. This includes modelling security objectives, security requirements, the results of risk analysis efforts and controls which are either in place or planned. The focus lies on the traceability of security requirements, threats, risks and controls.

Another important aspect is the provision of a functional model covering an organisation's IT infrastructure, information objects and their lifecycles, business processes and roles. To facilitate the security analysis of the assets, we utilise the functional dependencies among assets as a frame. This implies that we have consistent dependencies throughout the functional model. The meta-models are defined in the form of Unified Modelling Language (UML) class diagrams including a detailed description of types and relations. UML was chosen as a modelling language because of its widespread use and the availability of extensive tool-support.

To keep the security information model consistent despite multiple stakeholders continuously and simultaneously trigger changes, we defined a set of rules and checks (T.2). The rules are formally described using the Object Constraint Language (OCL) and will be validated running periodic checks triggered by particular types of changes to the security information model. Based on the previous choice of using UML as a modelling language, OCL was a natural choice for expressing related rules and invariants.

4.4 Security information lifecycle

The information held in the security information model undergoes several transitions as a direct result of the ongoing activities within the scope of ISM. To make use of these transitions for the supervision and control of collaborative ISM, we design a lifecycle for each type of processed information (T.3). The current lifecycle stages of the processed pieces of information and the information itself provide an overview of an organisation's information security status. In particular, the lifecycle stages reflect the progress and overall status of information security itself.

To design the lifecycles for the different types of information analysed in task O.3 and modelled in task T.1, we use the core activities of ISM as a basis. Each completed activity triggers transitions of the information held in the security information model. During the design phase of the security information lifecycle, we considered two types of changes. First, changes which are the result of completed activities and triggered by the stakeholder and, second, changes which are triggered automatically (e.g. periodic reviews of certain pieces of information).

From a technical perspective, we realise the lifecycles in task T.4 by defining sets of status attributes for each model element defined in the meta-models (T.1). The status attributes reflect the lifecycle phases of pieces of security information. We depict the phases using UML state diagrams for each type of information. The state diagrams contain the status attributes and the allowed transitions between them. The allowed transitions between the lifecycle phases are defined using OCL.

5 Related work

We are not aware of any other publications primarily focusing on collaborative aspects of ISM. In spite of that, there are several works which provide valuable insights and useful directions for our research. The socio-organisational aspects of security and security management have been gaining attention in recent years as Dhillon and Backhouse [11] point out in an analysis of current directions in security research. Also, Siponen emphasises the need to move toward a new generation of social, adaptable and empirically grounded information systems security methods [29].

In spite of the fact that some works only briefly touch on collaborative aspects of ISM, they provide interesting insights. Rutkowski et al. conducted an empirical study where they analysed the effects of using group support systems to support risk management [28]. The necessity to integrate security-relevant information which nowadays is still kept in different silos and the need to investigate what types of information should be considered is pointed out in [14]. Other works focus on specific aspects of collaboration between organisations. Kuo, for instance, presents an agent-based framework that integrates distributed information security facilities [21].

Other publications focus on questions related to the effectiveness of ISM. Björk conducted an empirical study of critical success factors for a successful implementation of an ISMS [4]. In our expert interviews, we identified similar factors influencing a successful delegation of responsibilities. Kankanhalli et al. conducted a study in which they tested relationships between organisational factors, security measures and information system security effectiveness [19]. We are using similar criteria for the analysis of the distribution of ISM responsibilities in organisations. Knapp et al. focus on factors influencing the overall organisational security effectiveness [20].

The findings of these works provide valuable inputs for the realisation of our vision of collaborative ISM. Hawkey et al. currently work on the identification of factors which have influence on security management. They are focusing particularly on human, organisational and technological factors [15]. Early research results of this group back our vision of collaborative ISM.

