Author(s): Kinnunen, Hanna; Siponen, Mikko

Title: Developing Organization-Specific Information Security Policies by using Critical Thinking

Year: 2018

Version: Published version

Please cite the original version:

Kinnunen, H., & Siponen, M. (2018). Developing Organization-Specific Information Security Policies by using Critical Thinking. In M. Tanabu, & D. Senoo (Eds.), PACIS 2018 : Proceedings of the 22nd Pacific Asia Conference on Information Systems. Opportunities and Challenges for the Digitized Society : Are We Ready? (pp. 2145-2157). Association for Information Systems. https://aisel.aisnet.org/pacis2018/244

PACIS 2018 Proceedings

Pacific Asia Conference on Information Systems
(PACIS)

6-26-2018

Developing Organization-Specific Information Security Policies

Hanna Kinnunen
University of Jyväskylä, hanna.k.kinnunen@jyu.fi

Mikko Siponen
University of Jyvaskyla, mikko.siponen@jyu.fi

Recommended Citation
Kinnunen, Hanna and Siponen, Mikko, "Developing Organization-Specific Information Security Policies" (2018). *PACIS 2018 Proceedings*. 244.
https://aisel.aisnet.org/pacis2018/244

Developing Organization-Specific Information Security Policies by using Critical Thinking

Completed Research Paper

Hanna Kinnunen
University of Jyvaskyla
PB 35, 40014 Jyvaskyla Finland
hanna.k.kinnunen@jyu.fi

Mikko Siponen
University of Jyvaskyla
PB 35, 40014 Jyvaskyla Finland
mikko.siponen@jyu.fi

Abstract

Information security policies (ISP) can be seen as a collection of rules, principles, or guidelines that steer the information security actions in organizations. The literature on ISP development discusses ISP from three viewpoints—content, method, and context—which together form the basis of an organization-specific ISP development method. However, previous approaches do not combine these dimensions on a practical level. This article applies Hare's (1981) theory of critical thinking in a method to support the decision-making needed in ISP development. A list of critical considerations for the ISP development process was created and applied in an action research project. The objective of informed decision-making was realized by creating a method that systematically gathers knowledge of the target organization before selecting rules for it. Supporting critical thinking in the ISP development process resulted in an organization-specific policy.

Keywords: Information security policy, development method, action research

Introduction

Virtually all textbooks and standards on information security management argue for the need for information security policies (ISPs). An ISP is a document that an organization can use to steer the use of information assets, and it forms the basis for all the information security actions in the organization (Soto Corpuz 2011; Yeniman Yildirim et al. 2011). ISP may refer to a highest-level information security strategy, or it could also include lower-level documents, such as user instructions and technical protocols (Baskerville and Siponen 2002; Cram et al. 2017; Klaic 2010). ISP can also refer to a family of policy documents, from an information security strategy to end user guidelines. However, this leads to a question: How should ISPs be developed? One common strategy is the use of the baseline approach (Baskerville and Siponen 2002).

Information security management has a long tradition of outlining and advocating the use of the baseline approach. In the 1970s, checklists were created that aimed at listing generic controls for all organizations (Baskerville 1993). Later, information security management standards were proposed, such as BS7799 (Willison and Siponen 2007), which have since received the status of ISO standards (the ISO 27000 series) (Trček 2003). The term baseline refers to following what is believed to be "commonly applied." Numerous authors have suggested that information security management and related investments should be based on such an approach (Pounder 1999; Wood and Parker 2004). The baseline approach is also advocated for the development of ISPs. For example, Janczewski (Janczewski 2000 p. 96, quoted in Baskerville and Siponen 2002) notes, "the best method of the ISP [Information Security Policy] development is to concentrate on the baseline approach [i.e., to implement widely used controls] and to implement as much as possible the security standards described [such as BS 7799]."

Unfortunately, a baseline approach (following security management standards or doing what other companies are doing) gives little advice on how to develop company-specific ISPs (Baskerville and Siponen 2002). This is because such an approach emphasizes common practices or what the standards say, which is not necessarily, what the company actually needs to do (Baskerville 1993; Siponen 2006). This issue is especially challenging for small organizations for three reasons. First, the standards and baselines may be based on experiences in large organizations (cf., BS7799 and the ISO 27000 series). Second, even at a minimum, the implementation and auditing of standards can cost tens of thousands of euros in working hours and services. Third, standards must be tailored to each company (Siponen 2006), and small organizations may have few security resources to do this: "many organisations face the challenge of understanding and translating the standards' requirements into something concrete and actionable" (Niemimaa and Niemimaa 2017, p. 2).

