The hunt for computerized support in information security policy management

A literature review

Elham Rostami
Department of Informatics, Orebro Universitet Handelshogskolan, Orebro, Sweden, and

Fredrik Karlsson and Ella Kolkowska
School of Business, Örebro University, Örebro, Sweden

Received 1 August 2019
Revised 9 October 2019
Accepted 9 October 2019

Abstract

Purpose – The purpose of this paper is to survey existing information security policy (ISP) management research to scrutinise the extent to which manual and computerised support has been suggested, and the way in which the suggested support has been brought about.

Design/methodology/approach – The results are based on a literature review of ISP management research published between 1990 and 2017.

Findings – Existing research has focused mostly on manual support for managing ISPs. Very few papers have considered computerised support. The entire complexity of the ISP management process has received little attention. Existing research has not focused much on the interaction between the different ISP management phases. Few research methods have been used extensively and intervention-oriented research is rare.

Research limitations/implications – Future research should to a larger extent address the interaction between the ISP management phases, apply more intervention research to develop computerised support for ISP management, investigate to what extent computerised support can enhance integration of ISP management phases and reduce the complexity of such a management process.

Practical implications – The limited focus on computerised support for ISP management affects the kind of advice and artefacts the research community can offer to practitioners.

Originality/value – Today, there are no literature reviews on to what extent computerised support the ISP management process. Findings on how the complexity of ISP management has been addressed and the research methods used extend beyond the existing knowledge base, allowing for a critical discussion of existing research and future research needs.

Keywords Literature review, Information security policy, Computerized support

Paper type Literature review

1. Introduction

Today, the not-so-big news is that governments, organised criminals and hacktivists are attacking organisations' information and information systems. As information has become

Information & Computer Security
Vol. 28 No. 2, 2020
pp. 215-259
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-07-2019-0079

the lifeblood of modern society it has also become a valuable asset. Therefore, it is not surprising that information security management, where the purpose is to safeguard an organisation's information assets, has become an important strategic issue (Van Niekerk and Von Solms, 2010). Organisations are in a situation where knowledgeable employees need to be the first line of defence. Unfortunately, breaching organisations still does not typically require advanced technical skills; many victims are tricked into opening attachments and clicking on links (Palmer, 2017; Albors, 2016; Kelion, 2013). In other cases, breaches are caused by employees' malicious actions, such as in the example of Morgan Stanley (Gara, 2015).

A fundamental method for addressing insider risk is to adopt information security policies. Existing literature uses the term information security policy (ISP) concepts in slightly different ways. Here we associate ISP "with its non-technical, organizational variant" (Cram *et al.*, 2018), focusing on the strategic and operational levels. In other words, policies addressing top management's strategic direction with regard to information security as well as those including issue-specific guidelines and procedures that employees must comply with on a daily basis (Baskerville and Siponen, 2002; Withman, 2008). However, over the years, we have continued to see that employees' poor compliance with ISPs is a persistent problem for many organisations (Ernst and Young, 2008; Ernst and Young, 2010; Pwc, 2014); findings that have also been supported by researchers (Herath and Rao, 2009; Nash and Greenwood, 2008; Siponen *et al.*, 2014; Stanton *et al.*, 2005; Johnston *et al.*, 2016).

At the same time, it has been shown that about half of all breaches caused by employees are accidental (Vroom and Von Solms, 2004; ENISA, 2014). Furthermore, research (Adams and Sasse, 1999; Stahl *et al.*, 2012; Karlsson *et al.*, 2017) has shown that the design and implementation of ISPs can sometimes impair employees' information security behaviour. They have found that policies can be cumbersome, contradictory and incompatible with existing work practices. Hence, managing ISPs to create a solid foundation for employees' information security behaviour is challenging.

In recognition of this, the number of ISP management studies has increased (Cram *et al.*, 2018) and researchers have contributed towards different kinds of support for the development, implementation and evaluation of ISPs, for example. These contributions address a wide variety of ISP management issues, such as ambiguity (Buthelezi *et al.*, 2016), goal coherency (Karlsson *et al.*, 2017), awareness (Gadzama *et al.*, 2014) and methods to increase compliance (Saran and Zavarsky, 2009). Moreover, these studies target different phases of the ISP management process. Some studies focus on one particular phase of such a process (Doherty and Fulford, 2006; Lindup, 1995). Other studies (Coertze and von Solms, 2013; Knapp *et al.*, 2009) do not treat phases of ISP management as isolated phenomena; instead they recognise that there is interaction between them. Thus, these studies cover more than one phase.

Without question the above-mentioned studies are examples of important contributions. However, they seem to rely on manual support for ISP management. This means that information security managers need to keep track of all the details and coordinate all actors involved, need to be knowledgeable in particular inquiry techniques and have to handle the interaction been different phases of an ISP management process. For example, if they want to carry out a compliance analysis targeting employees they need to be knowledgeable in theories and statistical techniques used in such inquiries. In addition, they need to find a way to reach out to employees and later integrate the results into other phases of the ISP management process.

One way forward is to automate activities associated with ISP management, using computerised support. This kind of support has been around for a long time in information system domains, such as systems development (Jürjens and Shabalin, 2007; Orlikowski, 1993; Pavlidis *et al.*, 2011), method engineering (Efendioglu *et al.*, 2016; Harmsen, 1997; Karlsson and Ågerfalk, 2012; Rossi *et al.*, 2004) and project management (Caniëls and Bakens, 2012;

Jaafari and Manivong, 1998; Raymond and Bergeron, 2008; Teixeira *et al.*, 2016). Even though such support is not without challenges, benefits have been reported. For example, when it comes to computerised support for project management, Raymond and Bergeron (2008) concluded that these systems "have direct impacts on project success, as they contribute to improving budget control and meeting project deadlines as well as fulfilling technical specifications".

Computerised support can also be found in the area of ISP management. For example, already in the start of this century Hoppe *et al.* (2002) and Vermeulen and Von Solms (2002) presented an example of computerised support for information security management; a software that included components for ISP management. A much later example is Syamsuddin and Hwang (2010). They presented a tool for the evaluation of ISP performance. Even though this kind of support has been reported on, it is not known to what extent researchers have actually suggested computerised support for ISP management as a complement or alternative to manual ways of working.

With this in mind, the aim of this paper is to survey existing ISP management research to scrutinise the extent to which manual and computerised support has been suggested, and the way in which the suggested support has been brought about. To the best of our knowledge, there exist a couple of recent literature reviews that systematise and synthesise existing ISP management research (Cram *et al.*, 2018; Flowerday and Tuyikeze, 2016; Alotaibi *et al.*, 2016). However, the extant reviews have yet to consider to what extent researchers have suggested computerised support for ISP management or to what extent suggested support relies on manual work. Specifically, we pose the following research questions:

RQ1. What are the most investigated phases in research on manual and computerised support for information security policy management?

RQ2. To what extent has research on manual and computerised support acknowledged the interaction between information security policy management phases?

RQ3. Which kinds of research methods dominate research on manual and computerised support for information security policy management?

Our results are based on a review of ISP management research published between 1990 and 2017. The study is based on a substantial list of papers that initially consisted of 1,880 research papers, including duplicates. Of these, 123 papers were singled out for further analysis (more details are given in Section 3). Our systematic review provides valuable insights into the extent to which manual and computerised support has been suggested by researchers to ease the burden of information security managers. We have also been able to discuss to what extent the interaction between ISP management phases has been addressed and the types of research methods most commonly used in existing studies. This paper thus contributes with a computerised support perspective on current ISP management research and pinpoints areas for future research.

This paper is structured as follows. Following this introduction, Section 2 describes existing literature reviews of ISP management research. Section 3 presents the research method adopted for our literature review. In Section 4, we present the results of our review. In Section 5, we discuss how our findings impact ISP management research. We end the paper with a short conclusion in Section 6.

2. Related research

ISPs are seen as an important managerial tool for regulating employees' information security behaviours, and this research stream has gained significant attention during the last two decades (Cram *et al.*, 2018). A number of literature reviews (Siponen and Oinas-Kukkonen, 2007;

Siponen *et al.*, 2008; Soomro *et al.*, 2016; Zafar and Clark, 2009) have highlighted ISP studies as an important category within a broader information security literature. Several literature reviews have addressed subsets of the ISP management process such as security awareness (Lebek *et al.*, 2013; Lebek *et al.*, 2014), culture (Karlsson *et al.*, 2015) and employees' behaviours and compliance (Guo, 2013; Sommestad *et al.*, 2014; D'arcy and Herath, 2011; Wall *et al.*, 2015; Siponen and Vance, 2014). Among these subsets of ISP management topics, employees' behaviours and compliance with information security policies has garnered the most attention. Cram *et al.* (2018) argue that the previous reviews of the ISP management literature make it difficult for researchers and practitioners to grasp the current state of knowledge on the whole process of the development, implementation, and effectiveness of ISPs in organisations.

In total, we have found only three reviews (Tuyikeze and Flowerday, 2014; Järveläinen, 2016; Cram *et al.*, 2018) of ISP research covering the entire ISP management process. Tuyikeze and Flowerday (2014) review 21 documents with the objective of understanding the ISP development life cycle. Based on that understanding they define a model for the formulation, implementation and enforcement of an ISP in an organisation. They categorise ISP development and implementation methods found in current literature into five phases:

(1) risk assessment;
(2) policy construction;
(3) policy implementation;
(4) policy compliance; and
(5) policy monitoring, assessment and review.