Other related works focus on aspects concerning the perspectives of different stakeholders involved in ISM such as business managers and information security professionals [26]. The current state-of-the-art and the shortcomings regarding tool support in IT security management have been analysed in [5]. The current shortcomings and the mentioned need to develop a new class of tools which support ISM underline the practical relevance of our research.

6 Conclusions and outlook

Within the scope of this paper, we presented our vision of a collaborative approach to ISM. One of our primary goals is to understand the organisational aspects which are relevant with regard to collaboration in ISM. We described a set of tasks which have to be performed in order to better understand organisational issues related to ISM. Another important goal is the development of technical concepts and solutions which support the implementation of collaborative ISM. A review of related literature and the preliminary results from a series of expert interviews underline

the theoretical and practical relevance of this topic.

Our results, so far, not only indicate that ISM actually is inherently collaborative but also that certain aspects can be supported by means of a model-based information system. Such a system allows for one thing to coordinate the exchange and reuse of security information among numerous stakeholders throughout an organisation and for another thing to derive information about the overall status of information security from status attributes in the underlying model. We intend to develop a prototype of such a model-based information system at a later date.

Other avenues for further development of collaborative ISM activities can be seen in surmounting the limitation of the scope of ISM with respect to the following two dimensions: (1) organisation, to include extra-mural organisational units, as well as (2) organisational layer which is discussed briefly in the following. Typically, the organisational structure that is targeted with ISM activities comprises subsidiaries, departments and work groups and thus corresponds to the business system layer in Nonaka's hypertext organisation [22]. While the business system layer has also been the primary focus of systematic organisational design activities, projects and thus the project system layer in Nonaka's terms have been of increasing importance in organisations due to the fact that organisational change and innovation are both brought about by projects and thus the corresponding collectives of people can be a prime focus of information security concerns.

Last but not least, in many organisations it is ultimately the knowledge assets that need to be protected by ISM activities. However, the relationship between ISM activities and knowledge assets has only recently been explored under the umbrella term of management of knowledge risks or knowledge security which connects the field of knowledge management to risk and security management [18,10,17].

First approaches indicate that governance of knowledge risks needs to include legal, organisational and technical measures [3] and thus could be included into an ISM concept. This is especially true due to the fact that knowledge assets in an organisation involve and are typically spread over a collective of persons as well as organisational and technical resources in order to be strategically relevant [2] which provides a direct link to the notion of collaboration in our ISM concept.

Acknowledgements

This work was jointly funded by the Tyrolean Future Foundation (Tiroler Zukunftsstiftung) project COSEMA under the Translational Research Programme and the EU project SecureChange under the Seventh Framework Programme.

References

[1] Alberts, C. J. and A. J. Dorofee, "Managing information security risks: the OCTAVE approach," Pearson Education, 2002.

[2] Barney, J. B., *Firm resources and sustained competitive advantage*, Journal of Management **17** (1991).

[3] Bayer, F. and R. Maier, *Governing knowledge risks - design and results of an empirical study*, in: *Proceedings of the 7th International Conference on Knowledge Management*, 2007, pp. 200–208.

[4] Björck, F., *Implementing information security management systems - an empirical study of critical success factors.*, in: J. Eloff, L. Labuschagne, R. Solms and G. Dhillon, editors, *Advances in information security management and small systems security* (2001), pp. 197–211.

[5] Botta, D., R. Werlinger, A. Gagné, K. Beznosov, L. Iverson, S. Fels and B. Fisher, *Towards understanding IT security professionals and their tools*, Proc. of the 3rd Symposium on Usable privacy and security (2007), pp. 100–111.

[6] Breu, R. and F. Innerhofer-Oberperfler, *Model based business driven it security analysis*, in: *Proc. of the Third Symposium on Requirements Engineering for Information Security (SREIS'05)*, 2005.

[7] Breu, R., F. Innerhofer-Oberperfler, M. Mitterer, T. Schabetsberger and F. Wozak, *Model-based security analysis of health care networks*, in: *Proc. eHealth2008, Vienna*, 235 (2008), pp. 93–100.