To make these reasons concrete consider the following example: An employee of a small company realizes that the company's partners and clients expect it to have an ISP, but the reality is that its information security procedures are almost non-existent. Looking at the existing guidelines on the subject, the first step is conducting a risk assessment (Flowerday and Tuyikeze 2016; Knapp et al. 2009; Rees et al. 2003). But, how does one identify which risks exist, and how is it possible to determine whether the threat is real? Which countermeasures should be chosen, and are they the right ones? Using standards such as ISO 27000, of course, leads to many other questions as well. Whatever answers the employee gives to these questions may be subjective and inaccurate if they are answered by guessing and not supported by a method that would help in making these decisions in a specific context (Klaic 2010).

Hence, methods are needed that can be used to build company-specific ISPs that are also suited for small and medium sized enterprises (SMEs). However, the current literature offers little help in this regard. The baselines or standards, or the countless calls to follow them (Höne and Eloff 2002; Pounder 1999; Trček 2003; Wood and Parker 2004), do not help to address these questions.

This paper aims to provide support for creating an ISP development method that results in an organization-specific information security policy. We use Hare's (1981) theory of critical thinking as basis for a method that supports the design of an ISP development method. A list of 11 critical considerations are developed as "tools" to support informed-decision making in the ISP context.

The rest of the paper is organized as follows. The next section reviews previous literature about developing information security policies followed by a section about creating rules. Then, we will introduce an action research project and its results. Finally, we discuss the findings and offer conclusions.

Previous Research

We examine the existing ISP research from three perspectives: content, method, and context (Figure 1). The dimensions are used here to help simplify the complexity of the ISP literature, although many ISP approaches cover more than one of the dimensions in some way. Understanding the different perspectives of previous research highlights the complexity of the issue as well as how different perspectives contribute towards an organization-specific ISP.

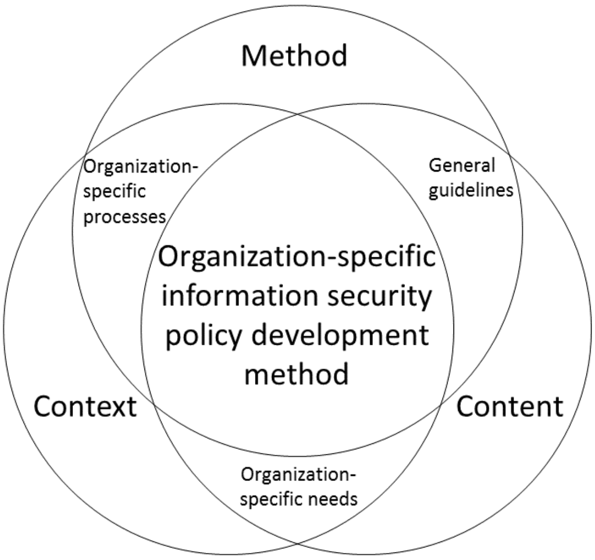
Method
Organization-specific processes
General guidelines
Organization-specific information security policy development method
Context
Content
Organization-specific needs

Figure 1. The three dimensions of ISP development

The ISP content is the set of rules, principles, or guidelines that have been chosen to govern the information security activities in an organization. Depending on the definition of ISP that is used, it can consist of only a brief executive-level statement or a wide range of instructions that relate to the secure processing of information (Doherty et al. 2009; Von Solms et al. 2011). The style of documenting the policy depends on the company and can consist of anything from one extensive handbook to a quick tips page on the intranet. In our study, the view of the content is mostly managerial and includes both the higher-level strategy and lower-level guidance.

The ISP development method is used to create the content of an ISP in a specific context. It can be anything from an ad hoc to a standardized procedure. The method can cover only the development of the ISP or also include the preparation and maintenance phases before and after the creation of the content. In this research, the method covers the knowledge gathering prior to ISP development, the actual decision-making regarding the content, and the approval of the final version of the ISP.

The context of an ISP refers to a specific organization, its circumstances, and environment. Context-specific design can make every ISP unique since it accounts for the differences between organizations. For example, Karyda, Kiountouzis, and Kokolakis (2005) listed the following contextual factors: organizational structure, organizational culture, management support, security officer, training and education, users' participation in the formulation process, and contribution to users' goals. In this article, we mostly focus on the organization members and business processes as representations of the context.

ISP Content

There are different notions of the areas and details an ISP is supposed to cover. The ISP may be one huge document covering everything, separate hierarchically connected policies (Von Solms et al. 2011), or a high-level policy, supplemented by guidelines for different users (Doherty et al. 2009). People also have different views about the tone and peremptory nature of the ISP. Different design theories can be applied to ISPs, from a law book-like compulsory rule set to general guidelines that are open for interpretation (Siponen and Iivari 2006).

Regardless of the choice of architecture for the documents, the breath, clarity, and brevity of the document is important to consider when the goal is to have the reader understand the content (Goel and Chengalur-Smith 2010). If the nature of the ISP is not clear to the organization members, this may hinder the adoption of the policy altogether (Lopes and Sá-Soares 2010).