Thus, the most important contribution of this literature review is to provide a process model for ISP management. The authors do not discuss any possible computerised support for this process or to what extent the ISP development and implementation methods identified in the literature cover the different phases of the ISP management process.

Cram *et al.* (2018) review 114 ISP-related publications from 34 journals and synthesised the current knowledge in the form of a research framework. The authors categorised the existing ISP literature into five relationships covering the entire ISP development process:

(1) influences on the design and implementation of ISPs (e.g., standards and guidelines);
(2) the influence of ISPs on the organisation (e.g. security culture) and individual employees (e.g. socioemotional well-being);
(3) the influence of the organisation and individual employee factors on ISP compliance (e.g. dispositional traits, sanctions, rewards);
(4) the influence of ISP compliance on organisational objectives (e.g. the frequency of security incidents); and
(5) adjustments to ISP design (e.g. policy updating and maintenance). Building on the analysis the authors identified research gaps that can be used as a basis for future research.

Cram *et al.* (2018) conclude that the vast majority of the current ISP literature focuses on understanding the drivers of ISP compliance, while fewer studies consider other aspects of ISP management. Studies considering other parts of ISP management are often based on practical considerations of managers responsible for the design and implementation of policies and not clearly founded in theory. Many of these studies are also conceptual, which according to Cram *et al.* (2018) may limit the possible impact of these studies for practice. They also argue

that almost none of the reviewed studies consider ISP management as an ongoing process where changes occur to policies over time. The authors argue that taking an iterative perspective towards ISP development, implementation, monitoring and adjustment, would uncover new and important insights, but at the same time applying such a perspective adds an additional complexity for information security managers. Cram *et al.* (2018) show that this type of research focuses mostly on conceptual factors that need to be considered when adjusting information security policies over time. However, almost no empirical research exists on how such adjustment is (or should be) managed in practice, leaving information security managers without support regarding this challenging task.

Although Cram *et al.* (2018) discuss the need for management support in the process of developing, implementing, monitoring, and adjusting ISPs, they do not assess to what extent existing research has proposed computerised support for this process. Moreover, they do not explicitly discuss to what extent existing studies cover the different phases of the ISP management process. Finally, although Cram *et al.* (2018) present an appendix containing an account of the research method used in the reviewed studies, they do not discuss these findings.

Järveläinen (2016) conducted a literature review of 46 papers focusing on ISP development. This review acts as a background to putting forth an integrated approach to ISP development and business continuity planning. She concludes that:

- ISPs are supposed to be a comprehensive set of long-lasting, general, technology-independent principles.
- The main objective of an ISP is to ensure the confidentiality, integrity and availability of data for an organisation.
- ISP should be developed based on the assessment of current and previously recognised risks.
- An organisation can have several different kinds of ISPs for different stakeholders and for that reason different groups of stakeholders should be involved in the ISP development.

Järveläinen (2016) does not discuss computerised or non-computerised support for ISP development.

3. Research method

A structured literature review is a "crucial endeavour" (Webster and Watson, 2002) for a research community, as it provides an overview and synthesis of what has been accomplished so far. It is therefore vital that it is carried out in a rigorous and comprehensive manner (Levy and Ellis, 2006). Our research method is quite straightforward on the general level, consisting of four main steps. That said, their implementation has been far from instrumental and below we discuss the details related to selecting and classifying papers. The general outline of the research process is as follows:

(1) Elseviers' database Scopus and Clarivate Analytics' database Web of Science were used to search for potential papers (see Section 3.1).

(2) The abstract of each paper was read and an initial decision was made as to whether the research related to ISP management (see Section 3.1).

(3) The introduction, related research and results sections were read for each paper in search of:

- the kind of research topics that the paper addressed to map them onto different phases of ISP management. We used the process model proposed by Flowerday and Tuyikeze (2016) for classification of the research topics (see Section 3.2).
- the different types of support – manual and/or computerised – that the paper suggested (see Section 3.3).
- the number of phases of ISP management that the paper covered, to classify the addressed interaction between different phases (see Section 3.4).

(4) The research method section of each paper was read (if such a section was found) and the research methods that the researchers claimed to have used were noted. These were classified using an extended version of Mingers' (2003a) research method framework (see Section 3.5).

Initially Steps 3 and 4 were carried out in an iterative pattern where the authors individually classified the same set of papers and later compared the classifications made. This was done to arrive at a stable interpretation of our analytical framework, i.e. where the authors classified the papers in the same way. A consistent use of the analytical framework was reached after three iterations. The first author then carried out the analysis of the remaining papers. Ambiguous papers were discussed by the authors and joint decisions were made. The result of the detailed analysis is found in Appendix 6; a summary is presented in Section 4.

3.1 Selection of papers

ISP management research appears both in conference proceedings and in international journals. Therefore, we aimed for an inclusive selection of papers. Our search of papers was carried out using Scopus and Web of Science. Scopus is "the largest abstract and citation database of peer-reviewed literature", indexing 20,000 peer-reviewed journals and 5.5 million conference papers, and Web of Science covers over 12,000 of the most high impact journals and over 150,000 conference proceedings (Franke and Brynielsson, 2014). Scopus provides a good coverage of the journals on the Association of Information Systems' journal ranking list and specific information security journals and conferences (Karlsson *et al.*, 2015). All in all, these two databases together provide a good coverage with regards to ISP management.

The search included papers published on the databases between 1990 and 2017. The year 1990 was selected because this was when Straub and Nance (1990) published their paper on computer abuse; it is an early example of information security management research that relates to ISPs. Our search included journal papers, conferences papers and workshop papers, regardless of the geographic region to gain an inclusive view of the field. Appendix 1 shows the search criteria that were used when searching in the databases; search fields included paper title, abstract and keywords. The set of keywords we used to construct the search criteria grew as we learned more about ISP management research based on our searches and reading of papers. The use of multiple search queries resulted in a substantial list of 1,880 research papers, including duplicates. After eliminating duplicates and papers that did not meet our inclusion criteria in Table I we ended up with a net list of 130 papers. In the end we were able to access and analyse 123 papers. The papers we were unable to access are listed in Appendix 3.

This reduction in relevant papers was due to our inclusive search strategy. It meant that papers were included in the first dataset if they were related to ISPs. For example, an extensive number of studies on employees' compliance with ISPs were therefore included. However, these papers have different emphases on ISPs. For example, Hedström *et al.* (2011) used actual ISPs as reference objects in the compliance analysis and are therefore included.

In addition, our inclusive search strategy meant that we, in our first dataset, came across papers about computerised tool support for implementing and automating technical information security policies. For example, Subramanian *et al.* (2011) proposed the PCAL-analyser, a computerised tool to ease the burden of security administrators when analysing technical ISPs; they provided an illustrative example comparing two Unix server security policies. Although such papers are about computerised support, they obviously fall short of the type of ISPs we are interested in. Nonetheless, we chose the abovementioned search strategy to ensure we would not miss any papers by making the search parameters too narrow.

3.2 Classification of research and information security policy management phases

The first component of our classification framework addresses research topics in relation to phases of ISP management. Existing literature provides more than one process model for such an analysis (Howard, 2007; Kadam, 2007; Peltier, 2004; Flowerday and Tuyikeze, 2016), which means that such a classification can be done in slightly different ways. We have chosen to use Flowerday and Tuyikeze (2016) ISP management process model; this is one of the more recent models and is based on a literature review. Hence, it gives us the possibility of comparing our findings with existing wisdom in the field.

As discussed earlier, Flowerday and Tuyikeze (2016) divide ISP management into five phases. We organised each of the 123 papers into one or more of these phases, because a paper can cover more than one part of the process model. The five phases are risk management, policy construction, policy implementation, policy compliance and policy monitoring. The risk management phase focuses on ISP management research that addresses an organisation's need to "identify the threats, vulnerabilities and risks that need to be mitigated" (Flowerday and Tuyikeze, 2016). Policy construction is about activities and aspects to consider when developing an ISP. This includes challenges related to writing a detailed policy and consultation with stakeholders. Policy implementation represents deployment activities and aspects of ISP management. This phase focuses on policy awareness, education and training. Policy compliance addresses employees' compliance and non-compliance with ISPs and different ways of assessing compliance/non-compliance. The final phase, policy monitoring focuses on audit and review aspects related to ISPs. Based on the audit and review results changes can be proposed.

3.3 Classification of type of support

Our interest in manual and computerised support for ISP management led us to complement the model put forward by Flowerday and Tuyikeze (2016). We added two categories – manual and computerised support – that cut across the five phases discussed above. This created an analytical matrix that enabled us to identify research that has addressed manual and/or computerised support for the different phases of ISP management. In this study, we

No.	Inclusion criterion
1	Paper is written in English
2	Paper is peer-reviewed
3	Paper focuses on information security policies as a study object
4	Paper focuses on information security policy management in organisations
5	Paper focuses on strategic and/or operational information security polices (i.e. technical policies were excluded)

Table I.
Inclusion criteria for papers

define manual support for ISP management as any justified and explicit guidance that assists an information security manager in terms of working with ISP management. For example, in our analysis of Karlsson *et al.* (2017) we found that they present eight criteria that can guide construction of ISPs. Computerised support for ISP management was defined as a software that assists an information security manager in working with ISP management. Thus, when analysing, for example, Coertze and von Solms (2013), we concluded that the presented software includes computerised support for risk management, policy construction, policy compliance and policy monitoring.

