State of the Art in Information Security Policy Development

Hanna Paananen , Michael Lapke , Mikko Siponen

PII: S0167-4048(18)31300-2
DOI: https://doi.org/10.1016/j.cose.2019.101608
Reference: COSE 101608

To appear in: *Computers & Security*

Received date: 15 November 2018
Revised date: 23 August 2019
Accepted date: 6 September 2019

Please cite this article as: Hanna Paananen , Michael Lapke , Mikko Siponen , State of the Art in Information Security Policy Development, *Computers & Security* (2019), doi: https://doi.org/10.1016/j.cose.2019.101608

State of the Art in Information Security Policy Development

Hanna Paananen, Michael Lapke & Mikko Siponen

Abstract

Despite the prevalence of research that exists under the label of "information security policies" (ISPs), there is no consensus on what an ISP means or how ISPs should be developed. This article reviews state-of-the-art ISP development by examining a diverse sample of literature on the subject. The definition and function of an ISP is studied first, revealing a rich tapestry of different notions behind the same term. When looking at the broad picture of the research on ISP development methods, we find different phases and levels of detail. Analyzing the different views on the content, context, and strategy alignment provides for further understanding on the complexity of the matter. As an outcome, we raise issues in ISP definitions and development methods that should be addressed in future research and practical applications. This review concludes that for state-of-the-art ISP development, the focus should shift more toward organization-specific information security needs, as the direction of the current research is still lacking contributions that would show how contextual factors could be successfully integrated into ISP development.

Key words: information security policy, literature review, policy development, development method, concept definition

1 Introduction

Organizations today operate in an environment where information is given increasing value and, at the same time, new methods are constantly evolving for the malicious use of this information. This has led organizations in all fields to look for ways in which to protect their information assets. A number of information security management textbooks highlight the necessity of having information security policies (ISPs) in organizations (Abrams & Bailey, 1995; Whitman, 2008). Additionally, information security standards such as ISO27001 (ISO/IEC 27001, 2013, pg. 11) prescribe ISPs as mandatory for information security management.

However, it has been reported that for some reason many organizations do not develop ISPs regardless that they recognize their importance and are aware of existing standards or frameworks (Abu-Musa, 2010; Yeniman Yildirim, Akalp, Aytac, & Bayram, 2011). In fact, there is still need for further research in what a good ISP means and how it should be developed (Baskerville & Siponen, 2002; Cram, Proudfoot, & D'Arcy, 2017). For example, the standards, while regulating for ISPs to be mandatory, provide little advice on how good policies are developed and what makes them effective (Höne & Eloff, 2002; Karyda, Kiountouzis, & Kokolakis, 2005; Siponen, 2005; Siponen & Willison, 2009). Over the years, many authors have provided guidance on development methods for ISPs (Flowerday & Tuyikeze, 2016; Knapp, Morris, Marshall, & Byrd, 2009; Olnes, 1994; Rees, Bandyopadhyay, & Spafford, 2003). While these methods are valuable, their ability to solve organizations' problems in in ISP development is not clear.

To come to the best possible understanding of ISP development in current research, the relevant literature should be analyzed. A few literature reviews have been undertaken before in this area. Klaic (2010) analyzed the definitions and methodologies of ISPs and information security management using a rather limited set of articles. Siponen and Willison (2007) did an extensive systematic literature review on information systems (IS) security research, analyzing the theories, methods, and aims of research papers from 1990–2004, but they did not focus solely on ISP development. Silic and Back (2014) reviewed information security research up to the year 2013 with similar research questions to those of Willison and Siponen (2007). Cram, Proudfoot, and D'Arcy (2017) examined

the ISP research by identifying key constructs and research gaps. Soomro, Shah, and Ahmed (2016) identified the roles of management in regard to ISPs. Dhillon and Backhouse (2001), Baskerville (1993), Siponen (2005), and Siponen and Oinas-Kukkonen (2007) studied the literature on IS security, including the organizational element.

This paper is differentiated from previous works as follows. Our review aims to understand what are the extant ISP development methods, their differences, and their relationships in terms of their content, context, and strategy. Additionally, we want to find out what are the different definitions and functions of ISPs. The previous works have not examined these specific questions. By answering these questions, we hope to gain a better understanding of the current state of ISP development methods and their research as well as their differences and issues. Purely technical policy development as well as compliance and awareness issues are outside the scope of this review.

The rest of this article is constructed as follows. First, we will explain our methodology. Then the following section will examine the different definitions and functions given to ISPs. The second section analyzes different approaches to ISP development by looking at the process, content, context, and business-strategy alignment. In the last sections, we will discuss the findings and provide conclusions.

2 Methodology

The literature for this review searched using the guidelines provided by Levy and Ellis (2006). First, a broad search was conducted on Google Scholar using search terms such as "information security policy" AND "development" to find papers on ISPs, and especially to find papers that would answer the research questions. Around 70 articles with promising topics were chosen as a starting point. Upon closer inspection, most of the articles did not answer the research questions. Most of the discarded articles were examples of actual ISPs or papers that did not focus on ISP development. After the screening process, less than 30 articles remained in the sample. After the Google Scholar searches, another search targeting solely academic literature was conducted using Elsevier's Scopus search engine (see Appendix 1). This search included prominent journals in the fields of information security and information systems without limitations on the year of publication. The search yielded a list of 87 articles, which were then evaluated first by excluding clearly non-related papers by title and then by doing a more detailed selection on the basis of the abstracts. The main reasons for exclusion were purely technical approaches and papers discussing ISPs only post implementation with no clear implications to ISP development. Some papers from the latter group were however included if they presented clear implications for ISP development. After the two elimination rounds the list had 29 articles and partly overlapped with the Google Scholar list. Then a backwards reference search was conducted from sample articles using their reference lists to find promising topics. For the most promising articles, a forward author search was also conducted to find the recent papers written by those authors. After all the searches had been undertaken, 87 articles on ISPs were chosen for the sample. Using this method for the literature search allowed us to gain a varied sample that was rich in alternative approaches, which might not have been possible if the focus had been on only a few specific journals or key words.

2.1 Articles

In this review, we use 87 articles on ISPs to create an overall picture of the current state of ISP development research. Most of the articles were published in academic journals (71) and the largest number of papers from a single journal was from *Computers and Security* (22). Twelve articles were from conferences and four were other publications. A list of the publications is provided in appendix two.

Since most of the papers were published as academic research, we also grouped them by research approach. Most (29) of the papers used for this review are conceptual in nature, proposing solutions in the ISP field yet not providing any empirical evidence. Most of the empirical research used surveys as the research method (17). A list of the research approaches is provided in Appendix 3.

3 The many meanings of the term "information security policy"

In this section, we will examine the definitions and functions of ISPs described in the literature. In many cases, ISPs are not clearly defined in the research articles and a single definition has not become dominant in the research on ISPs. Existing studies adopt different definitions of ISPs and studying them helps us in understanding the different approaches taken.

An ISP may refer to a technical or managerial policy (Baskerville & Siponen, 2002). ISPs under automated access control policies are widely studied in computer science in general and database security in particular (Sandhu & Samarati, 1994). The historical development and differences between different automated access control policies are fairly well known. For example, automated access control policies have been classified into different categories such as mandatory access control, discretionary access control, and role-based access control (Sandhu et al. 1996). In addition to automated access control policies, the term "information security policy" is also widely used in articles and textbooks in the IS and information security management disciplines (Baskerville & Siponen 2001). Therein, an ISP refers to document(s) regulating human actions regarding information security or expressing the organization's information security aims. A slightly narrower term is the information systems security policy that may be issued by the IT department (Balozian & Leidner, 2017) and cover only IT assets. This paper focuses on the managerial view of ISPs and excludes access control policies in database security. Furthermore, given our focus on organizational ISPs, cyber security policy development by governments is outside the scope of this paper.

In the ISP literature, the most-used terms are "security policy" and "information security policy." Some authors use these interchangeably, while others stress the difference between them (Klaic & Hadjina, 2011; Soto Corpuz, 2011). There are also different views on how information security-related directives should be connected to each other. Many authors recommend a comprehensive policy architecture with related documents from the strategic to operational levels, which all are called policies (Von Solms, Thomson, & Maninjwa, 2011). Technical and managerial policies are often mentioned as separate but interconnected (Baskerville & Siponen, 2002; Cram et al., 2017). Some authors refer to ISPs only when talking about high-level policies, therefore they exclude more specific guidelines or procedures as they are viewed as being outside the scope of ISPs (Klaic, 2010; Soto Corpuz, 2011).

3.1 Different definitions and functions of ISPs

Since there is so much variation in the use of the term "ISP" in the literature, it helps to gain an overall picture of the concept by examining the definitions and functions in detail. Table 1 summarizes the characteristics and functions of ISPs found in the literature. In general, it can be stated that the definitions and functions of ISPs are not explicitly discussed in many articles. Often, it seems to be expected that the reader already knows what the ISP comprises of and what it is expected to do in an organization.