There are different kinds of guides available for the content and controls in an ISP. One of the most well known is the ISO27002 standard, which recommends several areas of content, including management direction and cryptographic control (ISO/IEC 27002 2013). Standards such as this, in addition to laws and regulations, may be a requirement for doing business in some markets. However, standards may have a problem in that they focus more on the processes and implementation than on providing guidance for content development (Höne and Eloff 2002). General guidelines also tend to recommend more preventive actions than responsive ones, which makes them more suitable for businesses in predictable and stable markets, whereas companies in volatile markets require more adaptable guiding principles and recovery plans (Baskerville et al. 2014; Siponen and Iivari 2006).

Earlier approaches to ISP content stressed that the policy should strive to protect the confidentiality, integrity, and availability (assurance of service) of the information, but this view has been criticized for its focus on technological security (Sterne 1991). Focusing on information technology may leave gaps in security when, for example, the staff considers only digital files to be secret and not paper documents (Hedström et al. 2011). Contemporary views incorporate new areas to be considered in the ISP content, such as organization structure and culture (Klaic 2010). These organization-specific requirements complicate the decision-making on the content even further, which is why many authors have suggested methods for the development process.

ISP Development Method

The content of an ISP is created using some kind of method, whether formal or ad hoc. Previous approaches to security design in the 1970s involved checklists, where one could simply choose controls for his or her organization. Since then, methods have evolved through mechanistic engineering methods to logical-transformational methods (Baskerville 1993). Over the years, the complexity of ISP development and security management methodologies has increased (Klaic 2010).

The ISP development methods are often described as life-cycle models. These models depict the overall lifecycle of the ISP content and the tasks associated to it. PFRIES is a framework that was developed based on the product development and systems development lifecycle. It has four phases with two sub-phases that are to be repeated cyclically and feedback loops in every step (Rees et al. 2003). A slightly more complex model with influencing factors was created in a survey study targeted to information security professionals (Knapp et al. 2009). Flowerday and Tuyikeze developed a lifecycle model based on previous literature and verified it by asking security professionals whether they agreed with the concepts (2016). These methods share similar steps and provide a high-level framework for the ISP development process. The steps are risk assessment, policy development (and requirements), (definition and) implementation of controls, and maintenance (and monitoring).

In the lifecycle models, policy development is only one step in the whole process. In the quantitative research model used by Flowerday and Tuyikeze (2016), the variables in this step are writing the (detailed/low/high level) security policy and consulting stakeholders. The participation of stakeholders and organizational members was also highlighted in the answers for open-ended questions in the research of Knapp et al. (2009). In the PFRIES model (Rees et al. 2003) the policy development phase also includes the creation of a security strategy. The tasks for this step include identifying and prioritizing business and security initiatives and policy areas. This model recommends the participation of key management personnel (Rees et al. 2003).

Baskerville and Siponen (2002) provided more detailed instructions for the development process in the information security meta-policy. The meta-policy recommends identification and classification of policy subjects and objects. Then, the design process will determine the architecture and scope of the policies (Baskerville and Siponen 2002). Among these examples, the meta-policy gives the most practical instruction for the development phase.

As there are multiple methods from which to choose, organizations may have difficulties in choosing the right one. To overcome this problem, a process for choosing a method has been presented, which includes factors such as perception of risk and use of information technology (Mcfadzean et al. 2007). There are also tools that can be used to determine the state of information security in the organization as well as the next steps that should be taken (Saleh 2011).

However, while these models mention several factors that would help in making the ISP suitable for the company, many of them do not provide instructions for implementing them. In addition to the overall models, the literature also provides some techniques for specific areas of the method, for example, choosing the right people (Lapke and Dhillon 2008), identifying information (D'Aubeterre et al. 2008), and solving value conflicts (Burgemeestre et al. 2013).

Context of ISP

Context provides us with an interesting dilemma regarding how to create rules for the ISP. Since we need to respect the different needs of the organization, we cannot expect the same general policy recommendations to apply in all organizations (Baskerville & Siponen 2002). There are contextual factors that influence the development of the ISP. Karyda et al. (2005) identified seven such factors: organizational structure, organizational culture, management support, contribution to users' goals, security offices, user participation in the formulation process, training, and education. These factors connect to the content and method in different ways; for example, a security-ignorant organizational culture may be a reason to start a new cycle in the ISP development (Talbot and Woodward 2009).

Since the security culture of an organization can affect the ISP, it is advisable to have user participation in the ISP development process (Da Veiga and Eloff 2010). Insiders can be a great resource or a big risk to the information assets (Colwill 2009), which is why their participation is often recommended. The represented stakeholder groups in ISP development could be business units, executive management, human resources, IT department, legal advisors, and public relations (Maynard et al. 2011). The inclusion of different representatives may be of benefit in the implementation phase if they act as advocates of the ISP (Maynard et al. 2011; Rees et al. 2003).