3.4 Classification of the interaction between information security policy management phases

As discussed in the Introduction, there is interaction between different ISP management phases. This is also evident in the framework proposed by Flowerday and Tuyikeze (2016), where the five consecutive phases build on each other. For example, an ISP is developed based on threats and vulnerabilities identified during risk management. Compliance on the other hand needs to be understood and assessed based on the existing ISP. We have therefore analysed to what extent researchers have acknowledged the interaction between different phases in ISP management, i.e. the number of phases that individual studies have covered.

Table II presents this component of our analytical framework, which is a straightforward and intuitive use of the five phases suggested by Flowerday and Tuyikeze (2016). The leftmost column contains the three levels of interaction, and the second column shows the operational definitions. The general idea is that higher interaction includes more ISP management phases, while a lower interaction would focus more on a specific part of ISP management.

3.5 Classification of research methods

The fourth and final component in our classification framework concerns the research method used. Given that several frameworks are available for this purpose (Galliers, 1992; Mingers, 2003a; Palvia *et al.*, 2004; Dwivedi and Kuljis, 2008), it is inevitable that such a classification can be carried out in slightly different ways. We used an extended version of Mingers' (2003a) framework, even though it adopts a rather inclusive view of research methods. The main reason is that we benefited from the opportunity to make nuanced characterisations of the research methods used. Mingers' (2003a) original framework includes 13 types of research methods, to which we have added two. The first is design science, which has received increasing attention in recent years, most notably after he developed his framework. Finally, we have added the category "no method" to capture cases where the authors have not explicitly stated or described the research method(s) they have used.

Table II.
Level of acknowledged interaction between information security policy management phases

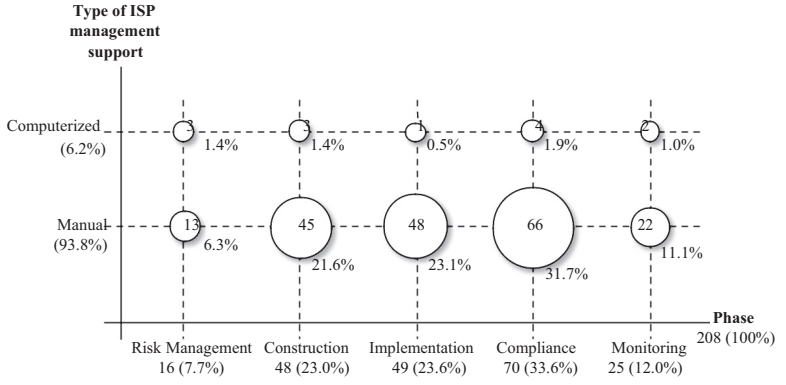
Level of interaction	Operational definition
Low	Research addressing one of the ISP management phases in Flowerday and Tuyikeze's (2016) framework, i.e. takes a silos model approach to ISP management. This is conceptualised as a single-phase paper
Medium	Research addressing two to four phases, either consecutive or separated, in Flowerday and Tuyikeze's (2016) framework
High	Research addressing all five ISP management phases in Flowerday and Tuyikeze's (2016) framework

All in all, our extended framework includes 15 types of research methods: action research, case study, consultancy, critical theory, design science, ethnography, experiment, grounded theory, interview, no method, participant observation, passive observation and measurement, qualitative content analysis, simulation and survey/questionnaire/instrument. The operational definitions of these types of research methods are found in Appendix 4. In our classification, we acknowledged the possibility of studies using a mixed-method (Creswell, 2003) or multi-method (Brewer and Hunter, 1989) approach, i.e. when a study includes the use of more than one research method.

4. Results

In this section, we present a summary of our literature review, structured into three subsections. The first subsection focuses on what are the most investigated phases of ISP management. We start by assessing research on manual support for ISP management and then continue with research on computerised support for ISP management. In the second subsection, we concentrate on to what extent research has addressed the interaction between ISP management phases. Finally, the last subsection presents the dominant research methods in the assessed studies. In addition, we analyse what kind of research methods have been used to research the interaction between the ISP management phases. The details of our analysis are found in Appendix 5–6.

The overall analysis shows that 117 papers have addressed manual support for ISP management, while only 7 papers have approached computerised support. It is clearly evident that researchers have put more emphasis on manual support than on computerised support for ISP management. Figure 1 characterises existing research further using a bubble chart. The horizontal axis contains the five phases found in Flowerday and Tuyikeze (2016) framework and the vertical axis shows the two types of ISP management support. A bubble chart shows three dimensions of the data. The size of a bubble is proportional to the frequency of papers that are in the pair of categories corresponding to the bubble coordinates. Our analysis suggests that all phases have been addressed for both manual and computerised support for ISP management, although with different degrees of emphasis. The shares have been calculated based on the total number of times the phases in the framework have been addressed.



Note: Please note that papers can address more than one phase, which means that the total number of addressed phases exceeds the actual number of papers

Figure 1. Existing research's overall emphasis of different phases

4.1 Information security policy management phases addressed

4.1.1 Research on manual support. In the bottom-left of Figure 1, we find risk management. The figure shows that it is the phase that researchers have devoted least attention to when it comes to manual support for ISP management. We found that the majority of papers in this area focused on ways of identifying risks, threats and vulnerabilities, and proposing solutions to mitigate them properly (Palmer *et al.*, 2001; Kadam, 2007; Simms, 2009; Tuyikeze and Pottas, 2011; Ismail and Widyarto, 2016). For example, Kadam (2007) suggests an approach for formulating ISPs: the first stage in such a process is threat identification and vulnerability assessment. Hence, the suggested stage is about risk management and Kadam suggests a tool for risk analysis using confidentiality, integrity and availability. The tool also includes possibilities for adding references to where the vulnerabilities are addressed in the ISP. The goal seems to be increased traceability in the ISP management process.

Construction is the second phase from the left in Figure 1. This phase is the third largest area of research concerning manual support for ISP management. Construction research has addressed what constitutes an ISP and why ISPs should be developed (Al-Hamdani and Dixie, 2009; Hong *et al.*, 2006; Cosic and Boban, 2010; Koziel, 2011). Researchers have also addressed how to formulate ISPs (Lindup, 1995; Tuyikeze and Pottas, 2011; Lopes and Oliveira, 2015c; Niemimaa, 2016), i.e. focusing on construction as an activity. We also identified a number of studies that addressed what factors should be considered during such processes to end up with effective ISPs (Gritzalis, 1997; Siponen and Iivari, 2006; Hong *et al.*, 2006; Renaud and Goucher, 2012). Finally, researchers have emphasised the importance of considering business requirements and goals when formulating ISPs (Doherty and Fulford, 2006).

Implementation is the third phase from the left in Figure 1, and the second largest area of research. We identified implementation research on factors that affect the effective adoption and enforcement of an ISP (Fragos *et al.*, 2007; Hong *et al.*, 2006; Yayla, 2011). Researchers, such as Karyda *et al.* (2003) and Kadam (2007), have also addressed when it is appropriate to implement ISP and who should be involved in such implementation. Another implementation aspect addressed is dissemination and successful deployments of ISPs (Fulford and Doherty, 2003; HöNe and Eloff, 2002b). Research on implementation has also devoted attention to the importance of employees' awareness and understanding of ISPs (Gadzama *et al.*, 2014; Ghazvini and Shukur, 2016; Ghazvini and Shukur, 2017). Finally, researchers have acknowledged the importance of paying attention to organisational differences during implementation. For example, Al-Hamdani and Dixie (2009) discuss how ISP implementation in small organisations differs from implementation in larger organisations.

Compliance is the fourth phase in Figure 1, and is by far the phase that researchers have devoted the most attention to over the years. Compared to the other phases, compliance research seems to have a quite unified focus; trying to increase the understanding of what explains employees' compliance and non-compliance. Such an increased understanding would feed into the other phases of ISP management; for example how to construct an ISP in a way that will improve compliance. Our review reveals that an extensive number of theories have been applied in this type of research. First, we identify a large number of studies that draw on theories from psychology. One such theory that has attracted a lot of attention is theory of planned behaviour (Aurigemma and Mattson, 2017a; Bulgurcu *et al.*, 2009a; Hu *et al.*, 2012; Bulgurcu *et al.*, 2010; Gerber *et al.*, 2016). Protection motivation theory (Pahnila *et al.*, 2013; Herath and Rao, 2009) is another theory from psychology that has been used to explore employees' compliance and non-compliance with ISPs. Second, researchers have also used theories from criminology to explain employees' compliance and non-

compliance, such as deterrence theory (Chen *et al.*, 2012), neutralisation theory (Bauer and Bernroider, 2017) and social control theory (Hsu *et al.*, 2015). Compliance research has also drawn on theories from sociology. Here we found theories such as social action theory (Hedström *et al.*, 2013). We also identified one theory, value-based compliance theory (Hedström *et al.*, 2011; Kolkowska *et al.*, 2017), which is specifically constructed in the sub-field of ISP management. One thing that is striking with regard to compliance research is that several of the abovementioned theories or parts thereof are frequently combined (Aurigemma and Mattson, 2017b; Ifinedo, 2012; Ifinedo, 2016; Kajtazi and Bulgurcu, 2013; Siponen *et al.*, 2006; Sohrabi Safa *et al.*, 2016; Hou *et al.*, 2011; Humaidi and Balakrishnan, 2015a).