	ISP characteristics	**ISP functions**
Steering the organization	Statement of security goals/strategy	Supports business goals
	Guidance/instruction	Control
	Statement of rules	Basis for performance measuring
The actor and the asset	Defines subjects	States responsibilities and authority
	Defines objects	Provides overview of information assets
Preparing for incidents	Comprehensive plan	Basis for security culture
	Addresses risks	Prevents loss/misuse of information
	Recovery plan	Ensures continuity
	Communication tool	Evidence of IS program

Table 1: ISP characteristics and functions

3.1.1 Steering the organization

An ISP is often described as the declaration of a desired state of security and it employs words such as "security goals," "strategy," "objectives," "intentions," and "desirable achievements." Some definitions also mention the policy as a reflection of values and beliefs (Hedström, Karin, Kolkowska, Karlsson, & Allen, 2011). Klaić (2010, pg. 1204) describes this as follows: "The IS policy document in the narrow sense represents a statement or declaration of the most important management persons (CEO, Executive Board, Minister...), about beliefs, goals, and reasons, and also general ways to accomplish desirable achievements in the field of information security." Many authors also recommend that the ISP should maintain and complement the organization's overall business goals (Anton & Earp, 2000). Saleh (2011) stated that the intention is not only to achieve security objectives (integrity, availability, confidentiality), but to ensure that the organization achieves its mission despite accidents and attacks against its information systems. From a policy-architecture point of view, these goals are usually stated in the higher-level documents (Baskerville & Siponen, 2002).

An ISP offers security direction for organizations to implement their information security management (Soto Corpuz, 2011). IT can be viewed as a tool that the management uses to communicate its vision and guide the rest of the organization (Sommestad, Hallberg, Lundholm, & Bengtsson, 2014; Von Solms et al., 2011). The instructions regarding actions (directions, guidance, procedures, instructions, methods, acceptable use) are mentioned in many articles as part of the user guidelines or lower-level security policies (Baskerville & Siponen, 2002; Burgemeestre, Hulstijn, & Tan, 2013; Galletta & Hufnagel, 1992; Sommestad et al., 2014). For example, Cram et al. (2017, pg. 607) described the content of issue-specific policies as follows "[they] include guidelines and procedures (i.e., acceptable use policies) that employees must adhere to in their daily interactions with information and technology resources." The function of the policy architecture is to support comprehensive control over information use (Von Solms et al., 2011). It can be seen as a precondition for implementing effective deterrents and it can state penalties and countermeasures (Balozian & Leidner, 2017; Doherty, Neil & Fulford, 2005; Knapp et al., 2009; Rees et al., 2003). Documented policy can also protect the company in case there are legal disputes over penalties (Tuyikeze & Pottas, 2010). While deterrence by penalties is a popular topic in the compliance literature, its counterpart, the reward, is not as widely studied (Chen, Ramamurthy, & Wen, 2012; Sommestad et al., 2014).

Depending on the definition, the ISP can function as a source of rules and protocols. Some see the ISP as a rulebook to be followed by all users of the organization's information (Yeniman Yildirim et al., 2011). Ward and Smith (2002) point out that ISPs provide security controls and protocols to guarantee the security of information systems. Klaić (2010) calls these required actions procedures, and states, that in addition to them, the policy should also describe guidelines on how these procedures can be followed. As the perceived role of the policy subject differs between texts, so does the need for absolute rules versus tools for independent decision-making (Ruighaver, Maynard, & Warren, 2010). Rule-based ISPs demanding absolute compliance suit organizations with stable environments and rule-oriented organizations (Siponen & Iivari 2006). Alternatively, organizations operating in volatile environments could adopt design theory for their ISPs that allow for security-related decisions to be made while adapting to new situations (Siponen & Iivari, 2006).

Metrics can be formed to measure the stated procedures or tangible goals of the policy. Von Solms, Thomson, and Maninjwa (2011, pg. 3) explain measuring as a form of control "control is normally exercised by capturing data at the lowest levels of execution and control: measuring compliance against the operational level policies". The policy could be designed in a way that its performance can be monitored and linked to monetary value. Some have suggested general quantitative metrics that the management can use to make information security decisions such as the return on the security investment (ROSI), fault tree analysis (FTA), the certainty factor (CF) and remedy allocation based on end effect cost (Klaic, 2010; Shirtz & Elovici, 2011). The sense of making these kinds of calculations may be questioned since there is no guarantee that making security initiatives would contribute towards better performance of the company or its supply chain (Sindhuja, 2014).

3.1.2 Addressing the actor and the asset

Baskerville and Siponen (2002) use the terms "information security subjects" and "objects" to distinguish between the actors affected by the policy and the information assets being protected. The function of a policy can be to help all the individuals affected by the policy (subjects) to make decisions about their actions when handling information (objects). The rights and responsibilities of the organization members are stated to help them make future decisions when handling information (Baskerville & Siponen, 2002; Doherty, Neil, Anastasakis, & Fulford, 2009; Siponen, 2005). It is important to remember that the policy is meant for the legitimate users of the information (Yeniman Yildirim et al., 2011), which may also include users external to the organization (Sindhuja, 2014). Some roles may also include the authority to make security decisions, approve other users' actions, and change the ISP (Goel & Chengalur-Smith, 2010; Ward & Smith, 2002; Wood, 1995). Some authors warn us about making overly simplistic assumptions about the authority of security decisions residing at the top tier of the organization and recommend an analysis of the actual power structure which may differ across organizations and cultures (Asai & Hakizabera, 2010; Coles-Kemp, 2009; Dinev, Goo, Hu, & Nam, 2009; Lapke & Dhillon, 2008).

The objects of the policy are usually described as information assets, systems, and data. In their definition, Abrams and Bailey (1995, pg. 128) focused on the object of the policy: "The policy should address the information assets of the organization, threats to those assets and the measures the management has decided are reasonable and proper to protect those assets." Some authors consider the ISP a part of IT governance (Abu-Musa, 2010) but others also mentioned that the policy should not be technology-specific (Klaic, 2010; Rees et al., 2003). Listing the assets and their levels of protection, can be useful to personnel enforcing the ISP (Lopes & Sá-Soares, 2010). In a broader scope, information is used by technology, stakeholders, and processes, which all affect the requirements for the protection of that information (Posthumus & Von Solms, 2004)

3.1.3 Preparing for incidents

It has been said that "security is how well you adhere to your formal security policies" (pg. 504, David, 2002) or in other words, there is no information security without an ISP. Hopefully this is not completely true, since a large portion of companies (7-58% depending on the study) operate without an ISP (Abu-Musa, 2010; Doherty, N. F. & Fulford, 2006; Yeniman Yildirim et al., 2011). Regardless, an ISP is an important mechanism in detecting, preventing and responding to security breaches (Doherty, N. F. & Fulford, 2006; Höne & Eloff, 2002; Horacio, Caceres, & Teshigawara, 2010).

The planning phase of ISP development can start by building security consciousness in the organization, thus guiding the organization into forming a secure working environment. This forces the company to plan ahead for the possibility that its information resources might encounter an attack or accident (Maynard, Ruighaver, & Ahmad, 2011). The ISP highlights the policy creators' (e.g. executive management's or IT department) commitment to security and it envisages an "ideal" operational environment (Balozian & Leidner, 2017; Ward & Smith, 2002). The policy-planning process creates an understanding of the need for security and defines acceptable security levels to protect information (Klaic & Hadjina, 2011; Ward & Smith, 2002; Yeniman Yildirim et al., 2011). The ISP can guide the information security culture of the organization so that the members help each other to prevent incidents (Asai & Hakizabera, 2010; Da Veiga & Eloff, 2010). The ISP should create a secure environment where the privacy of its subjects and other stakeholders is also considered (Talbot & Woodward, 2009).

The ISP can be derived from the strategic requirements for risk management (Soto Corpuz, 2011), whereby the strategic-level decision-makers use the policy as a tool to reduce the risk to the company's information assets. The most commonly used ways to describe risks to information are ensuring confidentiality, integrity, and availability (Glasgow, Macewen, & Panangaden, 1992; Gritzalis, 1997). Some authors add non-repudiation to the list (Siponen & Oinas-Kukkonen, 2007), or substitute availability with assured service (Sterne, 1991), or identification and authorization (Trompeter & Eloff, 2001). Some authors, however, see this approach as being too IT-centered or

vague (Dhillon, Gurpreet & Torkzadeh, 2006; Doherty, Neil et al., 2009; Sterne, 1991). Many have adopted a broader view where the planned protection and sharing of information is a vital part of creating business value (Ashenden, 2008).

In addition to preventing risks, the ISP may also serve as a plan to recover from materialized risks if continuity is coupled with information security (Baskerville, Spagnoletti, & Kim, 2014; Niemimaa & Niemimaa, 2019). ISP can guide the investigation of security incidents and provide procedures, for example, documenting the incident and containing it to limit further damage (Rees et al., 2003). A responsive way of dealing with risks is especially useful in organizations that operate in unpredictable markets (Baskerville et al., 2014). As information and IT provide companies with the means through which to operate and gain a competitive advantage, businesses must rely on their continuous availability even when risks materialize. To secure the continuation of operations, company boards should be interested not just in good IT governance but also in information security (Abu-Musa, 2010; Mcfadzean, Ezingeard, & Birchall, 2007).

As a collection of documented statements, the ISP in itself can be seen as a communicative object (Karlsson, Hedström, & Goldkuhl, 2017). An organization may develop an ISP to show evidence of its information security actions that comply with regulations and standards (Cram et al., 2017; Whitman, 2008). The evidence of being prepared for information security incidences may also be of interest to external stakeholders such as customers and partners. An ISP is viewed as the foundation of the information security efforts in a company (Lopes & Sá-Soares, 2010) and a written policy can be accepted as proof that work has been done to improve information security. Evidence of an ISP may be needed in court if the company's actions are challenged (Whitman, 2008).

