ATLANTIS PRESS

Advances in Economics, Business and Management Research (AEBMR), volume 37
International Conference on Transformations and Innovations in Management (ICTIM-17)

CRITICAL CONSIDERATIONS FOR ORGANIZATION-SPECIFIC INFORMATION SECURITY POLICY DEVELOPMENT

Hanna Kinnunen
University of Jyväskylä, Finland

Abstract

Organizations use information security policies (ISP) to guide the use of their information assets. Previous literature has presented ways to develop ISPs from suggested content to development methods; however, these approaches encounter problems when they are applied in organizations without adequate support. This paper introduces the development of a meta-methodology to support organization-specific ISP development. The approach is developed via action research with four Finnish companies. The results of the first two research cycles produced a list of 11 critical considerations, which were used to design ISP development methods. The critical considerations proved to be useful in designing different methods for different organization settings. However, they are only the first step towards a meta-methodology for designing ISP development methods.

Keywords: Information security policy, information security management, development method

JEL code: M15, M19

1. Introduction

Information security is a concern for nearly all organizations in modern society. However, many organizations are not prepared to counter threats to their information assets. One of the most important controls of information security is a firm's information security policy (Höne, Eloff 2002), but a large number of companies have not issued one (Colwill 2009). Governments concerned about the situation have laid down regulations for information processing (e.g., EU regulation 2016/679 on the protection of personal data and on the free movement of such data) and are recommending information security policies for all organizations, including SMEs and NGOs. Furthermore, information security management standards, such as the ISO27001, prescribe information security policies (ISP) as mandatory for organizations.

Information security policies can be seen as normative lists of actions that organization members are or are not supposed to do (Siponen, Iivari 2006), or as more general managerial directions for using information systems securely (Höne, Eloff 2002). Depending on the definition, ISPs can be considered only the highest-level strategic documents, or a larger set

of documents that also cover the application guidelines for the general statement (Siponen, Iivari 2006, Von Solms, Thomson & Maninjwa 2011). If we consider that the information system consists of intertwined technological and social systems (Lee 2001), then an ISP is something that is meant to change and maintain that system into one where the movement of information is controlled to avoid its misuse. The technical aspects of information systems security have been quite heavily researched (Willison, Siponen 2007), which is why this paper answers the call for the social aspects of information security management.

The contents of an ISP are mostly countermeasures for tackling information security issues. Depending on the organization and documents in hand, these may be more technical or organizational in nature. The content of the policy document may be completely composed within the organization, or external recommendations may be used, such as consultants, checklists and standards. However, research suggests that SMEs have insufficient knowledge of standards in order to implement them in their organizations (Yeniman Yildirim et al. 2011), and even in organizations were they are used, problems may arise if they are implemented without sufficient understanding of the firm's daily work practice (Hedström et al. 2011).

Previous research has presented methods for ISP development. Baskerville and Siponen (2002) proposed a meta-model for ISP development with the intention of providing support for policy development in emergent organizations. An empirical study used content analysis of open-ended survey answers to find constructs that would form an ISP process model (Knapp et al. 2009). Further, Flowerday and Tuyikeze (2016) created a policy development framework based on literature and validated it by surveying security professionals. Both of these approaches were created by gathering a large amount of information and fitting it to a model, which was then validated by asking for feedback from information security professionals. However, neither of the models contains information on how to convert the abstract model into a process used in an actual organization. More practical guidance for the actual process is included in the PFRIES model (Policy framework for Interpreting Risk in E-Business security), but it is still vague about the nature of information assets and what their environment means (Rees, Bandyopadhyay & Spafford 2003). The problem is that these approaches have not been validated in organizations, which means that we have no information about their success factors and failures.

Not all literature on ISP development proposes content and methods but some focus on influencing concepts and overall themes to be taken into consideration. For example, Karyda, Kiountouzis et al. (2005) presented seven contextual factors for the application of information security policies. Siponen (2000) argues that, in order to affect users' security behaviours, one must consider behavioural theories and satisfy their requirements. Requirements for an information security policy may also originate from known information security issues, an organization's goals and mission, or external stakeholders (Burgemeestre, Hulstijn & Tan 2013, Lopes, Sá-Soares 2010). Requirements for security may be widely different depending on the organization in question (Ølnes 1994), which is why using general templates for policies may be problematic (Flowerday, Tuyikeze 2016).