Finally, monitoring is the fifth investigated phase in Figure 1. As is shown in the figure, this phase has attracted relatively few papers, compared to research on compliance, construction and implementation. We have identified monitoring research that assesses and reviews the effectiveness of ISPs (Höne and Eloff, 2002a; Karyda *et al.*, 2003; Vroom and Von Solms, 2003; Corpuz and Barnes, 2010). Researchers have also focused on evaluating to what extent ISP objectives and business objectives are aligned (Mader and Srinivasan, 2005; Knapp *et al.*, 2009; Hong *et al.*, 2006). Finally, researchers have addressed solutions which can improve such an alignment (Talbot and Woodward, 2009; Ismail and Widyarto, 2016; Karlsson *et al.*, 2017).

4.1.2 Research on computerised support. Figure 1 shows that research on computerised support for ISP management research is far less common than research on manual support. In total we identified seven papers in the former category. Starting with risk management, we identified three papers addressing this phase (Vermeulen and Von Solms, 2002; Coertze *et al.*, 2011; Coertze and von Solms, 2013). Vermeulen and Von Solms (2002) propose a software tool – information security management toolbox – to automate a number of steps of information security management. The software tool they suggest is an implementation of a limited part of a method for information security management. Risk management is among the parts supported by the software tool, providing support in eliciting information security requirements that can be used as input for ISP construction. Later, Coertze *et al.* (2011) and Coertze and von Solms (2013) seem to have extended this work. However, the software tool has different names and seem to cover our investigate ISP management phases to different extent. In addition, it is difficult to judge whether the toolbox focuses on ISPs in particular or addresses information security management, of which policies are one component.

Construction has been addressed in three papers (Vermeulen and Von Solms, 2002; Coertze *et al.*, 2011; Coertze and von Solms, 2013). These papers all concern the same computerised support – the information security management toolbox. Vermeulen and Von Solms (2002) show in their implementation model of the tool how business-specific requirements help in selecting organisation-specific ISP statements. Although they do not provide any details, Coertze and von Solms (2013) claim that the toolbox supports the "drafting of dynamic policy".

Implementation has been addressed in one paper by Busch *et al.* (2016). They designed and implemented a number of persuasive information security features in an interactive Web-based tool. The purpose was to increase employees' awareness and knowledge of an organisation's ISP. Hence, this is related to implementation. The goal of the study was to evaluate the effectiveness of these different features.

Figure 1 shows that compliance has been addressed in four papers (Busch *et al.*, 2016; Saran and Zavarsky, 2009; Coertze and von Solms, 2013; Wang and Li, 2015). The above-mentioned paper by Busch *et al.* (2016), which evaluates the effectiveness of persuasive information security features, also promotes ISP-compliant behaviour. Saran and Zavarsky

(2009) studied a non-compliance problem with an Internet policy in an insurance company. Taking an inclusive view on computerised support for ISP management, they used emails to improve the situation. They tested and evaluated different methods for increasing ISP compliance: they investigated whether compliance was increased by sending different types of reminder emails to employees, saying that they needed to re-sign the organisation's Internet Usage Agreement. Coertze and von Solms (2013) provide the possibility of conducting compliance analyses using their suggested computerised toolbox for information security management. Finally, Wang and Li (2015) used computerised support to visualise employees' ISP compliance patterns.

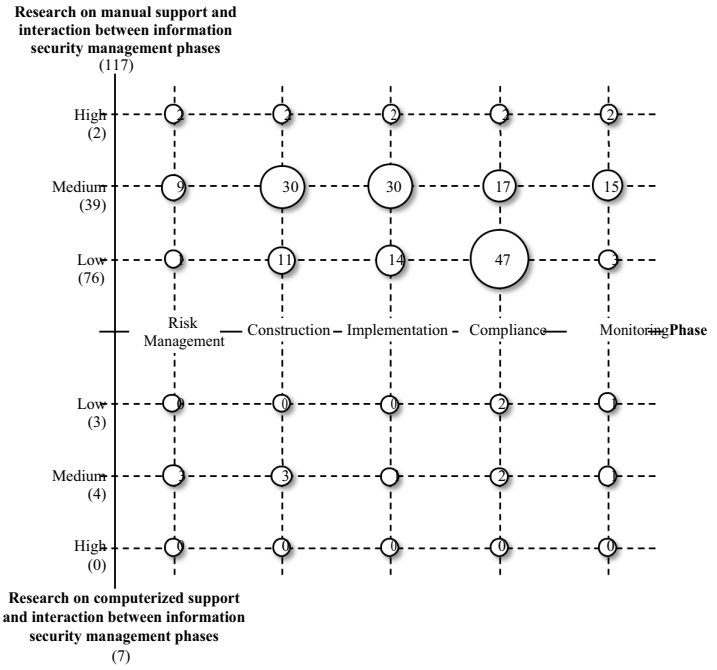
Finally, monitoring has been addressed in two papers (Syamsuddin and Hwang, 2010; Coertze and von Solms, 2013). Syamsuddin and Hwang (2010) introduced a framework that guides managers when "evaluating information security policy performance". The suggested framework, which was demonstrated as an Open Office Calc application, adopts the analytic hierarchy process to structure and understand performance. Their choice of demonstrator was based on their goal to show that this kind of support can be provided without the use of proprietary analytic hierarchy process software. The second paper is the previously discussed paper by Coertze and von Solms (2013). They argue that the toolbox components offer the opportunity to evaluate ISP management efforts carried out. Hence, such functionality is similar to the audit and review aspects put forth in the framework by Flowerday and Tuyikeze (2016).

4.2 Interaction between information security policy management phases

In this section, we analyse to what extent research has addressed interaction between phases in ISP management. As discussed in Section 3.4, interaction means to what extent researchers have treated the different phases as separate silos (for example focusing only on construction) or have combined them in the same study (for example addressing risk assessment, construction and implementation). The details of the analysis are found in Appendix 5 and Figure 2 presents an overview using a bubble plot. The figure is divided into an upper and a lower section containing analyses of research on manual and computerised support for ISP management respectively. The vertical axis shows the three types of interaction that we have defined earlier, i.e. how many ISP management phases have been included in a paper. On this axis, we also present the total number of papers that address a certain level of interaction. The horizontal axis shows the actual phases that have been acknowledged in research, using the five phases suggested by Flowerday and Tuyikeze (2016). Thus, in each intersection the bubbles show how much focus a particular phase has received in the context of a specific level of interaction (i.e. how many papers have been written on any particular interaction between phases).

4.2.1 Research on manual support. The upper section of Figure 2 presents research on manual support and the acknowledged interaction between ISP management phases. This part of the figure shows that the number of studies decreases when the addressed interaction between phases increases. This might not be a surprising finding in itself, because studies addressing higher levels of interaction are more resource consuming.

We can conclude that most papers, 76 articles out of 117, are found in the low interaction category. This means that these studies have a silos approach to manual support for ISP management (Gritzalis, 1997; Fulford and Doherty, 2003; Fragos *et al.*, 2007; Lopes and Oliveira, 2015a; Niemimaa, 2016), only addressing one phase. For example, Fragos *et al.* (2007) used the lens of circuit of power to understand the implementation of ISP in a public sector organisation. They showed that power relations are important during ISP implementation and that such relations need to be



Note: Please note that papers can address more than one phase, which means that the number of papers on the vertical axis is not a summary of how many papers have addressed particular phases

Figure 2.
Level of interaction within research on manual and computerised support for information security policy management

acknowledged. Although this is an important finding, this study is limited to a specific phase of ISP management, in this case implementation. Moreover, it is evident that research on compliance dominates when the acknowledged interaction is low. This should not be a surprising finding; as discussed above, compliance is the phase that has attracted the most attention in ISP management research overall. At the other end, we found that risk management is the phase that has received the least attention when the acknowledged interaction is low. We only identified one paper (Rees and Allen, 2008) that focused solely on this phase. Furthermore, only a small portion of the research has been devoted to policy monitoring as an isolated phase.

Figure 2 also shows that when the level of interaction is increased to medium – research combining two to four phases – the emphasis on different phases changes. We see that more focus is placed on construction and implementation, and less focus is placed on compliance. The details in Appendix 5 reveal that studies addressing manual support and two ISP management phases frequently combine construction-implementation (Gaunt, 1998; Abraham and Chengalur-Smith, 2011), construction-compliance (Buthelezi *et al.*, 2016; Choi, 2016) and implementation-compliance (Yang *et al.*, 2011; Mavetera *et al.*, 2015).

However, interest in including risk management and monitoring seems to have been low. Instead, Appendix 5 shows that more attention has been devoted to monitoring when three or more phases are combined. In such studies researchers seem to have concentrated on combining risk management, construction, implementation and monitoring (Palmer *et al.*,

2001; Simms, 2009; Corpuz and Barnes, 2010; Ismail and Widyarto, 2016). Hence, here compliance research received even less attention.

As Figure 2 shows, we only identified two papers in the high interaction category (Tuyikeze and Pottas, 2011; Knapp *et al.*, 2009), i.e. that addressed a combination of all five phases. For example, Tuyikeze and Pottas (2011) present a detailed roadmap for ISP management, to ensure that ISPs are "comprehensive, effective and sustainable" with regard to organisations' needs and regulatory requirements. Although the roadmap only includes four steps compared to the five phases found in Flowerday and Tuyikeze (2016) framework, the authors state that policy compliance should be considered part of policy monitoring and maintenance.