As companies' perception of risks, resources, and management-styles differ, so do the different definitions and functions of ISPs. Due to these different views, the literature also provides multiple different ways in which to develop an ISP that should fulfill the expectations regarding its nature and use.

4 ISP development methods

There are many different approaches available for ISP development. The methods recommended for developing ISPs have become more complex over the years, as have systems and organizations (Baskerville, 1993; Klaic, 2010). Baskerville (1993) studied security design methods through generations of IS development methods. They included checklist methods, mechanistic engineering methods, and logical-transformational methods.

Companies have multiple methods to choose from, but selecting the right one may be difficult. To help with this, a method exists for choosing the right information security approach where a business falls into one of four types (low/high perception of risk and the aim of IT use being either for an operational tool/competitive advantage) (Mcfadzean et al., 2007). The organization's information security goals also affect the choice of approach. Saleh (2011) created an information security maturity model (ISMM) for assessing the organization's capability to meet its security goals with five levels of compliance.

Since ISPs affect the organization, many authors recommend approaches that connect the ISP lifecycle to existing processes. Tying ISP development and maintenance to general management and strategic processes has become an increasingly popular approach (Klaic, 2010; Soto Corpuz, 2011). The alignment of processes can be undertaken on all levels from strategic to operational. One approach to highlight information flows and security concerns in operational-level business processes is via modeling languages such as Secure activity resource coordination (SARC) and the enriched-use case (D'Aubeterre, Singh, & Iyer, 2008).

The information security policy architecture (ISPA) suggests that policies should be created first at the highest level of the organization and then these strategic-level policies should be expanded or disseminated to tactical and operational levels as more detailed policies (Von Solms et al., 2011). The ISPA was created due to the observation that operational-level policies were not always in line with higher-level policies, since they were created by the staff to support daily operations. This is in line

with the view of Coles-Kemp (2009), who finds that decisions are not always made using the formal power structure. Lapke and Dhillon (2008) provide a method based on the circuits of power to map the power relationships in the organization and choose the right people to participate in the formulation of the policy.

There are differences in developing technical and managerial policies. Technical policies can be designed with logical formulas that describe how the system should operate (Glasgow et al., 1992). Earlier takes on organizational ISPs were similarly simpler since the variety of information and communications technology (ICT) solutions was smaller in organizations and views on the human factor received less attention. For example, Wood (1995) proposed that policies should be developed by gathering reference materials, deciding on a framework, and preparing a coverage matrix to check for the coverage between control categories and audiences. This view is an example of the observation that traditional security methods tend to reuse some underlying assumptions such as control orientation (Siponen, 2005).

4.1 Phases in ISP development

How ISP policy development is conducted has been described using a number of different approaches. A common practice is that the ISP development process is part of a larger lifecycle model. This view is commonly accepted and described in numerous textbooks with recommendations for the responsible personnel, tasks, and outcomes (Howard, 2003). A comparison between some exemplar ISP development models is depicted in Figure 1. These models are process-level representations of the entire ISP lifecycle. The different phases in the models have been presented as linear processes to highlight the similarities between the models. However, many of these original models recommend iterations in one or multiple phases.

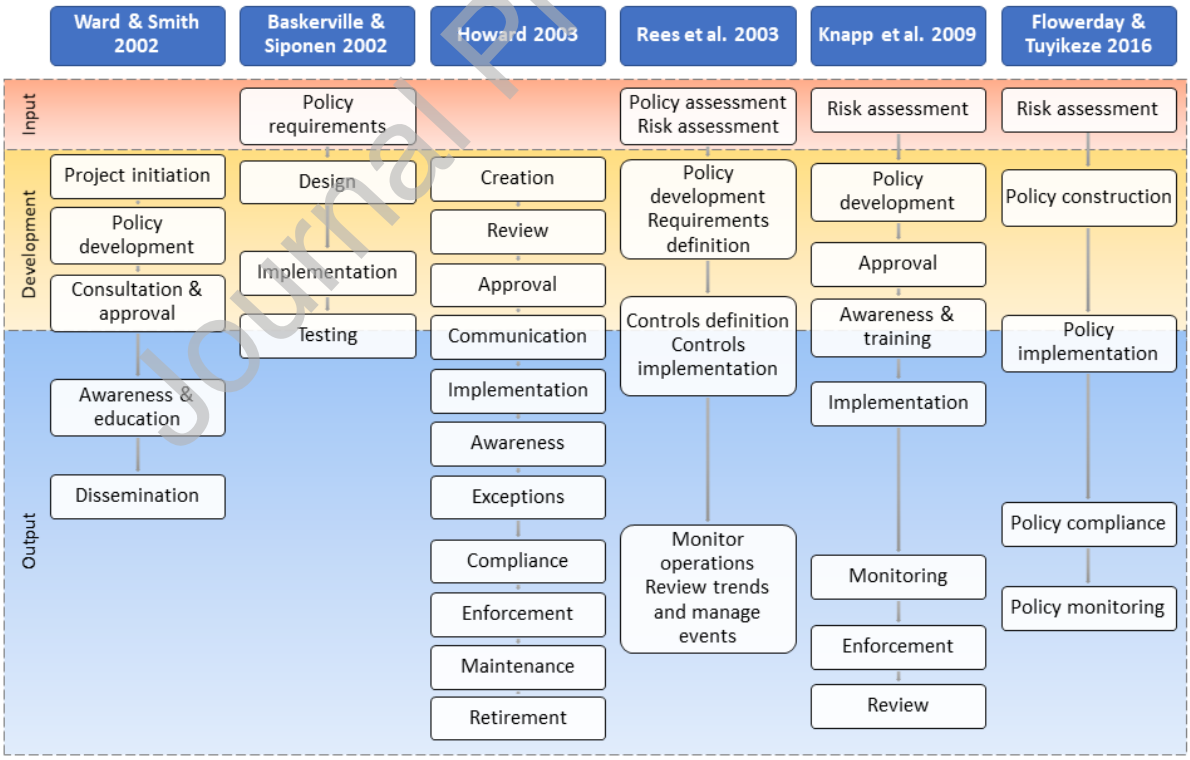

Figure 1: Process models for ISP development

Ward and Smith (2002) described five distinct phases in the development of an access control policy. This developmental method does not prescribe the input and analysis of raw data but describes the processing and outputs of the policy in detail. There are no explicit instructions for risk assessment or requirement-gathering, although they are mentioned as important. The other phases include policy development, consultation, awareness, and dissemination.

One major problem with stating general, "one-size-fits-all" policy development methods is the different characteristics and environments the organizations have. An *information security meta-policy* has been proposed to tackle this problem in emergent organizations where the policy might need frequent updates (Baskerville & Siponen, 2002). In the meta-policy the main requirements for creating a policy are the identification and classification of policy subjects and objects. Then the design process determines the architecture and scope of the policies. Lastly, the policy is implemented and tested. Baskerville and Siponen (2002) argue that following through with this strategic approach, it would assist in tailoring the policy to the organization in question.

Howard (2003) proposed eleven functions that must be performed during a security policy lifecycle: creation, review, approval, communication, implementation, awareness, exceptions, compliance, enforcement, maintenance, and retirement. The creation function contains many separate components that involve gathering the data, analyzing, and creating all at the same time. Some functions of this lifecycle are quite granular compared to other lifecycle models. For example, approval, communication, implementation, awareness, and exceptions could all be considered part of the implementation phase.

A *Policy Framework for Interpreting Risk in eCommerce Security* (PFIRES) (Rees et al., 2003) is cyclical in nature and consists of four stages (assess, plan, deliver, and operate), which all contain two sub-steps (see Figure 1). This lifecycle framework is stronger in describing the tasks in the input, development, and implementation stages as a policy moves through the lifecycle process. The method does not consider long-term maintenance issues nor discuss how the input might be analyzed prior to policy construction. The PFRIES has been critiqued for not supporting the translation of policy recommendations into requirements, and the suggested solution is *Goal-based requirements-gathering* (GBRAM) (Anton & Earp, 2000).

Knapp et al. (2009) created an organization-level process model that reaches outside the ISP development team and includes internal and external influencing factors. The model includes many iterations within and between different phases. The input is described as risk assessment, followed by policy development, approval, awareness and training, implementation, monitoring, enforcement, and review. This model also acknowledges the retirement of the policy, audits, and automated monitoring tools.

Another broad-reaching approach to ISP development was prescribed by Flowerday and Tuyikeze (2016). Again, risk assessment is prescribed as a primary input device into the process. This is followed by policy construction, policy implementation, policy compliance, and policy monitoring. Like the development framework PFIRES (Rees et al., 2003) and organization-level process model (Knapp et al., 2009), this method describes a cyclical process. It also describes additional inputs and motivations into the process including security policy guidance, security policy drivers, existing theories, management support, and employee support. The mechanisms for implementing the method or additional inputs are not discussed further than naming the stakeholders who are to be included in the process.

Figure 1 portrays the simplified versions of these ISP development methods for comparison. From these models, we can distinguish activities in the ISP development process input, development, and output. In the following sections, the development process is considered to consist of all the steps of the process that include creating or changing the content of the ISP. Inputs and outputs include other steps or processes that are linked to ISP development.

4.1.1 Before the development process

Before the actual ISP development process can begin, there are some steps that must occur in the organization to provide inputs for the process. There must be an initial decision made to start ISP development and some actions must be undertaken to analyze the current state of the organization. Herein, we treat the knowledge-gathering and analysis as a previous, separate process from the ISP's formulation. In reality, knowledge-gathering and policy development may also happen simultaneously in a rapid feedback loop (Knapp et al., 2009).