[8] Chang, S. and C. Ho, *Organizational factors to the effectiveness of implementing information security management*, Industrial Management & Data Systems **106** (2006), pp. 345–61.

[9] Deloitte Touche Tohmatsu, *Protecting what matters. the 6th annual global security survey* (2009).

[10] Desouza, K. C. and G. K. Vanapalli, *Securing knowledge in organizations*, in: K. C. Desouza, editor, *New Frontiers of Knowledge Management*, Palgrave Macmillan, 2005 pp. 76–98.

[11] Dhillon, G. and J. Backhouse, *Current directions in IS security research: towards socio-organizational perspectives*, Inf. Syst. J **11** (2001), pp. 127–154.

[12] Ernst & Young, *Moving beyond compliance: Global information security survey* (2008).

[13] Gilliam, D. P., "Managing Information Technology Security Risk," Computer Science **3233/2004**, Springer, 2004, 296-317 pp.

[14] Hale, J. and P. Brusil, *Secur (e/ity) management: A continuing uphill climb*, Journal of Network and Systems Management **15** (2007), pp. 525–553.

[15] Hawkey, K., D. Botta, R. Werlinger, K. Muldner, A. Gagne and K. Beznosov, *Human, organizational, and technological factors of it security*, in: *CHI '08: ext. abstracts on Human factors in computing systems* (2008).

[16] Innerhofer-Oberperfler, F. and R. Breu, *Using an enterprise architecture for it risk management*, in: *ISSA06: Proc. Information Security South Africa Conference*, 2006.

[17] Jennex, M. E., *Security and knowledge management success*, in: *Proceedings of the 2nd Secure Knowledge Management Workshop*, 2006.

[18] Jordan, J. and J. Lowe, *Protecting strategic knowledge: Insights from collaborative agreements in the aerospace sector*, Technology Analysis and Strategic Management **16** (2004), pp. 241–259.

[19] Kankanhalli, A., H. Teo, B. Tan and K. Wei, *An integrative study of information systems security effectiveness*, International Journal of Information Management **23** (2003), pp. 139–154.

[20] Knapp, K., T. Marshall, R. Rainer Jr, F. Ford and D. By, *Managerial dimensions in information security: A theoretical model of organizational effectiveness*, Oct **5** (2005), p. 2005.

[21] Kuo, M., *An intelligent agent-based collaborative information security framework*, Expert Systems with Applications **32** (2007), pp. 585–598.

[22] Nonaka, I., *A dynamic theory of organizational knowledge creation*, Organization Science **5** (1994).

[23] Peltier, T. R., "Information security risk analysis," Auerbach, 2001.

[24] PricewaterhouseCoopers, *The global state of information security* (2008).

[25] Pulkkinen, M., A. Naumenko and K. Luostarinen, *Managing information security in a business network of machinery maintenance services business - enterprise architecture as a coordination tool*, Journal of Systems and Software (2007).

[26] Rainer, R. K., T. Marshall, K. Knapp and G. Montgomery, *Do information security professionals and business managers view information security issues differently?*, Inf. Systems Security **16** (2007).

[27] Ruighaver, A., S. Maynard and S. Chang, *Organisational security culture: Extending the end-user perspective*, Computers & Security **26** (2007), pp. 56 – 62.

[28] Rutkowski, A., B. van de Walle and G. van den Eede, *The effect of group support systems on the emergence of unique information in a risk management process: A field study*, Proceedings of the 39th Annual Hawaii International Conference on System Sciences, 2006. HICSS'06. **1** (2006).

[29] Siponen, M. T., *Analysis of modern is security development approaches: towards the next generation of social and adaptable iss methods*, Information and Organization **15** (2005), pp. 339–375.

[30] Wood, C., "Information Security Roles & Responsibilities Made Easy," Information Shield, 2005.