4.2.2 Research on computerised support. The lower section of Figure 2 summarises research on computerised support and to what extent interaction between ISP management phases has been addressed. We can conclude that research on computerised support with low and medium interaction dominates, although the numbers are much lower compared to research on manual support. Actually, we were unable to identify any papers in the high interaction category. Even though papers with such acknowledged interaction are few in the area of manual support, we still found some.

Given the few papers on computerised support for ISP management it is not possible to identify any patterns regarding how phases are combined when the addressed interaction changes. For example, we found that the three papers that use a silos model address three different phases. Saran and Zavarsky (2009) measured whether reminder e-mails of a policy re-release have an impact on compliance, while Syamsuddin and Hwang (2010) address monitoring with their non-proprietary analytic hierarchy process software. Wang and Li (2015) address compliance when visualising compliance patterns. When we examine existing studies with medium interaction, we see that all phases are included at least once. For example, Busch *et al.* (2016) in their paper on persuasive information security features combine implementation and compliance. The three papers (Vermeulen and Von Solms, 2002; Coertze *et al.*, 2011; Coertze and von Solms, 2013) addressing the information security management toolbox have addressed different combinations of phases. Of these papers, Coertze and von Solms (2013) undertook the study that includes the highest number of ISP management phases, when introducing the ISP management toolbox to small, medium and micro-organisations. In this study, they address the combination of risk assessment, construction, compliance and monitoring.

4.3 Research methods used in research on information security policy management

The bubble charts in Figures 3 to 5 show our analysis of research methods used in existing research on ISP management. Figure 3 contains an analysis structured according to the two types of support – manual and computerised – that we are interested in. Figure 4 shows a more detailed analysis where the use of research method has been structured according to the phases in Flowerday and Tuyikeze (2016) framework. The upper section of this figure shows how research methods have been used in research on manual support; the lower section shows how research methods have been used in research on computerised support. Finally, Figure 5 contains an analysis of how frequently the research methods have appeared in studies with different types of interaction. This figure is also divided into two sections similarly to Figure 4.

In the figures we only present the research methods that have been used in existing research, which means the figures only contain a subset of our modified version of Mingers (2003a) framework. In total, we found that 14 different research methods were used for ISP management investigations. Thus, a wide variety of research methods have been used. That said, there are

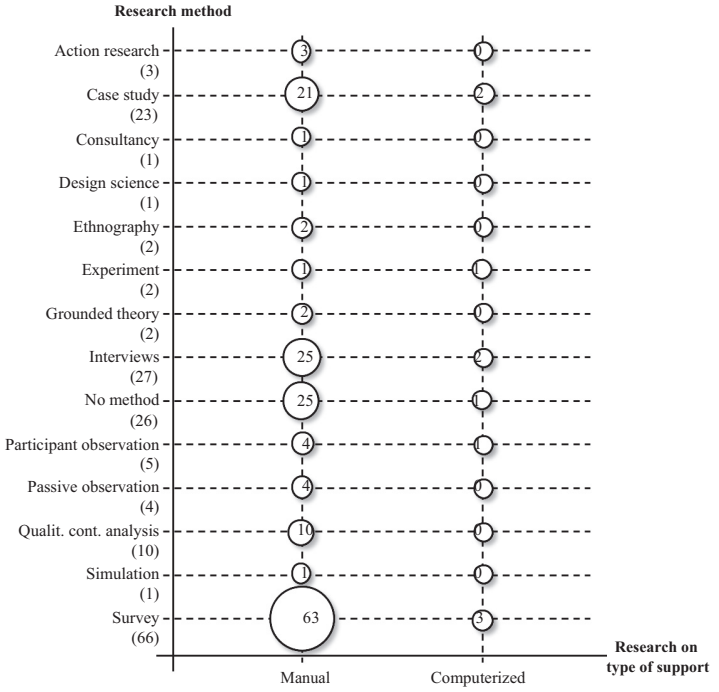


Figure 3.
Types of research methods used in research on information security policy management

substantial differences in frequency of use. We can clearly see that four research methods – survey, interview, no method and case study – dominate ISP management research.

4.3.1 Research on manual support. We start with an assessment of research methods used in research on manual support for ISP management. As is shown in Figure 3, survey is by far the most-used research method and seems to hold a special position in this kind of research. It is used in 63 out of 117 papers that address manual support. Moreover, as can be seen from the upper section of Figure 4, the majority of these papers focus on policy compliance (D'Arcy *et al.*, 2014; Bulgurcu *et al.*, 2010; Siponen *et al.*, 2006). Indeed, the figure reveals that compliance research seems to have a strong emphasis on surveys. As this phase constitutes a large share of the research on manual support for ISP management it becomes quite natural that the number of survey studies is high. As is shown in Figure 5, the majority of the survey studies do not address any interaction between the phases in Flowerday and Tuyikeze (2016) framework. This is in line with our previous analysis in Figure 2, where we show that researchers have mostly studied compliance as an isolated phase in ISP management.

Continuing in Figure 3, we find three research methods that are roughly equal in size: interviews, no method and case study. They have each been used in about one-fifth of the investigated studies on manual support. Starting with interviews, the upper section of Figure 4 shows that most of this research is concerned with policy construction (Yusufovna, 2008; Karlsson *et al.*, 2017), policy implementation (Karyda *et al.*, 2003; Abraham and Chengalur-Smith, 2011) and policy compliance (Knapp *et al.*, 2009; Hedström *et al.*, 2011). Compared to the use of surveys discussed above, none of these phases have such a clearly dominant position as policy compliance has in relation to survey studies. Furthermore,

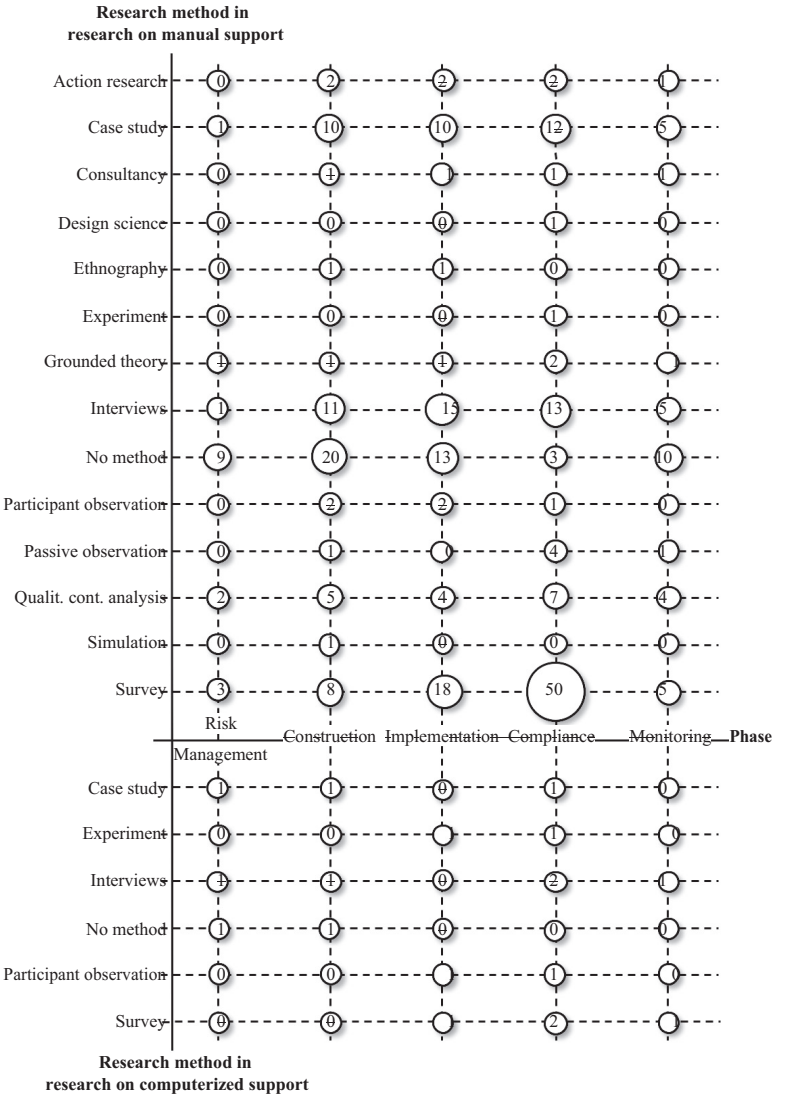
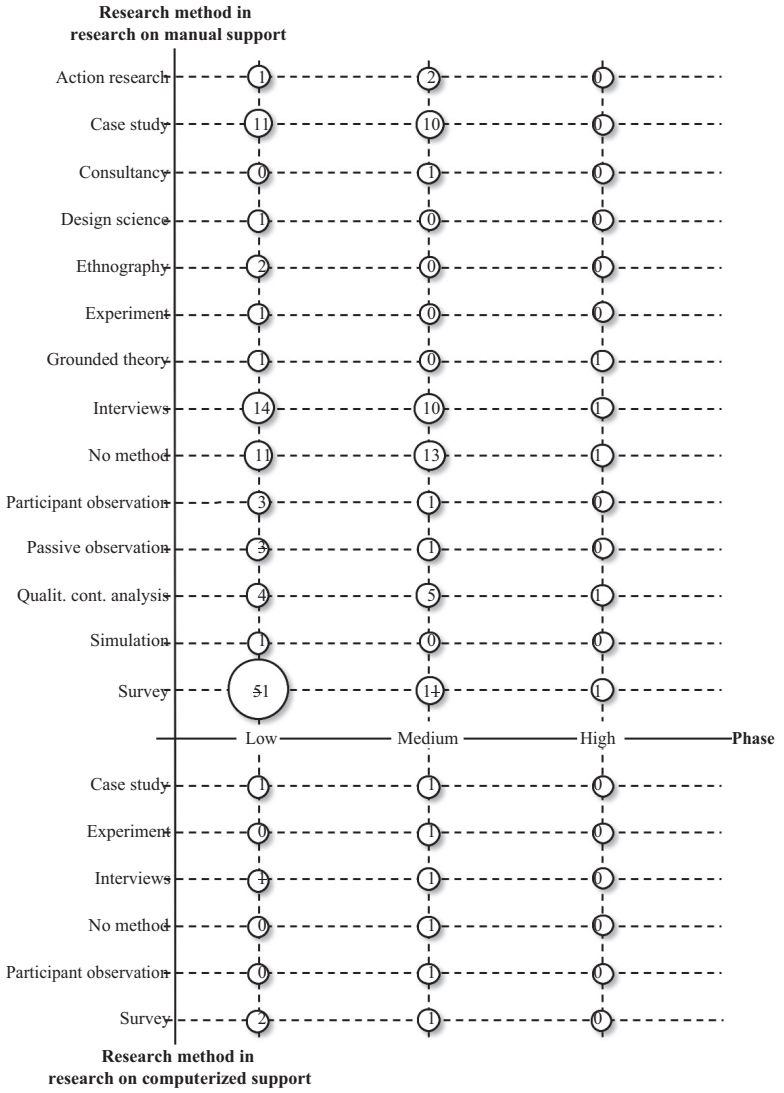