How an ISP is planned should be informed by the state of the organization and the state of security within that organization. Cram et al. (2017) identified three factors from previous research that influence ISP design: standards and regulations; the desired format; and internal and external risks. The approach for assessing the current situation and designing the ISP can have a top-down approach (standards, best practices) and/or a bottom-up approach (contextual, work-system originated) (Niemimaa & Niemimaa, 2019).

Trček (2003) offered a framework for IS security management and policy formulation. For the formulation of a security policy, this framework suggests adhering to the British standard, BS7799. This standard considers an input–process–output model for the creation of a security policy. The "input" for the framework includes reviewing the legislation, contractual obligations, standards, and requirements. The "process" of the framework includes analyzing the security organization, the control and assets, physical and environment security, personnel security, access control, and compliance. Solic et al. (2015) proposed a similar comprehensive evaluation, with a model that could calculate a wide range of security related areas into simple grades.

Trček's (2003) framework, along with many others (Burgemeestre et al., 2013; Cram et al., 2017; Horacio et al., 2010; Whitman, 2008), calls for the use of standards and legislation as inputs for the process. Common examples of laws affecting the formulation of ISPs are the Sarbanes–Oxley and Health Insurance Portability and Accountability Act (HIPAA) in the USA and the General Data Protection Regulation (GDPR) in the EU. Some standards like ISO27000 series (ISO/IEC 27001, 2013) or frameworks like COBIT (ISACA, 2019) may support the development of an ISP that complies with the law (Haworth & Pietron, 2006) but often the burden of fitting the two sets of external requirements together falls on the organization (Burgemeestre et al., 2013).

Many scholars warn against relying too much on predefined requirements such as standards when planning for information security (Cram et al., 2017; Dhillon, Gurpreet & Backhouse, 2001; Hedström, Karin et al., 2011). These approaches often rely on identifying persistent general risks but may overlook company-specific threats such as targeted attacks that are specifically designed for the organization by exploiting its weaknesses (Baskerville et al., 2014). These top-down approaches also need to be adapted to an organization, which in turn requires bottom-up approaches to understand local work practices. These two approaches may cause tensions that need solving mechanisms in the ISP development process (Niemimaa & Niemimaa, 2019).

The cyclical frameworks in Figure 1 (Knapp et al., 2009; Rees et al., 2003) acknowledge that there may be a previous policy that can be assessed in light of compliance, security incidents, and current requirements. The frameworks also recommend a risk assessment where the threats and vulnerabilities of the information assets are identified (Tuyikeze & Pottas, 2010). This can involve identifying threats, calculating values for assets, and evaluating business requirements from the information security standpoint (Flowerday & Tuyikeze, 2016; Rees et al., 2003; Tuyikeze & Pottas, 2010). Risk assessment in itself is an entire research area in both information security, and business management.

Baskerville (1993) created a taxonomy of three generations of IS security design methods: checklists, mechanistic engineering methods, and logical-transformational methods. Siponen (2005) continued the previous work by applying a theoretical perspective toward comparing the underlying assumptions of the major IS security methods: checklists, standards, maturity criteria, risk management, and formal methods. In this comparison, it can be seen that the methods prescribed by the practitioner-oriented papers fell into the first two generations. The "security principles" created for the healthcare field (Anderson, 1996; Gritzalis, 1997) imply a generic checklist (1st-generation IS security methods). The

call for standards as a critical form of input (Trček, 2003) typifies a 2nd-generation IS security method. This theoretical view is important for the analysis of IS security policy formulation because it demonstrates the existence of the continuing need for evolution in ISP methods. As research progresses, a more nuanced and detailed view of the required inputs for planning ISPs has become apparent.

4.1.2 ISP development

The policy development process itself consists of using the inputs to the process to design and formulate the ISP as an output. The design may include the policy architecture (Baskerville & Siponen, 2002; Von Solms et al., 2011), determining abstraction levels (Baskerville & Siponen, 2002), language format (Goel & Chengalur-Smith, 2010), and document format (Baskerville & Siponen, 2002). Although this is an area of IS development that is lacking in research, some themes can be induced from the literature. In this section, we cover all the phases of the development process that are related to designing, creating, or changing the contents of the ISP.

The phase involving the analysis of requirements from the policy inputs and the design of the form of the policy is not widely discussed in the literature. There may be a general list of topics to choose from and the choice of making several policies hierarchically (Baskerville & Siponen, 2002; ISO/IEC 27002, 2013; Von Solms et al., 2011), but the process of making organization-specific choices is not widely discussed. The concept of designing a policy based on the flow of information from a planning stage is mentioned in many articles but has not been researched as much. References have been made to strategizing and planning policy formulation (Baskerville & Siponen, 2002) but not in the wider context of the overall ISP lifecycle.

Depending on the architecture chosen for the ISP (Von Solms et al., 2011), the different level policies may need different development teams. Strategic-level policies may need input from the same people who created the business strategy, while different business units such as IT or human resources may develop the lower-level operational policies. The internal staff may be supported by consultants (Gritzalis, 1997). Whoever the actual developers are, they should have a comprehensive enough view of the operations of the company. For example, the IT department alone rarely has this knowledge, which may lead to an overly-technical ISP (Maynard et al., 2011). The positive side of including staff in ISP development is, that the implementation of the policy starts with the developers during the development process (Niemimaa & Niemimaa, 2019)

Trompeter and Eloff (2001) provided a framework for the implementation of socio-ethical controls in IS security. One of the main points of Trompeter and Eloff is that people should be placed at the center of the equation, rather than at its periphery by creating an ISP that includes socio-ethical issues (Trompeter & Eloff, 2001). One way to improve the effectiveness of these kinds of controls is to include staff in designing them to ensure that they do not conflict with people's information use rationale (Balozian & Leidner, 2017; Hedström, K., Karlsson, & Kolkowska, 2013). The local national culture affects the effectiveness of different controls, which is why understanding the local social norms and social control mechanisms is important when designing the ISP (Asai & Hakizabera, 2010; Dinev et al., 2009)

The content of the ISP documentation may vary greatly across organizations depending on the design principles they have adopted in forming it (Siponen & Iivari, 2006). The documentation may include only general statements and rationale, or details of responsibilities and countermeasures as well (Olnes, 1994). The statements in the ISP may vary from encouraging right actions and compliance to deterrence oriented with penalties for wrong actions (Balozian & Leidner, 2017; Siponen & Iivari, 2006).

Choosing the right format for the policy is not an insignificant task since it determines how the policy can be communicated to the stakeholders when it is finished. Defining key concepts in the document is often advised (Höne & Eloff, 2002; Trček, 2003) since the developers of the policy and the readers may understand the key concepts differently (Hedström, Karin et al., 2011). Keeping the text short and to the point helps in getting the message through (Goel & Chengalur-Smith, 2010). The impact of ISP characteristics on later compliance is not widely studied and there are contradictory findings of

the effects of policy characteristics (level of detail) on the later occurrence of security incidents (Balozian & Leidner, 2017).

Before the ISP can be implemented, it may need to go through an approval process. First, the development group should try to reach a consensus which the information security director should approve (Lindup, 1995). Different business areas can also review the content in order to eliminate ambiguity and difficulties in implementation (Talbot & Woodward, 2009). Most often, the approval phase refers to a formal approval from the organization's executive management (Flowerday & Tuyikeze, 2016; Höne & Eloff, 2002). Management's commitment to information security is important or the subject may not receive adequate time and attention in meetings (Talbot & Woodward, 2009). Approval from the highest level gives a credible mandate to implement the policy and demand compliance (Höne & Eloff, 2002; Soomro et al., 2016; Wood, 1995).

Baskerville and Siponen (2002) state that it is also necessary to test the new policy. The tests or reviews should check that the policy meets the requirements, matches the design, and reveals problems in implementation such as new threats (Baskerville & Siponen, 2002; Rees et al., 2003). Even pilot testing (Rees et al., 2003) or testing contingency plans in "real" situations (Mcfadzean et al., 2007) can be considered. The policy can go through different kinds of tests throughout the development process. Usually, with development methods, testing is carried out after acceptance and implementation. However, since testing may still result in changes to the ISP, it should be considered a part of development efforts.

Here, we have limited the ISP development process to only include tasks that create or change the policy document. In general, implementation is usually considered to happen after the ISP is ready. However, depending on the definition of the ISP, the implementation process can include developing sub-policies, which would make this phase a part of development efforts (Abrams & Bailey, 1995). Similarly, if the implementation efforts include testing that may lead to changes in the content, then it is still a part of the development process. Testing can also be a part of the maintenance phase of the completed policy and, in this situation, it functions as a tool to detect the need for a new development cycle (Olnes, 1994).

4.1.3 Outputs of the development process

The output of an ISP development project is the policy documentation. The literature on ISP development usually names tasks for the completed policy such as implementation, maintenance, enforcement, and monitoring (Figure 1). With technical ISPs, implementation is the process of putting a system into use and can include areas such as coding, off-the-shelf purchases, outsourcing, testing, and user training. Within managerial ISPs, this phase primarily refers to applying the policy within the organization by guiding and training the employees. A large portion of the ISP literature considers this phase of the policy lifecycle, especially from the viewpoint of compliance, awareness, and security incidence mitigation (Balozian & Leidner, 2017). Reviewing these articles is outside the scope of this paper. However, some of this work does have implications to the ISP development.