Managers often play a key role in the development and implementation of the ISP. Their input is vital when aligning the ISP with the business processes (Soomro et al. 2016). However, it must be noted that the official hierarchy of an organization may not reflect the real power structures, and selecting the right people to participate in the ISP development may require a method of its own (Coles-Kemp 2009; Lapke and Dhillon 2008).

Context affects both the content and the development method of an ISP. The various levels of context, from the company's market position to single individual's perceptions, make creating an organization-specific ISP quite complex. If the context is disregarded during the development of the ISP, there may be problems in its implementation and compliance (Chen et al. 2012). The content of an ISP is a "dead object" unless it is materialized in the actions of its subjects (Niemimaa and Niemimaa 2017).

Previous research introduces several ways that the content, method, and context influence each other in the ISP development process. However, many approaches describe ISP development from a high-level perspective, providing very little guidance for the practical work tasks. Especially the support for including contextual factors to the ISP development is scarce. Many of these approaches also lack empirical evidence of their successes and failures and justification for exclusion and inclusion of elements.

Theory for Creating Rules

The development of ISPs is a process that essentially aims at creating rules or principles for individuals in certain situations. Whether the rules are strict and particular or general and open for interpretation (Siponen and Iivari 2006), they still need to be thoughtfully selected by somebody. For the development of the rules, we apply R. M. Hare's (1981) normative theory from the field of philosophy. Karjalainen and Siponen (2011) have previously applied Hare's work to information security training.

Hare (1981) distinguishes two levels in moral thinking, intuitive and critical. The distinction has been used by philosophy from the times of Plato and Aristotle (Hare 1981, p. 25). At an intuitive level, decisions are made according to predetermined rules and conflicts between them are irresoluble (Hare 1981, p. 26). These may be called prima facie ("at first sight") principles (Hare 1981, p. 38). If intuitive-level thinking is used when creating an ISP, the method includes listing controls we think are the right courses of action, and this usually involves copying rules from others from whom we have learned these principles. Standards could be regarded as consisting of intuitive level principles. Such a method cannot resolve conflicts between rules or create new ones, even if the listed ones are poorly suited for the organization.

Critical thinking is used when rules conflict or when new rules are created (Hare 1981, p. 26, 40, 50). At the critical level, decisions are made based on careful consideration of possible outcomes of the action. In the context of ISPs, it may be difficult to identify the issues that require critical thinking. Either there may not be enough knowledge about the situation to create rules, or there may be an expectation of general rules for the situation and only intuitive level thinking is used. This may be the case when the ISP developers choose controls from checklists (Baskerville 1993) or even use a complete predefined ISP from a third party. If critical thinking is used when developing an ISP, "choices are made under the constraints imposed by the logical properties of the moral concepts and by the non-moral facts" (Hare 1981, p. 40).

The critical thinking method requires that we know which situation needs the rule and whether it is similar to other/earlier situations according to its relevant factors (Hare 1981, p. 52, 63, 89). Knowing who is affected by the rules and considering how they might feel about them is also important (Hare 1981, p. 92, 95). The answers to these questions are related to the scope, or the subjects and objects, of the policy (Baskerville and Siponen 2002), and determining them requires gathering information about the organization.

Simply understanding the situation in an organization is not enough to make a decision about rules that should be applied to it. The alternative choices for rules must be assessed in light of the known facts about the circumstances and the strengths of the preferences the affected people might have (Hare 1981, p. 124). When creating an ISP, this would mean that alternative rules should be considered from the point of view of the persons whose work they affect.

After considering the facts and outcomes of different rules, it is possible to choose the rule to be used in that situation. This is a new prima facie principle that should be applicable to the ISP subjects in the specific organization, but they cannot be expected to apply elsewhere (Hare 1981, p. 200). Hare does not present a universal algorithm for making moral decisions but rather leaves the labor of moral thinking to the people making the rules (Hare 1981, p. 212). According to Hare (Hare 1981, p. 218), all that can be done is to make sense of the available facts and reason logically about the requirements of the decision.

Action Research

If we want to understand the processes that occur during ISP development, we must choose a research approach that interprets real situations. We wanted to combine the researchers' knowledge about literature and the company view of real-life situations. Action research (AR) was chosen as a method that allows the researchers to provide input on the problem at hand. The research setting followed the guidelines provided by Baskerville (1999), including the cyclically repeated phases of diagnosing, action planning, action taking, evaluating, and specifying learning.

Data Gathering

The AR project was conducted over one and a half years in 2016–2017 (Figure 2) with a company, which we call ConsultCo. ConsultCo is a medium sized company operating in several cities in Finland. It provides consulting services including IT management and helpdesk. The company's aim was to create a new service product for ISP development. Before the first cycle of the AR project, it had designed a service process based on the ISO27002 standard, but this service was not yet provided to customers. With the help of the researchers, ConsultCo wanted to make the process more efficient and adjustable to its customers' needs.