Figure 4.
Types of research methods used

Note: Please note that papers can use more than one research method, which means it is not possible to summarise the number of studies analysed

Figure 5 reveals that interviews have been used to address low and medium interaction between ISP management phases.

Studies where the researchers have not explicitly described the used research method, classified as no-method papers in our framework, also account for about one-fifth of the studies reviewed. According to the analysis in Figure 4, we found that such papers are most frequently concerned with policy construction (Lindup, 1995; Siponen and Iivari, 2006),



Note: Please note that papers can use more than one research method, which means it is not possible to summarise the number of studies analysed

Figure 5.
Types of research methods used and types of interaction between phases

followed by policy implementation (Palmer *et al.*, 2001; Tsohou *et al.*, 2015). Figure 5 shows that not describing the used research method is equally frequent in studies with low and medium acknowledged interaction.

According to Figure 3, the case study is the fourth most frequently used research method; the fact is that there is not much difference in the frequencies of use of case studies,

interviews and no-method papers. Moreover, Figure 4 shows that the use of case studies resembles the use of interviews; it has mostly been used to research policy construction (Yusufovna, 2008; Karlsson *et al.*, 2017), policy implementation (Abraham and Chengalur-Smith, 2011; Lapke and Dhillon, 2015) and policy compliance (Hedström *et al.*, 2011; Buthelezi *et al.*, 2016). The details in Appendix 6 show that these two research methods are frequently combined. Figure 5 also shows that case study research seems to share the same pattern of addressing low and medium interaction between ISP management phases.

When it comes to the remaining research methods in our framework, they have been used in fairly low numbers. As Figure 3 shows, all of them have appeared in ten or fewer studies on manual support. For example, qualitative content analysis has appeared in ten papers. Figure 4 shows that these studies have included a broad range of the phases in Flowerday and Tuyikeze (2016) framework. The reason is, according to Figure 5, that this research method is often part of studies with medium acknowledged interaction between ISP management phases. Continuing in Figure 3, participant observation and passive observation were only used in four studies each; given this low frequency it is not possible to identify any patterns in terms of how they have been used. Finally, we found a small number of studies that used ethnography (Niemimaa, 2016; Niemimaa and Niemimaa, 2017), action research (Lopes and Oliveira, 2015b; Lopes and Oliveira, 2015c; Lopes and Oliveira, 2016), grounded theory (Knapp *et al.*, 2009; Balozian and Leidner, 2016), experiment (SanNicolas-Rocca *et al.*, 2014), simulation (Doherty and Fulford, 2006), consultancy (Talbot and Woodward, 2009) and design science (Kolkowska *et al.*, 2017). For example, in the last study, design science was used to develop a method for analysing reasons behind employees' compliance and non-compliance. It should be mentioned that we did not identify any use of critical theory in research on manual support for ISP management.

4.3.2 Research on computerised support. Turning our attention once more to research on computerised support for ISP management, we can see in Figure 3 that fewer types of research methods have been used compared to those used in research on manual support for ISP management. Given that we have identified few papers on computerised support, it is natural to find a more limited set of research methods both with regard to breadth and frequency. Moreover, the limited number of papers on computerised support makes it difficult to identify any patterns when it comes to how research methods have been combined with different phases (Figure 4) and the addressed interaction between ISP management phases (Figure 5).

As is shown in Figure 3, the most-used research method is survey (Busch *et al.*, 2016; Syamsuddin and Hwang, 2010; Wang and Li, 2015). It is followed by case study (Coertze *et al.*, 2011; Saran and Zavarsky, 2009), and interview (Coertze and von Solms, 2013; Wang and Li, 2015), each of which have been used in two papers. We also identified use of experiment (Busch *et al.*, 2016) and participant observation (Busch *et al.*, 2016); each method has been used in one paper. Finally, we found one paper that did not give any account of the research method used (Vermeulen and Von Solms, 2002). This means we did not identify any papers on computerised support that used the following research methods: action research, critical theory, consultancy, design science, ethnography, grounded theory, passive observation, qualitative content analysis and simulation.

5. Discussion

Our literature review considers the entire process of ISP management, similarly to Tuyikeze and Flowerday (2014), Järveläinen (2016) and Cram *et al.* (2018). It contributes to previous knowledge by explicitly focussing on the extent to which manual and computerised support have been suggested, and the ways in which the suggested support have been brought

about. Figures 1 to 5 show the patterns we found in the current literature. Based on our findings, some notable lessons can be learned with regard to:

- the phases investigated in research on manual and computerised support for ISP management;
- to which extent interaction between these phases has been acknowledged; and
- types of research methods used.

5.1 Investigated information security policy management phases

In our analysis of existing ISP management research, we identified 117 studies that considered manual support and only seven studies that considered computerised support. This low number of studies considering computerised support was unexpected since the first studies within this area were published already at the turn of the century (Hoppe *et al.*, 2002; Vermeulen and Von Solms, 2002). Taken together, our results show that existing ISP management research has focused mainly on manual support, and research with an explicit focus on computerised support is, to date, very scarce. Indeed, this points towards a considerable knowledge gap in ISP management research and provides an important opportunity for future research: to develop, test and evaluate computerised support. Such research is important to understand what effects computerised support could have on ISP management.

The avenues for future research on support for ISP management were made even more specific when we analysed the existing research using Tuyikeze and Flowerday's (2014) framework. This analysis showed that all phases have been addressed in papers on both manual and computerised support, albeit not with similar emphases. In papers on manual support, the focus was mostly on policy compliance, followed by policy implementation and policy construction. Risk management and policy monitoring are phases that have received the least attention. This pattern corroborates findings in previous literature reviews (Tuyikeze and Flowerday, 2014; Cram *et al.*, 2018; Wang and Li, 2015). Lack of ISP management research concerning risk management may lead to insufficient understanding of organisations' needs and/or addressing of organisation-specific threats, vulnerabilities and risks, which in turn makes it difficult to develop effective ISPs. Limited research on policy monitoring, which focuses on audits and reviews of ISPs, may result in difficulties in keeping ISPs up-to date and adjusting them to organisations' continuously changing requirements and needs. Hence, in general more research concerning risk management and policy monitoring is needed.

In contrast to the previous reviews, our review also analysed the phases investigated in research on computerised support for ISP management. Because of the low number of studies focusing on computerised support, it is difficult to discuss any patterns in distribution between the ISP management phases. We can conclude that computerised support for ISP management is understudied in relation to all five phases of ISP management. Consequently, the research community does not know if and how computerised tools can support information security managers in identifying risks and vulnerabilities, construction, implementation and monitoring of ISP as well as in the analysis of ISP compliance. This lead us to suggest areas for future research. It would be interesting to study how methods and models suggested in research on manual support could be used as starting points for the development of computerised support. It would also be interesting to study which ISP management phase(s) would gain the most benefits from using computerised support and how efficient such support would be for information security managers.

5.2 The extent to which the interaction between phases has been acknowledged

Although a couple of researchers (Tuyikeze and Pottas, 2011; Tuyikeze and Flowerday, 2014; Knapp *et al.*, 2009; Rees *et al.*, 2003) have emphasised the importance of considering the entire process of managing ISP, our analysis shows that the current research focuses mostly on a single ISP management phase. Compliance studies dominate this latter kind of research, which may indicate that existing research treats compliance as a separate area in ISP management. This research does not explore how other phases, such as policy construction or policy implementation may influence compliance and non-compliance. Lack of knowledge on how policy compliance interacts with other phases of ISP management leaves information security managers with limited understanding of how ISPs can be adjusted, modified and updated based on analysis of compliance and non-compliance. Hence, more research within this area is needed.