In any organization, information is exposed to three elements: processes, technology and stakeholders. It is important to remember that not all information security risks include technology (Posthumus, Von Solms 2004). Previous literature has identified factors that influence the development of ISPs. They influence both the content and the activities of the process; however, there is still a need to bring these three dimensions together at the organizational level.

The goal of this paper is to develop a meta-methodology for developing organization-specific information security policies. The main requirement for the methodology is that it integrates with management processes to avoid developmental duality between security and other business processes. The approach is developed via action research with Finnish companies. This paper contains the initial results of two action research cycles and a discussion.

2. ISP development in action

Previous literature has offered solutions for ISP development regarding its content, the method used and the factors influencing the development. However, the literature alone cannot provide answers on how the company-specific approach works in real situations. In order to understand how the concepts from the literature can be used in companies, they were studied in action research (AR). The action research followed the guidelines presented by Baskerville (1999) and included five phases to be repeated in a cyclical manner: diagnosing, action planning, action taking, evaluating and specifying learning. This research method was chosen to gain a deep understanding of the design and use of ISP development methods in companies and to provide direct support to the companies during the process.

2.1 Infrastructure

The client-system infrastructure was established formally, since the researchers and the participating companies were committed to a development project aiming to create new methods for the development of information security policies. The participating companies and their requirements for the action research project are:

- Company 1: A medium-sized consulting company developing a service process to provide ISP development services to customers in different fields;
- Company 2: A small consulting company developing a service process to provide ISP development services to customers mostly in highly regulated fields;
- Company 3: A large corporation in consulting and ICT services which is aiming to refine their current ISP development process to better fulfil the requirements of their customers in the public and private sectors;
- Company 4: A medium-sized company providing ICT design-related services in a highly internationalised value chain aiming to develop their ISP to support changes.

2.2 First cycle: Critical considerations

In the beginning of the AR project, the diagnosing of the situation was done by analysing the existing literature on the topic. The first course of action was to interview representatives of the four companies. Every company was represented by one or two persons who had the adequate knowledge and mandate to participate in the project. During the action-planning phase, themes and questions were formulated for semi-structured interviews. The aim was to understand the companies' current situations and their needs they have for the ISP development method. The evaluation of the interviews led to a deeper understanding of the companies' needs (see previous section). The specifying learning phase led to a list of recommendations to improve the ISP development methods (see table 1). These recommendations were called 'critical considerations'.

Table 1: Critical considerations, literature where the consideration is mentioned, companies (C1, C2, C3, C4) which mentioned the consideration in the interviews (and examples), companies (C1, C2) which used the consideration in their method.

Critical consideration	**Literature mention**	**Interview mention**	**Used in method**
The organization's management is motivated to take action toward information security	(Knapp et al. 2009, Trček 2003, Von Solms 2001, Wood 1995, Ashenden 2008)	C3 C1: Managers must be involved C2	C1 C2
ISP is aligned with business strategy	(Von Solms, Thomson & Maninjwa 2011, Lopes, Sá-Soares 2010, Galletta, Hufnagel 1992, Coles-Kemp 2009, Posthumus, Von Solms 2004, Rees, Bandyopadhyay & Spafford 2003, Burgemeestre, Hulstijn & Tan 2013)	C3	C1 C2
Information security policy is defined in a way that is understandable to the organization members /subjects	(Lopes, Sá-Soares 2010, Hedström et al. 2011, Flowerday, Tuyikeze 2016, Myyry 2009, Chen, Ramamurthy & Wen 2012)	C4 C1: Subjects must participate C2: People understand the need for security	(C1) C2
Understand the operational context of the ISP	(Ashenden 2008, Wood 1995, Ølnes 1994, Flowerday, Tuyikeze 2016, Rees, Bandyopadhyay & Spafford 2003, Von Solms 2001)	C4 C2: Laws /regulations, technological changes, standards	(C1) C2
Stakeholder groups / people affected by the ISP are identified	(Baskerville, Siponen 2002, Ashenden 2008, Ølnes 1994, Flowerday, Tuyikeze 2016, Posthumus, Von Solms 2004, Trompeter, Eloff 2001,	C4	C1

Table 1, cont.