A study that explicitly examined implementation, found that there was no statistically significant relationship between the adoption of IS security policies and the incidence of security breaches (Doherty, Neil & Fulford, 2005). Though this may seem to be detrimental to the core assumption of the effectiveness of security policies (i.e., that the policy is the bedrock of effective security within an organization), in reality it bolsters the case for sound security policies. The authors suggested that difficulties in raising awareness, difficulties in enforcement, overly complex policy standards, inadequate resourcing, or the failure to tailor policies might be to blame (Doherty, Neil & Fulford, 2005). There may also be problems in linking the high-level policy statements into actionable guidelines (Pathari & Sonar, 2012). This would suggest a disconnection in the middle layer of the policy architecture (Pathari & Sonar, 2012; Von Solms et al., 2011).

Empirical ISP research usually considers only one phase in the ISP lifecycle. A very popular research topic is the link between a general ISP statement and the intention to comply (Herath & Rao, 2009). However, there are very few works that would examine a longer sequence of actions in information security management. For example, the link between how the policy statements are created and how

that affects the subjects' security behavior or the severity of security incidents, is rarely examined. It has been found that the normative believes of the expectations of other organization members does influence the intention to comply with an ISP (Herath & Rao, 2009). The ISP development process can be a part of creating and communicating these expectations among the ISP subjects.

To ensure subjects' awareness of the ISP there is a need for user training (Heikka, 2008) and testing (Baskerville & Siponen, 2002). Especially activities involving user participation are important when trying to change security behavior (Albrechtsen, 2007). Furthermore, the efforts to translate formal change of the new policy into the informal change in security behavior requires continuous long-term efforts in order to institutionalize the changes (Dhillon, G., Syed, & Pedron, 2016). This may require a tremendous amount of work since the organization subjects may have adopted values and behaviors from other users, or policies at home, or other organizations that affect their adoption of the new ISP (Asai & Hakizabera, 2010; Horacio et al., 2010; Spinellis, Kokolakis, & Gritzalis, 1999).

Considering compliance from the ISP development viewpoint, it may be prudent to consider resistance before full-scale implementation. Lapke and Dhillon (2008) analyzed resistance to security policies through the lens of power relationships. The study found that although the establishment had a well-documented and planned set of processes in place for the formulation and implementation of security policies, it failed to explicitly acknowledge the effect of resistance and implicit power brokers. They found that the entities responsible for policy formulation would be best suited to performing an extensive analysis on the impact a security policy might have on productivity prior to implementation. Siponen (2000) argues that resistance to security measures may also arise from a person seeing certain actions as totally wrong or deficient and that policy makers should be ready to justify their choices for the guidelines if challenged. These studies imply that measures undertaken during ISP development as well as during user training and testing could suppress some of the resistance during implementation. If the nature and importance of an ISP is not clear in the organization, it may hinder its adoption altogether (Lopes & Sá-Soares, 2010).

In the cyclical ISP development models, the output of the development phase returns later as an input to a new ISP development or revision process. The reasons for a new iteration in the development cycle may be changes in the business environment (e.g. a merger), new systems or technology (e.g. moving to cloud), or a failure to reach the security goals assigned to the current policy (Baskerville & Siponen, 2002; Dhillon, G. et al., 2016; Doherty, N. F. & Fulford, 2006; Rees et al., 2003). Detecting changes and reaching goals can be done by monitoring predetermined metrics, which can be developed for every level of ISPs and connect to the next level (Von Solms et al., 2011). Detecting high-level trends in ISP effectiveness requires a strategic view of ISP development.

4.2 Content of the ISP

The ISP development methods are designed to produce content for the ISP's documentation. We must acknowledge that organizations and ISP development method designers have different notions of the areas and details of what the content is supposed to cover. An organization might have one huge document covering everything, separate hierarchically connected policies each containing hundreds of directives (David, 2002), or a high-level policy, supplemented by guidelines (Klaic, 2010; Pathari & Sonar, 2012). An example of a hierarchical policy structure is provided in the ISPA, which has strategic-, tactical-, and operational-level policies (Von Solms et al., 2011). Policies may also only cover some aspects of information use such as approved system use, or they may be targeted at different groups (Doherty, Neil et al., 2009). Sterne (1991) has proposed that we should distinguish between automated security policies and policies governing human behavior and determine the links between the two. Balozian and Leidner (2017) further distinguished the ISP as a procedural countermeasure and security culture as an environmental countermeasure.

A classic definition of ISP goals might be to protect the confidentiality, integrity, and availability (assurance for the service) of information but this view has been criticized for its strong focus on technical security (Sterne, 1991). Focusing on the controls instead of the security of the actual information assets may leave gaps in coverage of the ISP. For example, concentrating only on IT controls may leave gaps in security. One case study found that healthcare professionals considered the

privacy regulations as only covering digital patient records, but not the paper records that were also in use (Hedström, Karin et al., 2011).

As we learned from examining the ISP definitions, people have different views on the nature of the ISP content. Some see it as a collection of rules (rather like a law book) and others see it more as a guiding document helping users of information make better decisions about its protection (Ruighaver et al., 2010). Some authors promote the rule-oriented view, which incorporates sanctions within the ISP based on deterrence theory (Straub, 1990). The content and form of the ISP depends on the organization, its operational environment, and values (Ruighaver et al., 2010). Siponen and Iivari (2006) investigated normative theories from philosophy as tools for designing and implementing ISPs. They recommend that all-inclusive and strict policies only suit organizations in which exceptional situations occur rarely and the subjects are not expected to make security decisions. If, however, the organization faces new opportunities from its environment and trusts its employees to make decisions, a more loosely defined policy may be appropriate (Ruighaver et al., 2010). In addition, the enforcement tactics stated in the policy may vary from punishing incorrect behavior to rewarding good deeds, and these should be connected to the culture and values of the organization (Balozian & Leidner, 2017; Chen et al., 2012).

Probably the best-known guides for ISP content are security standards such as ISO27002. Another source of content is regulations such as EU directives for processing personal information. Haworth and Pietron compared the ISO standard and the Sarbanes-Oxley act of 2002 (SOX, in USA) and found that complying with the standards helps in complying with the regulations as well. However, Höne and Eloff (2002) compared several international standards and noticed that they tend to focus more on the processes of implementing the policy rather than on providing guidance for the development of its content. It has also been noted that general guidelines for policy content seem to be providing more support to preventive actions rather than responsive ones (e.g. Spinellis et al., 1999). Preventive actions are suitable for environments where risks and suitable countermeasures are known, but for ever-changing dynamic markets, this approach may be impossible, and policies for responsive actions are needed (Baskerville et al., 2014).

Some authors suggest industry-specific content and development methods for ISPs. Especially the medical field is well represented in this regard since it offers interesting dilemmas between the security of private patient information, strong regulations, and patient wellbeing (Hedström, K. et al., 2013; Karlsson et al., 2017). Anderson (1996) and Gritzalis (1997) present principles to guide the formulation of ISPs in medical facilities, with a special focus on the ethical issues relating to patient information. However, providing general principles for policies becomes challenging when organizations move to more complex and decentralized IS. Ward and Smith (2002) proposed a set of eight indicative policies for organizations with distributed systems. Lindup (1995), on the other hand, recommended a security treaty for organizations, which comprises of independent units to highlight the individual needs as well as common goals of the units.

As we have established, ISPs can take many forms, but which is the best? Karlsson et al. (2017) found that employees had trouble following policies due to inadequate explanation and use of terms, inconsistent explanations of the controls, and unexplained policy architecture. Goel and Chengalur-Smith (2010) created metrics for policy document breadth, clarity, and brevity. suggest that these attributes may influence the policy subjects' ability to comprehend the document, which would lead to better compliance and information security.

When we look at the publication years of these articles, we notice a move from specific principles to more organization-dependent points of view in terms of the content. Traditional approaches focused on simpler views of information and IS. The contemporary views, however, have incorporated new contextual areas of interest into ISPs such as organizational structure and culture (Klaic, 2010).

4.3 Context in ISP development

The section on content highlighted how creating recommended content that would suit all companies is hard or even impossible, since the context of the policy affects its content in different organizations. Karyda et al. (2005) identified seven contextual factors that influence the formulation and

implementation of ISPs: organizational structure; organizational culture; management support; contribution to users' goals; security officers; users' participation in the formulation process; and training and education. Shortcomings in these factors such as a security-ignorant organizational culture should be seen as reasons to start developing or revising the ISP (Talbot & Woodward, 2009).

Galletta and Hufnagel (1992) created a model where the context affects both the content and the policy development process, and eventually, compliance. The research to validate their model was unable to prove that compliance resulted from the context-specific design of the policy or the users' personal inclination to follow rules. Later, it was shown that a person's attitude, the perception of control, and subjective norms do affect the intention to share knowledge about information security, (Safa & Von Solms, 2016) and thus contribute to the security culture of the organization.

Da Veiga and Eloff (2010) created a framework and assessment instrument for an information security culture to evaluate the cultural changes related to security measures. They noted that the security culture can also affect the security measures, such as ISPs, and suggested user participation in the development process, especially in individualistic organizations. Insiders have been deemed one of the largest risks for information security, since they have access to the information assets, and can unintentionally or maliciously use them in an undesirable way (Colwill, 2009), which is why many authors emphasize their role. Multinational organizations may have to adopt multiple different approaches to counter the insider threat, since the security culture is also influenced by the local culture that varies across countries (Asai & Hakizabera, 2010).