Furthermore, our analysis shows that the number of studies decreases when the number of addressed phases increases (see Figure 2), indicating that the complexity of the entire ISP management process is not addressed in current research. Taken together, the acknowledged interaction between ISP management phases in research on both manual and computerised support is generally low, which has implications for both research and practice. From a research point of view, more research on the interactions between the ISP management phases is needed to support the iterative nature of the process, i.e. to ensure efficient maintenance and updating of ISP based on input from the other phases. As of now, this limited understanding prevents researchers from uncovering new and valuable insights and providing advice to practitioners. From a practical point of view, the lack of models, methods and tools relating to the entire ISP management process leaves information security managers with fragmented support for this process.

As stated in the Introduction, computerised tools have successfully been used in other information system disciplines to support complex processes. Therefore, we believe that computerised support has the potential to aid in the ISP management process and reduce its complexity by helping information security managers to govern the interaction between the different phases. Yet again, the lack of research on computerised support for ISP management becomes a considerable limitation of current research. Here, several important future research opportunities materialise. It is important to understand how ISP management phases interact with each other; i.e. what should be input and output from each phase, for computerised support to be effective in work involving such interaction. It would also be interesting to investigate how and to what extent computerised support could be provided for the entire ISP management process and the interaction between its various phases. Having computerised support in place would also provide opportunities for studying the effects of such support.

5.3 Dominant research methods

Our review provides details on what research methods have been used in research on manual and computerised support for ISP management. We have shown how the research methods were distributed between the ISP management phases (see Figure 4) and also distributed between studies acknowledging different levels of interaction between these phases (see Figure 5). These findings extend the existing knowledge base, as none of the previous literature reviews explicitly discussed research methods used in research on ISP management (Tuyikeze and Flowerday, 2014; Järveläinen, 2016; Cram *et al.*, 2018). Cram *et al.* (2018) compiled the research methods used in the reviewed studies; however, it is unclear what analytical framework was used for this categorisation.

In the current review, the research methods were analysed using an extended version of Mingers' (2003a) framework (see Section 3). Similarly to Cram *et al.* (2018), we found that ISP management research is to a large extent based on survey methods (66 out of 123 studies). This is mainly because most ISP management research has addressed compliance, where survey seems to be the preferred research method. Our analysis further shows that although 14 types of research methods have been used, only four of them (survey, interview, no method, and case study) were used extensively. The large share of studies (26 out of 123) with no explicitly described research method surprised us, in spite of Cram *et al.* (2018) showing a similar pattern.

As shown in Figure 4, studies with no method were mainly found in the construction and implementation phases. From a research point of view it is worth noting that not explicitly describing the research method makes it problematic to assess the research results and decreases the studies' reliability. Thus, we can conclude that researchers in the area of ISP management could be more explicit in their use of research methods. From a practical point of view, studies that do not explicitly describe used research method(s) may be experienced as abstract and consequently provide limited guidance for practitioners; for example, concerning policy construction.

Mingers (2003a) argues that research methods belong to certain paradigms, even if some of the methods can be used in several paradigms. According to Mingers (2003a), a paradigm refers to "the general orientation of a research method and its basic assumptions". Thus, given the skewed frequency of the research methods used in ISP management research we can conclude that only a limited number of perspectives have been addressed in this area. Mingers (2003a) classifies research methods into positivist, interpretive, and intervention oriented; these methods are related to different research outcomes: prediction, understanding and change. We did not find any studies that used critical theory and only a few studies that used action research, design science or consultancy (see Figure 4). All these methods are categorised by Mingers as methods involving interventions which "inherently involve bringing about change to the research situation" (Mingers, 2003a). The fact that none of the studies on computerised support used design research or action research is surprising since these two methods are considered to be supportive in designing artefacts.

These findings have implications for both research and practice. From a research point of view, a broader use of research methods would help approach ISP management problems from several perspectives and offer different types of research outcomes. From a practical point of view, the Introduction shows a need for improvement (bringing about change) of the complex ISP management process; thus more intervention studies applying research methods such as action research and design science are needed. In particular, these methods become crucial if we are to increase research on computerised support for ISP management.

5.4 The limitation of the study

In this study, we have reported on the extent to which researchers have suggested manual and computerised support of ISP management, and the research methods used in such research. Naturally, the findings rely on our search strategy and on our selection of papers. We have been explicit about our selection of papers, which is based on searches in the Scopus and Web of Science databases. Of course, other search strategies would have been possible, such as the one used by Cram *et al.* (2018). Thus, we do not claim that we have identified all studies on ISP management; rather, we have used a sample of good size from the relevant outlets.

The use of our analytical framework involved subjective judgment. It was not always an instrumental task to classify papers into different phases or types of research methods. However, our initial triangulation of the classifications, based on the authors' individual analyses, strengthens our findings. Furthermore, we have tried to make our procedures as explicit and transparent as possible by providing a complete account of our searches and classifications of papers in Appendices 1–6, making it possible to scrutinise the work in detail.

6. Conclusion

The aim of this paper was to survey existing information security policy (ISP) management research to scrutinise the extent to which manual and computerised support have been suggested, and the ways in which the suggested support have been brought about. To this end we used the ISP management process framework proposed by Flowerday and Tuyikeze (2016) together with an extended version of Mingers' (2003a) research method framework. We can conclude that the existing research focuses mainly on manual support for ISP management. Computerised support has received very little attention.

The majority of papers on manual support address a single ISP management phase and there are few studies that deal with the entire complexity of the ISP management process. Policy compliance is the phase that has received the most attention; however, it has mostly been studied in isolation. When it comes to research on computerised support, we were unable to identify any patterns in terms of how researchers have addressed the interaction between ISP management phases. This was due to the limited number of papers that have been written on computerised support. With regard to research methods, only a small repertoire of research methods has been used extensively. The majority of the studies used survey, interview, and case study. In a considerable number of papers, no research method was accounted for. Furthermore, it is interesting that we found few studies that employed action research and design science, i.e. targeting intervention and change. This is especially surprising given that supporting ISP management is about providing practical advice and artefacts. Taken together this makes it difficult for practitioners to assess the practical usefulness of many of these recommendations and artefacts.

Our findings suggest that future research on ISP management should:

- to a larger extent address the interaction between ISP management phases, i.e. addressing the complexity of the entire ISP management process; this applies to research on both manual and computerised support for ISP management;
- apply more intervention research to develop computerised support for ISP management, i.e. studies that use design science and action research as research methods. Intervention research would help in assessing the practical usefulness of such support; this recommendation should not be interpreted as meaning that other research methods are not useful; in many cases, they are useful in different steps of design science and action research studies. For example, surveys and interviews can be used during the evaluation of suggested artefacts; and
- investigate to what extent computerised support can enhance the integration of different ISP management phases and reduce the complexity of such a process; as so few studies have been carried out on computerised support it is very much unknown to what extent and in what way this type of support can ease the burden of information security managers when working with ISP management.

References

Abdelwahed, A.S., Mahmoud, A.Y. and Bdair, R.A. (2016), "Information security policies and their relationship with the effectiveness of the management information systems of major Palestinian universities in the Gaza Strip", *International Journal of Information Science and Management (IJISM)*, Vol. 15 No. 1.

Abed, J., Dhillon, G. and Ozkan, S. (2016), *Investigating Continuous Security Compliance Behavior: Insights from Information Systems Continuance Model*, AIS Electronic Library (AISeL).

Abraham, S. and Chengalur-Smith, I.N. (2011), *The Role of Conflict Resolution in Designing and Implementing Information Security Policies: An Institutional Perspective*, AMCIS.

Adams, A. and Sasse, M.A. (1999), "Users are not the enemy", *Communication of the ACM*, Vol. 42, pp. 41-45.

Albors, J. (2016), "Application not compatible': Bayrob may be stealing your info [online]", welivesecurity: ESET, available at: www.welivesecurity.com/2016/01/28/application-not-compatible-bayrob-may-be-stealing-your-info/ (accessed 1 May 2018).

Al-Hamdani, W.A. and Dixie, W.D. (2009), "Information security policy in small education organization", *2009 Information Security Curriculum Development Conference*, *ACM*, *New York, NY*.

Al-Izki, F. and Weir, G.R.S. (2016), "Management attitudes toward information security in Omani public sector organisations", *2016 Cybersecurity and Cyberforensics Conference (CCC)*, *IEEE*, *Piscataway, NJ*.

Al-Mukahal, H.M. and Alshare, K. (2015), "An examination of factors that influence the number of information security policy violations in Qatari organizations", *Information and Computer Security*, Vol. 23 No. 1, pp. 102-118.

Almusharraf, A., Dhillon, G. and Samonas, S. (2015), *Mismatched Understanding of is Security Policy: A Repgrid Analysis*, AIS Electronic Library (AISeL).

Alotaibi, M., Furnell, S. and Clarke, N. (2016), "Information security policies: a review of challenges and influencing factors", *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, *IEEE*, *Piscataway, NJ*.