	Burgemeestre, Hulstijn & Tan 2013)		
Security requirements are determined at the company level	(Baskerville, Siponen 2002, Von Solms, Thomson & Maninjwa 2011, Lopes, Sá-Soares 2010, Ølnes 1994, Knapp et al. 2009, Karyda, Kiountouzis & Kokolakis 2005, Flowerday, Tuyikeze 2016, Posthumus, Von Solms 2004, Rees, Bandyopadhyay & Spafford 2003, D'Aubeterre, Singh & Iyer 2008, Burgemeestre, Hulstijn & Tan 2013, Wood 1995)	C3: Customer, law and standard requirements C4: Value chain requirements C1: Different business areas included in development, some require the use of standards C2: Identified risks	C1 C2
ISP specifies the information affected by the policy	(Baskerville, Siponen 2002, Lopes, Sá-Soares 2010, Silic, Back 2014, Posthumus, Von Solms 2004, Rees, Bandyopadhyay & Spafford 2003)	C3: Information assets	C1 C2
Authority and responsibilities are stated	(Baskerville, Siponen 2002, Coles-Kemp 2009, Ølnes 1994, Bulgurcu, Cavusoglu & Benbasat 2010, Chen, Ramamurthy & Wen 2012, Trompeter, Eloff 2001, Wood 1995)	C4: Document owners stated C1: Managers of business areas have responsibilities	(C1) C2
Indicators for compliance and goals are built into the ISP	(Baskerville, Siponen 2002, Von Solms 2001, Von Solms, Thomson & Maninjwa 2011)	C3 C1: Customer chooses the metrics C2: Same metrics as in other monitoring	C1 C2
Information security development and maintenance are connected with the business processes	(Baskerville, Siponen 2002, Galletta, Hufnagel 1992, Posthumus, Von Solms 2004, D'Aubeterre, Singh & Iyer 2008)	C3 C4 C1 C2: Working methods	C1 (C2)
Policy is evaluated and tested in the organization	(Baskerville, Siponen 2002, Ølnes 1994, Rees, Bandyopadhyay & Spafford 2003)	C3 C1: Continuous evaluation C2: Checked once per year	C2

The critical considerations are a collection of recommendations for good ISP development suggested in research articles (see Table 1) and interviews. They highlight things that organizations should consider while formulating their own ISP. The considerations can be used to form an organization-specific ISP development method.

2.3 Second cycle: Designing methods

After the first AR cycle, the diagnosing phase was conducted alongside the previous specifying learning phase. The list of critical considerations was further developed by adding a few examples of their use for each of them. The plan was to give the companies new ideas and the liberty to use the critical consideration as they wish in their method designs.

The action-taking phase aimed to work with the companies to design an organization-specific ISP development method. The two consulting companies, Companies 1 and 2, moved on to the second cycle. The special feature of these companies is that they developed their methods as service products. The critical considerations were introduced to the companies via workshops, where they were discussed and fine-tuned.

Before the introduction of the critical considerations, Company 1 had designed an initial service process based on the ISO27002 standard. The recommended considerations were presented to the company and discussed in workshops. These discussions led to the re-design of the ISP development method that the firm would use with its clients who had ordered policy-development projects.

Their ISP development method starts with a meeting to motivate the executives of the company and to gain their mandate for the project. Then, the company's processes are mapped and evaluated from a security perspective. Risks are evaluated based on the processes, and the company's business strategy is assessed. Next, the actual ISP workshops are held for selected representatives of the client organization's staff. The topics of the workshops are based on ISO27002, and participants are chosen based on their expertise with the topics. The consultant then writes the results of the workshops into a Policy Management system and the client evaluates the content.

Company 2 had in their service selection an online tool for requirements monitoring, and they were interested in designing an ISP development method where this tool could be utilised. They wanted a lightweight ISP development method that would suit their smaller customers who only need a basic information security policy to meet regulatory requirements.

The method Company 2 developed had six requirements that included 2–5 tasks to meet these requirements. The requirements were: 'ensure motivation to take actions towards information security', 'ISP aligns with business strategy', 'business risks identified', 'policies are easy to use', 'understand the operational context of the policy' and 'test deploy, evaluate & update'. The tasks associated with these requirements are meant to be completed in iterations, adding depth to the security measures as needed.