Managers have a significant role in the development and implementation of the ISP since they are responsible for many key tasks that contribute to the success of the ISP such as the alignment of information security and business processes (Soomro et al., 2016). However, Coles-Kemp (2009) finds that many approaches to information security have simplified views of the organization; namely, that the company structure reflects the distribution of power and authority, and that decisions can always be made through a formal process. This is why contextual knowledge can also be sought from other stakeholders.

The ISP development process may include several internal and external stakeholder groups such as business unit representatives, executive management, human resources, ICT specialists, security specialists, legal and regulatory bodies, public relations, the user community, and representatives of supply chain (Maynard et al., 2011; Sindhuja, 2014). Different stakeholders view information security differently, and they will have different metaphors and terminology to describe the same information-processing tasks (Abrams & Bailey, 1995). By including stakeholders in the development process, they may be committed to it, and act as advocates post-implementation (Maynard et al., 2011; Rees et al., 2003). It must also be noted that the person's role in the organization is not the only thing that affects their security behavior; it is also affected by their individual personality and aspirations (Ashenden, 2008).

Since ISPs are descriptions about desired and undesired actions, some authors see them as reflections of values. Different stakeholders can have different values, which raises the question regarding whose values the ISP serves (Siponen, 2000). To make design decisions about ISPs, a value-based argumentation method has been proposed to solve conflicts between, for example, business interests and regulations (Burgemeestre et al., 2013). The value-based compliance model tackles the same problem by seeing users' non-compliance as a rational action due to their different values that are in conflict with the ISP (Hedström, Karin et al., 2011). For example, healthcare staff tend to put patient safety and keeping appointment schedules before correct information security actions. This is in line with the finding that people who are open to changing their values may act against policies, whereas those who do not make higher-level decisions about their values and only try not to get punished will follow the policy (Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009).

We find that the context of the ISP can affect both the content and the development method of the policy. Context not only refers to the externally identifiable characteristics of the organization such as process charts and competitors but also to the inner characteristics of the individual subjects of the policy. On a higher level, the policy should meet the security requirements and support the business

objectives of the specific business (Karyda et al., 2005). Disregard for the context while developing the policy may lead to resistance or failure during implementation and compliance (Chen et al., 2012).

4.3.1 Integration of the information security policy with the business strategy

One contextual factor that deserves special attention is the company's business strategy. A strategy is a plan to achieve the overall goal toward which the business is directed. The business policies, including ISPs, support the effort to reach these goals by directing the actions in the company. One widely used approach to business strategy is Porter's (1979) Five Forces Framework that consists of four forces (the bargaining power of customers, the bargaining power of suppliers, the threat of new entrants, and the threat of substitute products) influencing a fifth force: the level of competition in an industry.

Strategic IS planning identifies system and technology related projects that could create competitive advantage and support reaching business goals (Doherty, N. F. & Fulford, 2006) IS alignment with the business strategy indicates how much the IS plan reflects the business plan (King, 1978). This alignment could be approached from a socio-organizational perspective where the alignment refers to more of a balancing of the social–organizational changes as a result of the IT/system insertion (Barley, 1990). It could also be examined through a managerial lens such as strategic information systems planning (SISP) (Earl, 1993). Four areas of focus in SISP are noted for their presence in the literature: aligning IS investment with business goals, exploiting IT for competitive advantage, directing the efficient and effective management of IS resources, and developing technology policies and architectures.

Information security brings in a third level of strategic alignment alongside business strategy and IS planning processes. In some cases, secure systems development and IS development are separate processes and activities (Siponen, 2005). This developmental duality is a source of conflicting requirements between a system's normal functionality and information security requirements. The similar duality may occur with high-level ISP documents if business goals and information security goals give different priorities for information use (Karlsson et al., 2017). Duality can also explain users' resistance when the security is added afterwards (Siponen, 2005). If it blocks the purposed functionality of the system, users may be resistant to the security implementation (Albrechtsen, 2007).

In order to avoid developmental duality and the problems that it brings, the ISP should be aligned with the organization's business goals (Anton & Earp, 2000; Höne & Eloff, 2002). Including ISP development in the strategic management cycle could ensure that the alignment is constant even when the organization's goals change (Baskerville & Siponen, 2002; Soto Corpuz, 2011). However, while the reasoning for ISP – strategy alignment is obvious on paper, it may not be the reality in many organizations (Abu-Musa, 2010). If the business strategy is not considered in the ISP analysis and planning stages, it may lead to high-risk assets being protected even though they are not strategically relevant (Burgemeestre et al., 2013). When the ISP is planned to contribute toward the strategic goals of the organization, it can also be easier to justify the investments made in security (Klaic, 2010).

Many ISP development methods suggest ways to include the business strategy in the policy such as including the senior management (Doherty, N. F. & Fulford, 2006; Flowerday & Tuyikeze, 2016; Knapp et al., 2009). However, there are few clear instructions on how this management involvement might be executed. Von Solms et al. (2011) presented an "ideal" information security governance environment where the management direction starts from the strategic management level and the tactical- and operational-level policies are directly derived from the high-level policies. This approach gives clear tasks to the different management levels but little advice on how to best execute them.

McFadzean et al. (2007) researched things that influence the information security strategy at board level. The directors' perception of risk and the role of IT influence how they direct planning, adoption, and use of information security measures in the organization. The perceptions are presented in a grid with two axes: low/high perception of risk and IT as an operational/strategic tool. The perception grid is intended to be used in creating an information security strategy by mapping the current situation, identifying contextual factors that influence the strategy, and setting future goals. The grid helps in understanding how the company is situated compared to its competition and how the

applications' portfolio is supporting the goals. Most importantly, the grid helps in aligning the information security strategy with the business strategy (Mcfadzean et al., 2007). By understanding the types of risks and the strategic need for IS, it is possible to move on to making decisions about choosing the right mix of prevention and response strategies (Baskerville et al., 2014; Doherty, N. F. & Fulford, 2006).

ISPs can be aligned with business strategies at the highest level of the policy architecture. The information security strategy should complement the business strategy, and the lower-level policies should prescribe actions that lead to the realization of these goals. However, without proper planning and a methodological approach, the alignment may easily fail and lead to the dual development of business and information security goals.

5 Discussion

The goal of this paper was to understand the definitions and functions given to ISPs in the literature and the ISP development process including its many dimensions. Our analysis of the literature yielded several interesting observations about the state of the current research and research gaps that should be addressed by future research.

Our review of the research found a wide array of interpretations of the concept under study: ISPs. It is critical to have an understanding of what an ISP is so that both practitioners and researchers can be clear about what they are discussing. Although different interpretations can add richness to understanding a concept, it can also lead to confusion and ambiguity. There are distinctions between technical and managerial policies, policy architecture, and the documents included under the term. Describing the exact meaning of the concept would help in comparing and further developing research contributions. We detected the following notions with differentiated meanings in the literature and advice that they should be clarified when discussing or researching ISPs.

- Level of abstraction/detail/architecture: not only the process level abstraction, but also the strategic and operational levels
- Focus area (technical/managerial): discussing differences and relationships need to be determined before giving recommendations for development
- ISP subjects & objects: not defining the subjects and objects may lead to misunderstandings of the applicability of research results.
- Peremptory nature of the statements: authors have different assumptions about the management styles in organizations and how directives are stated and followed

A surprising observation can be made from the ways in which an ISP is defined and its functions are described. Many articles explain that the purpose of an ISP is to "facilitate the prevention, detection, and response to security incidents" (Cram et al., 2017, pg. 605). While there is no reason to dispute this definition, it does overlook the obvious reason for information security. Apart from businesses that have information security as an integral part of their value proposition (e.g. banks, services for armed forces, data centers), most organizations actually exist for a completely different reason than security. Information security issues are something that come with the operating environment and the organization merely tries to cope with them using ISPs. There seems to be a need for definitions and research approaches that step out of the information security-centered worldview and try to see information security as an enabler for reaching organizational goals. If security measures are at any point developed for the sake of security and not for the business, there is the danger of doing unnecessary, and in many cases, unwanted work.

Since ISPs may mean many different kinds of documents to different organizations, there is thus no single description of what it comprises. Our analysis revealed many characterizations and functions given to ISPs. However, many articles did not elaborate on these background assumptions of the term. We can distinguish between the description and function of a policy even though many authors mix the notions. What the ISP *is* must adequately support what the ISP *does*. For example, insufficient instructions cannot lead to comprehensive control over people's actions. We must also refrain from making the presumption that the existence of any characteristic of a policy would automatically lead

to any of its functions. For example, the mere existence of predefined sanctions may not lead to perfect compliance. A wider understanding of the different definitions and functions an ISP, may help practitioners widen their view of the nature of the policy in development. This is also an area where empirical research contributions were surprisingly scarce rising the question, why are there so many recommendations for the content of the ISP but so few pieces of evidence that these content recommendations lead to better information security? Interviews with experts and longitudinal studies could help in answering this call.

The flow of information described in the definition of the concept is also a critical aspect in terms of understanding security policy development. From the analysis of different lifecycle models, four phases could be identified: an analysis phase, a policy formulation phase, a policy implementation phase, and a policy maintenance phase. While these lifecycle models are often called ISP development methods, in actuality, only one phase of the model is responsible for creating new content for an ISP. In our analysis, we chose to focus on this phase and call the previous and consecutive phases the inputs and outputs.