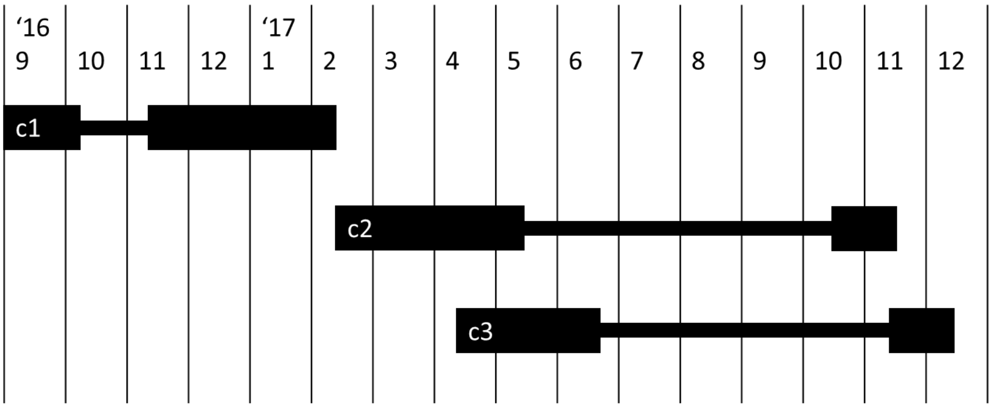

Figure 2. Research timeline with three AR cycles

The client–system infrastructure was established formally since the researchers and the company were committed to a development project aiming to create new methods for the development of ISPs. The company had two main informants and several other people participating in the project. ConsultCo asked two of its clients for permission to have a researcher monitor the process. Both client cases (c2 and c3 in Figure 2) had significant down time between the main part of the work and when the policy was finally accepted and the project ended.

In the first AR cycle, the diagnosing of the situation was done through an interview with ConsultCo and in a workshop between the company representatives and researchers. A comprehensive literature review was also conducted to understand previous approaches. The diagnosing phase led to an action planning phase, in which a list of critical considerations was created. The critical considerations were drawn from the ideas of Hare's (1981) work and were meant to be used as a tool to promote context-based decision-making. In the action-taking phase, these considerations were then introduced to the company and discussed in workshops. The discussions led to the re-design of ConsultCo's existing ISP development method. The method was tested inside the company to see how it would support the company's internal ISP development (c1 in Figure 2). In the evaluation phase, the critical considerations were evaluated according to the feedback from ConsultCo.

In the second AR cycle, the diagnosing was done alongside the evaluation of the previous cycle. The first version of the critical considerations was revised and provided to ConsultCo again with tips about different alternatives to cover the subjects. During the action taking phase, the method was tested in a real situation with a client (c2 in Figure 2). When this cycle was evaluated, it was clear that the planned working method needed adjustment.

In the third AR cycle, the problems of the previous cycle were diagnosed with ConsultCo, and changes were made to the process. The two client cases overlapped, but since they both followed the steps of the ISP development process, it was possible to execute the AR learning cycle with the first client before the same step was executed with the second client (c3 in Figure 2). After the third AR cycle, ConsultCo was happy with the distribution of work in the method.

Results

The diagnosis phase of the first AR cycle revealed that the existing literature or standards did not give ConsultCo adequate tools with which to support its clients' decision-making in the ISP development process. A contact person at ConsultCo described the needs regarding a good ISP development method as follows:

> *It is vital that the policy process starts from the company executives and has their commitment and mandate. It is not the job of the chief information officer or information security manager or any single hero; instead, it is an issue for the whole organization. If these two things do not come together, then it is useless for anyone to spend time making it [the ISP].*
> *- Product Manager at ConsultCo*

The researchers turned to Hare's theory of critical thinking to for a method that could be used to support ConsultCo in designing an ISP development method that facilitates thought processes and decision-making. The method has three general steps: gather knowledge, assess outcomes, choose rules. Hare's theory combined with themes from previous literature (Kinnunen 2017) as well as knowledge gained through the interview resulted in the notion of critical considerations.

A critical consideration is a topic that requires decision-making in the ISP development process. The topics steer towards considering what kind of knowledge should be gathered about the organization and assessing what action should be taken. The purpose of the critical considerations was to promote critical thinking in the ISP development method design process. For this research project, we created a list of eleven considerations.

- The organization's management is motivated to take action toward information security
- The ISP is aligned with business strategy
- The ISP is defined in a way that is comprehensible to the organization members/subjects
- Understand the operational context of the ISP
- Stakeholder groups/people affected by the ISP are identified
- Security requirements are determined at the company level
- ISP specifies the information affected by the policy
- Authority and responsibilities are stated
- Indicators for compliance and goals are built into the ISP
- Information security development and maintenance are connected with the business processes
- Policy is evaluated and tested in the organization

These considerations were presented to ConsultCo with tips on different ways to implement them in a method. The company agreed that all of these considerations should be part of an organization-specific ISP development method. One of the most notable changes that ConsultCo implemented in its own method after discussing the critical considerations was the addition of a section where business strategy is discussed in light of information security with the higher management. The rest of the considerations were included in the steps as part of the workshop content. The method had the following steps: kick-off, process mapping, risk review, strategy alignment, ISP workshops, review, and approval. The most important tools for the consultant were slide sets containing outlines of the workshops, a process drawing tool and an information system for storing and linking process data.