Both Company 1 and Company 2 used the critical considerations in their methods. The use of these considerations is noted in Table 1, where the notations C1 and C2 refer to the companies explicitly using this consideration in their method. The markings in parentheses mean that the consideration is present in the method as an intended part of some of its other steps. The

critical considerations were used in both designed methods, except for 'Stakeholder groups / people affected by the ISP are identified' and 'Policy is evaluated and tested in the organization', which were only used by one company.

3. Discussion

Previous literature has proposed general content for ISPs, general methods for ISP life cycles and different factors that might affect ISP development. However, the literature lacks information on how to turn these abstract and general guidelines into working ISP development methods in an organization. In particular, approaches suitable for SMEs are scarce. Without adequate support for ISP development, the result may be policies that cause extra work, are forgotten or are even opposed.

The previous section presents the results of an action research project put forth to tackle the problems found in some other approaches. The research method was particularly suitable for a problem that requires a deep understanding of the real problems companies face and the actions they are able to perform to tackle them.

This paper has outlined critical considerations, which are components of a meta-methodology for ISP development. They were developed to highlight problem areas that were identified from previous literature and interviews with companies. The list of considerations was further developed with the companies as they gave their comments and applied them to design their own methods. The critical considerations can be combined to other approaches to highlight matters that must be decided at the organization level. Company 1 provides an example of a method that combines the ISO27002 standard and the critical considerations.

The critical considerations are not the final meta-methodology, nor is the list exhaustive. The research setting in Finland might have influenced the list, even though international research literature and internationally operating companies were included. Further cycles of AR are planned to confirm that the critical considerations are useful and, possibly, to find new ones. Thus far, the relationships among the critical considerations, ISP content and previous methods have proven to be very complex, but further research can help make connections that will result in further development of the meta-methodology.

Although the work is still on-going, the critical considerations have been well received in the companies. They highlight the integration of information security into the daily operations of a company as well as its strategic goals. The organization-specific approach can help in adding information security as a natural part of an organization's information flow, instead of just being considered a hindrance to daily work.

4. Conclusion

This paper has presented a new approach to organization-specific information security policy development. Previous literature has proposed general content for ISPs, general methods for

ISP life cycles and different factors that might affect the ISP development. The literature however lacked information on how to turn these abstract and general guidelines to a working ISP development method in an organization. Especially approaches suitable for SMEs are scarce.

An action research project was conducted to find an approach for adding more organization-specific aspects for ISP development. This approach provided deep understanding of the real life problems companies face and gave the opportunity for the researchers to provide suggestions. The two action research cycles presented in this paper resulted in a list of 11 critical considerations which can be used to create an ISP development method that meets the specific needs and limitations of the organization.

Acknowledgements

This research project was funded by European Regional Development Fund through Tekes (the Finnish funding agency for innovations). I would also like to thank Professor Mikko Siponen, Dr Michael Lapke and Dr Hadi Ghanbari for their input in creating the critical considerations.

References

Ashenden, D. (2008) "Information Security management: A human challenge?", *Information Security Technical Report,* Vol. 13, No. 4, pp. 195-201.

Baskerville, R. (1999) "Investigating information systems with action research", *Communications of the AIS,* Vol. 2, No. 3, pp. 2-31.

Baskerville, R. and Siponen, M. (2002) "An information security meta-policy for emergent organizations", *Logistics Information Management,* Vol. 15, No. 5/6, pp. 337-346.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness", *MIS Quarterly,* Vol. 34, No. 3, pp. 523-548.

Burgemeestre, B., Hulstijn, J. and Tan, Y. (2013) "Value-based argumentation for designing and auditing security measures", *Ethics and Information Technology,* Vol. 15, No. 3, pp. 153-171.

Chen, Y., Ramamurthy, K. and Wen, K. (2012) "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?", *Journal of Management Information Systems,* Vol. 29, No. 3, pp. 157-188.

Coles-Kemp, L. (2009) "Information security management: An entangled research challenge", *Information Security Technical Report,* Vol. 14, No. 4, pp. 181-185.