The inputs for ISP development can be standards, regulations, a desired format, risk analysis, contractual obligations, user-related requirements, previous policies, logs of security incidents, and business requirements. What data the developers should gather to inform the formulation of a security policy is well represented in the standards and other literature. However, using predefined lists of focus areas for information-gathering may be problematic four reasons. (1) The list may not be comprehensive enough, leaving blind spots that can be exploited. (2) Secondly, a list may cause a false sense of security if the requirements of the developers only aim to satisfy the requirements of the list instead of finding the actual organization-specific requirements. (3) Third, the human aspects of the security requirements such as the culture, emotions, personality traits, and policy fairness (Cram et al., 2017) are still underrepresented in these lists and their dismissal may perhaps lead to problems in implementation. (4) Lastly, the externally defined top-down approaches may be designed for large knowledge-intensive organizations and not be usable for making ISPs for smaller companies.

The inputs for the ISP development process need to be sufficient in order for the process to be completed successfully. Many of the lifecycle models for ISP development give very general instructions for the actual formulation of the policy based on the inputs. However, there are some special techniques for making choices in the development phase such as the methods for solving value conflicts. While there are many calls for, for example, user and management participation, meeting organizational requirements, and assuring quality documentation, there are very few research-based recommendations on how to do these things well.

The recommendations for including the involvement of different organization members in the development phase stem from the research on ISP implementation and compliance. These are research topics for the outputs of the ISP development process. One popular topic is determining the causative effects on an organization's user acceptance of a policy. A newer approach to this question lies in the inevitable change in power relationships that occurs during policy implementations. An interesting question is how these research topics have affected the view on ISP development. For example, the research on power relationships (Lapke & Dhillon, 2008) leads to the conclusion that the possible conflicts that arise from the change in power relationships can be reduced by better design of the ISP in the first place. Very few authors discuss this link between problems in implementation and maintenance and poor ISP development. It would seem that this is an area where research could contribute greatly to practice if proper means to use research findings would be provided to the practitioners.

Monitoring information security during ISP maintenance should be able to indicate the quality of the ISP design. In cyclical models, the detected issues are one of the reasons why the cycle should start again from the beginning. Other reasons to start a new cycle can be linked to a predetermined lifespan for the ISP or to changes in the organization such as a new strategy if the ISP process is tied to the strategical planning process. Many of the lifecycle models give very little advice on the proper ways to detect a suitable time for ISP revision. Without a proper plan for ISP revisions, it may be that changes are made only when security incidents are detected and have already caused harm to the

information the ISP was supposed to protect. This is why it would be advisable to include the creation of performance metrics during ISP development to avoid ad hoc changes made in a state of panic.

How information flows and changes from inputs to the output is critical in understanding the links between different issues during the policy lifespan. Insufficient knowledge-gathering on the organization-specific issues before ISP development may lead to issues in implementation and maintenance. Many methods for ISP development mention influencing factors such as management support and customer requirements. Addressing these various issues requires techniques and methods that allow for meeting the organization-specific requirements and producing a quality ISP that continuously fits its purpose. This could be researched by comparing the development methods and the resulting policies of different organizations.

In relation to the context of the ISP, our review also assessed the alignment of the ISP and the business strategy. A major issue can be developmental duality if these strategies are developed on their own tracks and independent from each other. This is one of the major reasons as to why ISP development requires managerial support and direction. The goals of the ISP and the business should be the same and not conflicting. This may help in justifying information security investments and add credibility to the implementation efforts. One way of ensuring the joint goals of business and information security is to add policy development as part of the strategy process.

The most striking finding of this literature survey was that there was not much to be found. While ISPs are generally thought to form the basis of the information security actions in an organization, it is a surprisingly little researched area. There are so many conceptual models, best practices and standards for ISPs that many conventions are taken for granted. However, there seems to be a need to challenge these assumptions to gain understanding of the real-life issues of making ISPs. While many process models for ISP development seem logically sound, when taken to a high enough abstraction level, there should always be room for rival solutions if only to strengthen the consensus. Furthermore, there is still much to be learned about the lower level phenomena that relate to, for example, aligning information security and business goals, policy decision-making, recognizing information security needs, behavior of ISP developers, and the policy – organizational culture fit.

The state of the art in ISP development seems to be acknowledging organization-specific requirements and the need to manage the human factors as well as the technical side. The research on these issues is mainly conceptual, but over the last few years, some techniques and methods have already been developed through empirical research. The need now is to find ways to combine the research on different factors into a methods that are proven to help organizations in making better ISPs. Explanatory, predictive, and design theories in this field could move ISP development into a new era, providing useful tools to organizations operating in this information-driven society.

6 Conclusion

This literature review revealed a rich tapestry of topics on ISP development. Several themes emerged that may point the way toward expanding this domain. The analysis of the research methodologies used in previous research showed a preponderance of conceptual research. ISP research could use more studies on empirical theory building or testing as well as artifact building.

Our analysis yielded knowledge about the most commonly used definitions and descriptions of ISP functions. Having common ground in terms of conceptual clarity can provide for a better understanding as well as the improved effectiveness of ISPs within organizations. This is particularly true given the vague and sometimes conflicting perspectives of the ISP itself. Definitional confusion and contradiction can lead to miscommunication and ineffective policies. Failure to specify the underlying assumptions of the meaning of the term can also lead to fragmentation in the field of research and result in ambiguity.

An analysis of the ISP development phases showed that gaps exist within the process in both theory and praxis. The literature mentioned many examples of different sources for requirements that function as inputs for ISP development. However, there is little support available for the gathering of organization-specific requirements and for ensuring that all requirements are identified. While the

current ISP development methods highlight the contextual factors, they fall short in providing methods that would ensure information security that counters organization-specific threats. The output of the development process, the ISP, is widely studied from the awareness and compliance point of view, but not many connections have been made between these research contributions and the development phase.

This review concludes that the state of the art in ISP development is the increasing focus on organization-specific information security needs. The research in this area is still lacking contributions that would show how contextual factors could be successfully integrated into ISP development. This paper helps in understanding the multiple dimensions of ISP development, where these contextual issues can be addressed.

Funding

This research was partly funded by project grant from European regional development fund and Business Finland.

Declaration-of-competing-interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Abrams, M., & Bailey, D. (1995). Abstraction and refinement of layered security policy. In M. D. Abrams, S. G. Jajodia & H. J. Podell (Eds.), *Information security: An integrated collection of essays* (pp. 126). Los Alamitos, CA, USA: IEEE Computer Society Press.

Abu-Musa, A. (2010). Information security governance in saudi organizations: An empirical study. *Information Management and Computer Security, 18*(4), 226-276.

Albrechtsen, E. (2007). A qualitative study on users' view on information security. *Computers & Security, 26*(2007), 276-289.

Anderson, R.A security policy model for clinical information systems. Paper presented at the *IEEE Symposium on Security and Privacy,* 30-43.

Anton, A., & Earp, J.Strategies for developing policies and requirements for secure electronic commerce systems. Paper presented at the *1st Workshop on Security and Privacy in E-Commerce at CCS2000,*

Asai, T., & Hakizabera, A. U. (2010). Human-related problems of information security in east african cross-cultural environments. *Information Management and Computer Security, 18*(5), 328-338.

Ashenden, D. (2008). Information security management: A human challenge? *Information Security Technical Report, 13*(4), 195-201.

Balozian, P., & Leidner, D. (2017). Review of IS security policy compliance: Toward the building blocks of an IS asecurity theory. *Data Base for Advances in Information Systems, 48*(3), 11-43.

Barley, S. (1990). The alignment of technology and structure through roles and networks. *Administrative Science Quarterly, 35*(1), 61-104.

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.

David, J. (2002). Policy enforcement in the workplace. *Computers and Security, 21*(6), 506-513.

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers and Security, 56*, 63-69.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal, 2001*(11), 127-153.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16*, 293-314.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal, 19*(4), 391-412.

Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers and Security, 25*(1), 55-63.

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.

Doherty, N., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: An exploratory analysis. *Information Resources Management Journal, 18*(4), 21-39.

Earl, M. (1993). Experiences in strategic information systems planning. *MIS Quarterly, 17*(1), 1-24.

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

Galletta, D. F., & Hufnagel, E. (1992). A model of end-user computing policy: Context, process, content and compliance. *Information & Management, 22*(1), 1-18.

Glasgow, J., Macewen, G., & Panangaden, P. (1992). A logic for reasoning about security. *ACM Transactions on Computer System, 10*(3), 226-264.

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

Gritzalis, D. (1997). A baseline security policy for distributed healthcare information systems . *Computers & Security, 16*(8), 709-719.

Haworth, D., & Pietron, L. (2006). Sarbanes–Oxley: Achieving compliance by starting with iso 17799. *Information Systems Management, 23*(1), 73-87.

Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals the importance of user rationale. *Information Management and Computer Security, 21*(4), 266-287.

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. doi://dx.doi.org/10.1016/j.jsis.2011.06.001

Heikka, J.A constructive approach to information systems security training: An action research experience. Paper presented at the , *1*(1) 1-8.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

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

Horacio, G., Caceres, R., & Teshigawara, Y. (2010). Security guideline tool for home users based on international standards. *Information Management and Computer Security, 18*(2), 101-123.

Howard, P. (2003). The security policy life cycle: Functions and responsibilities. In H. Tipton, & M. Krause (Eds.), *Information security management handbook* (4th ed., pp. 999). Boca Raton: CRC Press, LLC.

ISACA. (2019). About COBIT 5. Retrieved from https://cobitonline.isaca.org/about

ISO/IEC 27001. (2013). In Finnish Standards Association S. (Ed.), *Lnformotion technology. security techniques. lnformotion security monogement systems. requirements* International organization for standardization.