After the changes were made, ConsultCo proceeded with a practice run within their own organization, where the ISP also needed updating. The company held an online meeting for representatives from different business areas, with the responsible consultant leading them through the process. The idea was to complete the company process map and identify weak spots and then move on to the actual ISP workshop content, which is based on ISO27002. The process mapping and evaluation were found to be surprisingly difficult and time consuming. They also did not result in enough knowledge for the following ISP workshops. This resulted in modifications of the information system ConsultCo uses for storing the process information. The company added indicators for the needs of information in relation to confidentiality, integrity, and availability as well as for the current state of the process (green, yellow, red). These indicators were used to get a better idea of the most urgent needs in the subsequent risk evaluation phase.

The experiences with the test run resulted in changes in the working order. In cycle two, with the first real customer, the process mapping was split into two half-day workshops. This timeframe was much more realistic, but issues remained. The participants in the workshops were representatives of all business areas, which led to a situation where the process being mapped was only familiar to some of them while others got bored. Even with a full day of work, the mapping had to be prioritized to only cover the most business-critical processes. In this cycle, however, the information system better supported the extraction of vital knowledge about the client organization.

In the third AR cycle, the process workshops were made even shorter. The business area representatives participated in the kick-off meeting, but the following process meetings only covered one business area at a time, and the participants included the representative and some other key persons. The time reserved for the workshop was cut down to around two hours per business area since the participants' concentration had been observed to decrease in longer meetings. If the process mapping was not finished in time, the consultant asked the participants to fill out a spreadsheet representing the information system fields as "homework." In this way, the participants had sufficient guidance to perform the process mapping independently, and all mapping could be completed before the risk evaluation.

The risk assessment focused on the areas that were found to be critical in the process mapping. After the risk assessment, the next phase involved the actual policy workshops. These had one representative from each business area. Since this phase used the information gathered in previous workshops, the amount of participants could be smaller. The topics of the policy workshops were adapted from ISO27002. However, after mapping the processes, the consultant was able to better plan the areas that would be important to the client and what could be given minimal attention. The client representatives also obtained a better understanding about the situation in their processes and could thus make more informed decisions about the policy.

After the policy workshops, the consultant wrote down the decisions in the information system. The content was then reviewed by the client representatives. After any modifications were made, the ISP was approved. Then, the development project came to an end and the implementation of the policy started. The results of the workshops were saved in the information system for later use in evaluation and auditing. A representative from ConsultCo modestly described the outcome of the method as follows:

> *The policy is reviewed and approved in a group meeting where all the business areas are represented. At this point, the clients have clearly considered what they must change in their daily operations. […] If there are conflicts with the business needs, some changes to the ISP can still be made at this point. This far only cosmetic changes have been made, so it seems that the method creates a policy that is good enough.*
> *- Information Security Officer at ConsultCo*

Discussion

The existing literature provides us with a wide range of recommendations for creating an ISP. The different recommendations portray the three perspectives of ISP development: content, method, and context. However, they often cover just one or two perspectives. If there is an expectation of baseline content or method, it might limit the way context is taken into account. Moreover, a predefined ISP development method might not lead to quality content for every context. The content is expected to affect the context in implementation, but how does the context affect the content in development? Is the predefined method supposed to affect the context, or should the context affect the method? If we make assumptions about how these dimensions affect each other, we are in danger of giving some of them too little attention.

The similarity of lifecycle models for ISP development raises the question whether these models with similar steps are time proven and have earned their status through testing. On the other hand, could it be that the alternatives for them are not adequately researched which leads to the hegemonic status of the life-cycle approach. The continuous improvement, which is expected through cyclical models, is important in ISPs since rarely do organizations stay stagnant forever. However, there is need to critically examine the process, its tasks and recommended timespan.

Hare's theory of critical thinking provides us with a fresh view on ISP development. It urges us not to take information security rules for granted but to consider them in the specific circumstances of each organization. It guides us to focus on gathering knowledge about the situation and consider the outcomes of different choices and people's preferences. One major flaw of including only security personnel in the ISP development process is that they may have very little knowledge on how alternative rules could affect the organization or about the preferences of the people affected by the rules would have.

In this research project, we used a list of example critical considerations. Their purpose was to support the application of the method based on critical thinking into the ISP development domain. They guide both the gathering of knowledge about the organization and assessing the outcomes. The critical considerations are by no means to be taken as a complete and exhaustive list of things to consider when developing an ISP. Indeed, that would go against our view that one should not accept *prima facie* principles in new circumstances but always consider whether they apply. However, using such a list helped ConsultCo in identifying issues in ISP development that they had not covered in their previous design of the development method.