Colwill, C. (2009) "Human factors in information security: The insider threat – Who can you trust these days?", *Information Security Technical Report,* Vol. 14, No. 4, pp. 186-196.

D'Aubeterre, F., Singh, R. and Iyer, L. (2008) "Secure activity resource coordination: empirical evidence of enhanced security awareness in designing secure business processes", *European Journal of Information Systems,* Vol. 17, No. 5, pp. 528.

Flowerday, S.V. and Tuyikeze, T. (2016) "Information security policy development and implementation: The what, how and who", *Computers & Security,* Vol. 61, pp. 169-183.

Galletta, D.F. and Hufnagel, E. (1992) "A model of end-user computing policy: Context, process, content and compliance", *Information & Management,* Vol. 22, No. 1, pp. 1-18.

Hedström, K., Kolkowska, E., Karlsson, F. and Allen, J.P. (2011) "Value conflicts for information security management", *The Journal of Strategic Information Systems,* Vol. 20, No. 4, pp. 373-384.

Höne, K. and Eloff, J. (2002) "What Makes an Effective Information Security Policy?", *Network Security,* Vol. 2002, No. 6, pp. 14-16.

Karyda, M., Kiountouzis, E. and Kokolakis, S. (2005) "Information systems security policies: a contextual perspective", *Computers & Security,* Vol. 24, No. 3, pp. 246-260.

Knapp, K.J., Morris, F.R., Marshall, T.E. and Byrd, T.A. (2009) "Information security policy: An organizational-level process model", *Computers & Security,* Vol. 28, No. 7, pp. 493-508.

Lee, A.S. (2001) "Editor's Comments", *MIS Quarterly,* Vol. 25, No. 1, pp. iii-vii.

Lopes, I. and Sá-Soares, F. (2010) "Information Systems Security Policies: a Survey in Portugese Public administration", *IADIS International Conference Information Systems*.

Myyry, L. (2009) "What levels of moral reasoning and values explain adherence to information security rules? An empirical study", *European Journal of Information Systems,* Vol. 18, No. 2, pp. 126-139.

Ølnes, J. (1994) "Development of security policies", *Computers & Security,* Vol. 13, No. 8, pp. 628-636.

Posthumus, S. and Von Solms, R. (2004) "A framework for the governance of information security", *Computers & Security,* Vol. 23, No. 8, pp. 638-646.

Rees, J., Bandyopadhyay, S. and Spafford, E. (2003) "PFIRES: A Policy Framework for Information Security", *Communications of the ACM,* Vol. 46, No. 7, pp. 101-106.

Silic, M. and Back, A. (2014) "Information security: Critical review and future directions for research", *Information Management & Computer Security,* Vol. 22, No. 3, pp. 279-308.

Siponen, M. (2000) "A conceptual foundation for organizational information security awareness", *Information Management & Computer Security,* Vol. 8, No. 1, pp. 31-41.

Siponen, M. and Iivari, J. (2006) "Six Design Theories for IS Security Policies and Guidelines", *Journal of the Association for Information Systems,* Vol. 7, No. 7, pp. 445-473.

Trček, D. (2003) "An integral framework for information systems security management", *Computers & Security,* Vol. 22, No. 4, pp. 337-360.

Trompeter, C. and Eloff, J. (2001) "A Framework for the Implementation of Socio-ethical Controls in Information Security", *Computers & Security,* Vol. 20, No. 5, pp. 384-391.

Von Solms, B. (2001) "Information security - A multidimensional discipline", *Computers & Security,* Vol. 20, No. 6, pp. 504-508.

Von Solms, R., Thomson, K. and Maninjwa, P.M. (2011) "Information Security Governance control through comprehensive policy architectures", *Information Security South Africa (ISSA), 2011*, pp. 1.

Willison, R. and Siponen, M. (2007) "A Critical assessment of IS Security Research Between 1990-2004", *IDEAS Working Paper Series from RePEc*.

Wood, C. (1995) "Writing InfoSec Policies", *Computers & Security,* Vol. 14, pp. 667-674.

Yeniman Yildirim, E., Akalp, G., Aytac, S. and Bayram, N. (2011) "Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey", *International Journal of Information Management,* Vol. 31, No. 4, pp. 360-365.