ISO/IEC 27002. (2013). In Finnish Standards Association S. (Ed.), *Information technology - security techniques - code of practice for information security controls* International organization for standardization.

Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. *Computers and Security, 67*, 267-279.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: A contextual perspective. *Computers & Security*, *24*(3), 246-260. doi://dx.doi.org/10.1016/j.cose.2004.08.011

King, W. (1978). Strategic planning for information systems. *MIS Quarterly, 2*(1), 27-37.

Klaic, A.Overview of the state and trends in the contemporary information security policy and information security management methodologies. Paper presented at the *Mipro*, Croatia. 1203-1208. Retrieved from https://jyu.finna.fi/PrimoRecord/pci.ieee12031208.pdf

Klaic, A., & Hadjina, N.Methods and tools for the development of information security policy — A comparative literature review. Paper presented at the 1532-1537. Retrieved from https://jyu.finna.fi/PrimoRecord/pci.ieee15321537.pdf

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.Power relationships in information systems security policy formulation and implementation. Paper presented at the *16th European Conference on Information Systems (ECIS)*, Galway, Ireland.

Levy, Y., & Ellis, T. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science: International Journal of an Emerging Transdiscipline, 9*, 18-212.

Lindup, K. (1995). A new model for information security policies. *Computers & Security*, *14*(8), 691-695.

Lopes, I., & Sá-Soares, F.Information systems security policies: A survey in portugese public administration. Paper presented at the *IADIS International Conference Information Systems*, 61-69.

Maynard, S. B., Ruighaver, A. B., & Ahmad, A.Stakeholders in security policy development. Paper presented at the *9th Australian Information Security Management Conference*, Edith Cowan University, Perth Western, Australia. 182-188.

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.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? an empirical study. *European Journal of Information Systems, 18*(2), 126-139.

Niemimaa, M., & Niemimaa, E. (2019). Abductive innovations in information security policy development: An ethnographic study. *European Journal of Information Systems,*

Olnes, J. (1994). Development of security policies. *Computers & Security, 13*(8), 628-636.

Pathari, V., & Sonar, R. (2012). Identifying linkages between statements in information security policy, procedures and controls. *Information Management and Computer Security, 20*(4), 264-280.

Porter, M. (1979). How competitive forces shape strategy. *Harvard Business Review, 57*(3), 87-94.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security, 23*(8), 638-646.

Rees, J., Bandyopadhyay, S., & Spafford, E. (2003). PFIRES: A policy framework for information security. *Communications of the ACM, 46*(7), 101-106.

Ruighaver, A. B., Maynard, S. B., & Warren, M. (2010). Ethical decision making: Improving the quality of acceptable use policies. *Computers and Security, 29*(7), 731-736.

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442-451.

Saleh, M. (2011). Information security maturity model. *International Journal of Computer Science and Security, 5*(3), 316-337.

Sandhu, R. S., & Samarati, P. (1994). Access control: Principle and practice. *IEEE Communications Magazine, 32*(9), 4-48.

Shirtz, D., & Elovici, Y. (2011). Optimizing investment decisions in selecting information security remedies. *Information Management and Computer Security, 19*(2), 95-112.

Silic, M., & Back, A. (2014). Information security: Critical review and future directions for research. *Information Management & Computer Security, 22*(3), 279-308.

Sindhuja, P. N. (2014). Impact of information security initiatives on supply chain performance an empirical investigation. *Information Management and Computer Security, 22*(5), 450-473.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Siponen, M. (2005). An analysis of the traditional IS security approaches: Implications for research and practice. *European Journal of Information Systems, 14*(3), 303-315.

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., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *The Data Base for Advances in Information Systems, 38*(1)

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267-270.

Solic, K., Ocevcic, H., & Golub, M. (2015). The information systems' security level assessment model based on an ontology and evidential reasoning approach. *Computers and Security, 55*, 100-112.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security, 22*(1)

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.The enterprise information security policy as a strategic business policy within the corporate strategic plan. Paper presented at the *The 8th International Symposium on Risk Management and Cyber-Informatics: RMCI 2011,* Orlando, Florida, USA. 275-279.

Spinellis, D., Kokolakis, S., & Gritzalis, S. (1999). Security requirements, risks and recommendations for small enterprise and home-office environments. *Information Management and Computer Security, 7*(3-4), 121-128.

Sterne, D.On the buzzword security policy. Paper presented at the *IEEE Computer Society Symposium on Research in Security and Privacy,* Oakland, CA. 219-230.

Straub, D. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Talbot, S., & Woodward, A.Improving an organisations existing information technology policy to increase security. Paper presented at the *7th Australian Information Security Management Conference,* Perth, Western Australia,. 120-128.

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

Trompeter, C., & Eloff, J. (2001). A framework for the implementation of socio-ethical controls in information security. *Computers & Security, 20*(5), 384-391.

Tuyikeze, T., & Pottas, D.An information security policy development life cycle. Paper presented at the *Proceedings of the South African Information Security Multi-Conference (SAISMC 2010),* 165.

Von Solms, R., Thomson, K., & Maninjwa, P. M.Information security governance control through comprehensive policy architectures. Paper presented at the *Information Security South Africa (ISSA), 2011*,

Ward, P., & Smith, C. (2002). The development of access control policies for information technology systems. *Computers & Security, 21*(4), 356-371.

Whitman, M., E. (2008). Security policy: From design to maintenance. In R. Baskerville, D. W. Straub & S. E. Goodman (Eds.), *Information security: Policy, processes, and practices* (pp. 123-151). Armonk, NY: Routledge.

Willison, R., & 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, 14*, 667-674.

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.

Appendix One

Scopus Search term:

EXACTSRCTITLE ("European Journal of Information Systems")
OR EXACTSRCTITLE ("Information Systems Journal")
OR EXACTSRCTITLE ("Information Systems Research")
OR EXACTSRCTITLE ("association of IS")
OR EXACTSRCTITLE ("Journal of MIS")
OR EXACTSRCTITLE ("Journal of Strategic Information Systems")
OR EXACTSRCTITLE ("MIS Quarterly")
OR EXACTSRCTITLE ("Communications of the association for information systems")
OR EXACTSRCTITLE ("Information and management")
OR EXACTSRCTITLE (“Data Base for Advances in Information Systems")
OR EXACTSRCTITLE ("Information management and computer security")
OR EXACTSRCTITLE ("Computers and security")
AND TITLE-ABS-KEY (“security policy”)
AND TITLE-ABS-KEY (develop*)
OR TITLE-ABS-KEY (creat*)
OR TITLE-ABS-KEY (formula*)
OR TITLE-ABS-KEY (method*)

Appendix Two

Number of articles per publication outlet:

- *ACM Computing Surveys* 1
- *ACM Transactions on Computer Systems* 1
- Book/Publication 4
- *Communications of the ACM* 1
- *Computers & Security* 22
- *Computers in Human Behavior* 1
- Conference 12
- *Ethics and Information Technology* 1
- *European Journal of Information Systems* 6
- *Information & Management* 3
- Information Management & Computer Security 11
- *Information Resources Management Journal* 1
- Information security technical report 3
- *Information Systems Journal* 3
- *Information Systems Management* 1
- *Information Systems Research* 1
- *International Journal of Computer Science and Security* 1
- *International Journal of Information Management* 3
- *Journal of Management Information Systems* 1
- *Journal of Strategic Information Systems* 2
- *Journal of the Association for Information Systems* 1
- *Logistics Information Management* 1
- *MIS Quarterly* 2
- *Online Information Review* 1
- *The Data Base for Advances in Information Systems* 2

Appendix Three

Number of articles per research approach:

- Action research 2
- Case study 10
- Conceptual 29
- Design science 4
- Experiment 1
- Grounded theory 2
- Literature review 11
- Other approach 11
- Survey 17

Biographies for the article "State of the Art in Information Security Policy Development"

6.1 Hanna Paananen, University of Jyvaskyla, Finland

Hanna Paananen is a doctoral researcher of Information Systems in University of Jyvaskyla. She has a M. Sc. (econ.) in Information systems and BBA in Business management. Her main research interests are in organizational information security management and development methods.

6.2 Michael Lapke, University of Mary Washington, United States

Michael Lapke is an Associate Professor of Information Systems at the University of Mary Washington in Fredericksburg, VA. He joined UMW in 2012 and previously held positions at East Carolina University and Rhode Island College. He also joined the faculty of the University of Jyvaskyla in 2016 for a research project in Information Systems Security Policy development under the supervision of Mikko Siponen. Dr. Lapke earned his doctorate at Virginia Commonwealth University in Richmond, Virginia under the guidance of Gurpreet Dhillon. His primary research area is Information Systems Security, IS Security Policy, Privacy in Healthcare, and Accounting Information Systems.

6.3 Mikko Siponen, University of Jyvaskyla, Finland

Mikko Siponen is full professor of Information Systems. He has served ten years as a Vice dean for research, head of department, vice head or director of a research center. His degrees include Doctor of Social Sciences, majoring in Philosophy; M.Sc. in Software Engineering; Lic.Phil. in information systems; and Ph.D. in Information Systems. He has received over 10 million EUR of research funding from corporations and numerous other funding bodies. Besides leading industry-funded projects, Siponen has been a PI on projects for the Academy of Finland, the EU, and the Finnish Funding Agency for Innovation. His current H index is 43, and he has more than 8200 citations (Google Scholar). He has published more than 55 articles in journals such as MIS Quarterly and Information Systems Research.