The critical considerations combine the dimensions of content, method, and context. They are intended to support the creation of a method that uses the knowledge about the context to create content. As the considerations informed the formulation of the ISP development method at ConsultCo, similar themes can be used to create a suitable method for any organization. However, the focus must always be on facilitating critical thinking by gathering knowledge about the organization, evaluating possible outcomes, and making rational choices based on the facts.

Applying the critical considerations resulted in ConsultCo changing its ISP development method from standards-based towards company-specific requirements. The focus on company-specific requirements resulted in a method that complements the business operations of the company instead of assuming that a premade information security framework would be sufficient to provide security. This approach required the participation of the personnel from all business areas to gather an adequate amount of knowledge about the organization. Once the business area representatives had spent time considering the business operations from an information security point of view, it became easier for them to make decisions about the new rules. At the end of the development process, the representatives had already considered the outcomes of the new rules, which could benefit the implementation process.

There are some lessons we can learn from using the theory of critical thinking and critical considerations as a method for ISP development. First, the mapping of business processes is important but time consuming. Workshop participants had difficulties in describing their tasks on a higher-level and identifying the use of information in these processes. This required a group effort to identify differing views and connections between processes. Second, the time between the workshops gave the participants an opportunity to process the security perspective of their daily work. They were able to get into an information security mind-set, which helped them to understand the outcomes of different choices better. These examples show how different working techniques can help the critical thinking and the extraction of information security related knowledge from the organization. Future research should look into how behavioural and cognitive theories can be used to support the use of the theory of critical thinking in an ISP development method.

This research has shown that applying the theory of critical thinking in an ISP development method can help overcome some of the problems of previous approaches. It focuses the method on the individuals whose task it is to choose the new rules for their organization. It supports the developers of organization-specific ISPs by focusing their efforts on gathering knowledge about the specific information environment. Moreover, it provides support in evaluating the information environment of the organization and identifying needs for information security actions.

Limitations

Using a consulting firm as the test organization for the method may be seen as a limitation or a strength of this study. As the consultants are not creating the policy for their own organization, their comprehension of the target organization’s inner workings might be less than perfect. Conversely, consultants have the unique ability to try the method in new settings, which would not be possible when the policy is created inside the company.

The complete study was conducted in Finland. This may have significantly affected the results, but very much in a positive way since using the native language of the subjects probably reduced their resistance significantly. However, accommodating employees’ moral judgements and providing tools to include everyone’s opinions might not be at the top of the priority list in other countries.

The three AR cycles of this study were conducted with medium-sized companies (50-250 employees). The main contribution of this article the critical considerations that can be used to support critical thinking are useable in an organization or any size. However, the examples given here on the requirements gathering and analysis may not be applicable to organizations with different structure or culture.

Conclusions

ISPs are widely accepted to be a vital part of securing business information and constitute the basis of an organization’s information security actions. There are standards and methods available for the creation of ISPs, but they do not provide adequate support for organization-specific ISP development, especially in smaller organizations. An ISP development method should not only consider the internal logic of the method but also the quality of the content and the context of the ISP. The method of critical thinking can be used as a meta-method to create rules for a specific context. The results of an AR project show that applying the meta-method of critical thinking and critical considerations can help in creating an organization-specific ISP development method. Gathering enough knowledge about the specific circumstances of the organization helped the developers choose the best-suited rules for the information security actions.

Acknowledgements

We would like to thank Business Finland and European Regional Development Fund for funding this research project. We would also like to thank Dr Michael Lapke and Dr Hadi Ghanbari for their help in creating the critical considerations.

References

Baskerville, R. 1999. Investigating information systems with action research. Communications of the AIS 2 (3), 2-31.

Baskerville, R. 1993. Information Systems Security Design Methods: Implications for Information Systems Development. ACM Computing Surveys 25 (4), 375-414.

Baskerville, R. & Siponen, M. 2002. An information security meta-policy for emergent organizations. Logistics Information Management 15 (5/6), 337-346.

Baskerville, R., Spagnoletti, P. & Kim, J. 2014. Incident-centered information security: Managing a strategic balance between prevention and response. Information & Management 51 (1), 138-151.

Burgemeestre, B., Hulstijn, J. & Tan, Y. 2013. Value-based argumentation for designing and auditing security measures. Ethics and Information Technology 15 (3), 153-171.

Chen, Y., Ramamurthy, K. & Wen, K. 2012. Organizations' Information Security Policy Compliance: Stick or Carrot Approach? Journal of Management Information Systems 29 (3), 157-188.

Coles-Kemp, L. 2009. Information security management: An entangled research challenge. Information Security Technical Report 14 (4), 181-185.

Colwill, C. 2009. Human factors in information security: The insider threat – Who can you trust these days? Information Security Technical Report 14 (4), 186-196.

Cram, W. A., Proudfoot, J. G. & D’Arcy, J. 2017. Organizational information security policies: a review and research framework. European Journal of Information Systems 26 (6), 605-641.

Da Veiga, A. & Eloff, J. 2010. A framework and assessment instrument for information security culture. Computers & Security 29 (2), 196-207.

D'Aubeterre, F., Singh, R. & Iyer, L. 2008. Secure activity resource coordination: empirical evidence of enhanced security awareness in designing secure business processes. European Journal of Information Systems 17 (5), 528-542.

Doherty, N., Anastasakis, L. & Fulford, H. 2009. The information security policy unpacked: A critical study of the content of university policies. International Journal of Information Management 29 (6), 449-457.

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

Goel, S. & Chengalur-Smith, I. N. 2010. Metrics for characterizing the form of security policies. Journal of Strategic Information Systems 19 (4), 281-295.

Hare, R. M. 1981. Moral thinking : its levels, method, and point. Oxford : New York: Clarendon Press ; Oxford University Press.

Hedström, K., Kolkowska, E., Karlsson, F. & Allen, J. P. 2011. Value conflicts for information security management. The Journal of Strategic Information Systems 20 (4), 373-384.

Höne, K. & Eloff, J. 2002. Information security policy — what do international information security standards say? Computers & Security 21 (5), 402-409.

ISO/IEC 27002 2013. Information technology - Security techniques - Code of practice for information security controls. International organization for standardization.

Karjalainen, M. & Siponen, M. 2011. Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches. Journal of the Association for Information Systems 12 (8), 518-555.

Karyda, M., Kiountouzis, E. & Kokolakis, S. 2005. Information systems security policies: a contextual perspective. Computers & Security 24 (3), 246-260.

Klaic, A. 2010. Overview of the state and trends in the contemporary information security policy and information security management methodologies. MIPRO, 1203-1208.

Knapp, K. J., Morris, F. R., Marshall, T. E. & Byrd, T. A. 2009. Information security policy: An organizational-level process model. Computers & Security 28 (7), 493-508.

Lapke, M. & Dhillon, G. 2008. Power Relationships in Information Systems Security Policy Formulation and Implementation. 16th European Conference on Information Systems (ECIS).

Lopes, I. & Sá-Soares, F. 2010. Information Systems Security Policies: a Survey in Portugese Public administration. IADIS International Conference Information Systems.

Maynard, S. B., Ruighaver, A. B. & Ahmad, A. 2011. Stakeholders in Security Policy Development. 9th Australian Information Security Management Conference.

Mcfadzean, E., Ezingeard, J. & Birchall, D. 2007. Perception of risk and the strategic impact of existing IT on information security strategy at board level. Online Information Review 31 (5), 622-660.

Niemimaa, E. & Niemimaa, M. 2017. Information systems security policy implementation in practice: from best practices to situated practices. European Journal of Information Systems 26 (1), 1-20.

Pounder, C. 1999. The revised version of BS7799 — so what's new? Computers & Security 18 (4), 307-311.

Rees, J., Bandyopadhyay, S. & Spafford, E. 2003. PFIRES: A Policy Framework for Information Security. Communications of the ACM 46 (7), 101-106.

Saleh, M. 2011. Information Security Maturity Model. International Journal of Computer Science and Security 5 (3), 316-337.

Siponen, M. & Iivari, J. 2006. Six Design Theories for IS Security Policies and Guidelines. Journal of the Association for Information Systems 7 (7), 445-473.

Siponen, M. 2006. Information security standards focus on the existence of process, not its content. Communications of the ACM 49 (8), 97-100.

Soomro, Z. A., Shah, M. H. & Ahmed, J. 2016. Information security management needs more holistic approach: A literature review. International Journal of Information Management 36 (2), 215-225.

Soto Corpuz, M. 2011. The Enterprise Information Security Policy as a Strategic Business Policy within the Corporate Strategic Plan. The 8th International Symposium on Risk Management and Cyber-Informatics: RMCI 2011, 275-280.

Sterne, D. 1991. On the buzzword security policy. IEEE Computer Society Symposium on Research in Security and Privacy.

Talbot, S. & Woodward, A. 2009. Improving an organisations existing information technology policy to increase security. 7th Australian Information Security Management Conference.

Trček, D. 2003. An integral framework for information systems security management. Computers & Security 22 (4), 337-360.

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

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

Wood, C. C. & Parker, D., B. 2004. Why ROI and similar financial tools are not advisable for evaluating the merits of security projects. Computer Fraud & Security 2004 (5), 8-10.

Yeniman Yildirim, E., Akalp, G., Aytac, S. & Bayram, N. 2011. Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. International Journal of Information Management 31 (4), 360-365.