Arif, M. (2011), "What matters most among human factors to comply with organisations information security policy", *International symposium on Human aspects of information security and assurance (HAISA 2011), HAISA*.

Asai, T. and Hakizabera, A.U. (2010), "Human-related problems of information security in East African cross-cultural environments", *Information Management and Computer Security*, Vol. 18, pp. 328-338.

Aurigemma, S. and Mattson, T. (2014), "Do it or ELSE! Exploring the effectiveness of deterrence on employee compliance with information security policies".

Aurigemma, S. and Mattson, T. (2017a), "Privilege or procedure: evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls", *Computers and Security*, Vol. 66, pp. 218-234.

Aurigemma, S. and Mattson, T. (2017b), "Deterrence and punishment experience impacts on ISP compliance attitudes", *Information and Computer Security*.

Balozian, P.Y. and Leidner, D. (2016), *Is Security Menace: When Security Creates Insecurity*, AIS Electronic Library (AISeL).

Baskerville, R. and Siponen, M. (2002), "An information security meta-policy for emergent organizations", *Logistics Information Management*, Vol. 15 Nos 5/6, pp. 337-346.

Bauer, S. and Bernroider, E.W. (2017), "From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization", *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, Vol. 48 No. 3, pp. 44-68.

Bauer, S., Bernroider, E.W.N. and Chudzikowski, K. (2017), "Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks", *Computers and Security*, Vol. 68, pp. 145-159.

Bernik, I. (2016), "Compliance with information security policies in the slovene insurance sector", *ECCWS2016-Proceedings fo the 15th European Conference on Cyber Warfare and Security Academic Conferences and publishing*, p. 28.

Bhardwaj, A., Subrahmanyam, G.V.B., Avasthi, V. and Sastry, H. (2016), "Design a resilient network infrastructure security policy framework", *Indian Journal of Science and Technology*, Vol. 9 No. 19.

Brewer, J. and Hunter, A. (1989), "The multimethod approach and its promise", *Multimethod Research: A Synthesis of Styles*, Vol. 175, pp. 13-28.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2009a), "Roles of information security awareness and perceived fairness in information security policy compliance", *AMCIS 2009 Proceedings, AMCIS*, p. 419.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2009b), "Effects of individual and organization based beliefs and the moderating role of work experience on insiders' good security behaviors", *2009 International Conference on Computational Science and Engineering*, *IEEE*, *Piscataway, NJ*, pp. 476-481.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523-548.

Busch, M., Patil, S., Regal, G., Hochleitner, C. and Tscheligi, M. (2016), "Persuasive information security: techniques to help employees protect organizational information security", *International Conference on Persuasive Technology*, *Springer*, *Cham*, pp. 339-351.

Buthelezi, M.P., Van Der Poll, J.A. and Ochola, E.O. (2016), "Ambiguity as a barrier to information security policy compliance: a content analysis", *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, *IEEE*, *Piscataway, NJ*.

Caniëls, M.C.J. and Bakens, R.J.J.M. (2012), "The effects of project management information systems on decision making in a multi project environment", *International Journal of Project Management*, Vol. 30 No. 2, pp. 162-175.

Chen, Y., Ramamurthy, K. and Wen, K.-W. (2012), "Organizations' information security policy compliance: stick or carrot approach?", *Journal of Management Information Systems*, Vol. 29 No. 3, pp. 157-188.

Cheng, L., Li, Y., Li, W., Holm, E. and Zhai, Q. (2013), "Understanding the violation of is security policy in organizations: an integrated model based on social control and deterrence theory", *Computers and Security*, Vol. 39, pp. 447-459.

Cherdantseva, Y. and Hilton, J. (2013), "A reference model of information assurance and security", *2013 International Conference on Availability, Reliability and Security*, *IEEE*, *Piscataway, NJ*.

Cheung, S.K.S. (2014), "Information security management for higher education institutions", *Intelligent Data Analysis and Its Applications*, Vol. 1.

Choi, M. (2016), "Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing", *Sustainability*, Vol. 8 No. 7.

Coertze, J. and Von Solms, R. (2013), "A software gateway to affordable and effective information security governance in SMMEs", *2013 Information Security for South Africa*, *IEEE*, *Piscataway, NJ*, pp. 1-8.

Coertze, J., Van Niekerk, J. and Von Solms, R. (2011), "A web-based information security management toolbox for small-to-medium enterprises in Southern Africa", *2011 Information Security for South Africa*, *IEEE*, *Piscataway, NJ*.

Corpuz, M. (2011a), "Enterprise information security policy assessment: an extended framework for metrics development utilising the goal-question-metric approach", *Proceedings of the 15th World Multi-Conference on Systemics*, Cybernetics and Informatics. *International Institute of Informatics and Systemics (IIIS)*.

Corpuz, M. (2011b), "The enterprise information security policy as a strategic business policy within the corporate strategic plan", *Proceedings of the 15th World Multi-Conference on Systemics*, Cybernetics and Informatics. *International Institute of Informatics and Systemics (IIIS)*.

Corpuz, M. and Barnes, P.H. (2010), "Integrating information security policy management with corporate risk management for strategic alignment", *Proceedings of the 14th World Multi-Conference on Systemics*, *Cybernetics and Informatics (WMSCI 2010)*.

Cosic, Z. and Boban, M. (2010), "Information security management – defining approaches to information security policies in ISMS", *IEEE 8th International Symposium on Intelligent Systems and Informatics*, *IEEE*, *Piscataway, NJ*.

Cram, W.A., Proudfoot, J.G. and D'arcy, J. (2018), "Organizational information security policies: a review and research framework", *European Journal of Information Systems*, Vol. 26 No. 6, pp. 605-641.

Creswell, J.W. (2003), *A Framework for Design. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, SAGE, pp. 9-11.

D'arcy, J. and Herath, T. (2011), "A review and analysis of deterrence theory in the is security literature: making sense of the disparate findings", *European Journal of Information Systems*, Vol. 20 No. 6, pp. 643-658.

D'arcy, J., Herath, T. and Shoss, M.K. (2014), "Understanding employee responses to stressful information security requirements: a coping perspective", *Journal of Management Information Systems*, Vol. 31, pp. 285-318.

Dinev, T., Goo, J., Hu, Q. and Nam, K. (2009), "User behaviour towards protective information technologies: the role of national cultural differences", *Information Systems Journal*, Vol. 19 No. 4, pp. 391-412.

Doherty, N.F. and Fulford, H. (2006), "Aligning the information security policy with the strategic information systems plan", *Computers and Security*, Vol. 25 No. 1, pp. 55-63.

Doherty, N.F., Anastasakis, L. and Fulford, H. (2009), "The information security policy unpacked: a critical study of the content of university policies", *International Journal of Information Management*, Vol. 29 No. 6, pp. 449-457.

Dwivedi, Y.K. and Kuljis, J. (2008), "Profile of is research published in the European journal of information systems", *European Journal of Information Systems*, Vol. 17 No. 6, pp. 678-693.

Efendioglu, N., Woitsch, R. and Utz, W. (2016), "A toolbox supporting agile modelling method engineering: ADOxx. org modelling method conceptualization environment", *IFIP Working Conference on The Practice of Enterprise Modeling*, *Springer*, *Cham*, pp. 317-325.

Enisa (2014), *ENISA Threat Landscape 2014. Overview of Current and Emerging Cyber-Threats*, European Union Agency for Network and Information Security.

Ernst and Young (2008), "Ernst and Young 2008 Global Information Security Survey", Ernst and Young.

Ernst and Young (2010), "Borderless security – Ernst and Young's 2010 Global Information Security Survey", Ernst and Young.

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

Fragos, C., Karyda, M. and Kiountouzis, E. (2007), "Using the lens of circuits of power in information systems security management", *International Conference on Trust, Privacy and Security in Digital Business*, Springer, Berlin, Heidelberg.

Franke, U. and Brynielsson, J. (2014), "Cyber situational awareness – a systematic review of the literature", *Computers and Security*, Vol. 46, pp. 18-31.

Fulford, H. and Doherty, N.F. (2003), "The application of information security policies in large UK-based organizations: an exploratory investigation", *Information Management and Computer Security*, Vol. 11, pp. 106-114.

Gadzama, W.A., Katuka, J.I., Gambo, Y., Abali, A.M. and Usman, M.J. (2014), "Evaluation of employees awareness and usage of information security policy in organizations of developing countrties: a study of federal inland revenue service, Nigeria", *Journal of Theoretical and Applied Information Technology*, Vol. 67 No. 2.

Gaigole, M. and Khere, N. (2012), "Web-base group decision support system for information security decision making in case of Indian E-Government systems", *Advanced Materials Research*, Vol. 403, pp. 954-962.

Galliers, R.F. (1992), *Information systems research: issues, methods and practical guidelines. Blackwell scientific*.

Gara (2015), "Morgan stanley fires rogue employee after customer data leak [online]", Forbes, available at: www.forbes.com/sites/civicnation/2018/04/26/five-numbers-that-show-the-impact-free-college-can-have/#2ac2d9f27d01 (accessed 1 May 2018).

Gaunt, N. (1998), "Installing an appropriate information security policy", *International Journal of Medical Informatics*, Vol. 49 No. 1, pp. 131-134.

Gerber, N., Mcdermott, R., Volkamer, M. and Vogt, J. (2016), *Understanding Information Security Compliance-Why Goal Setting and Rewards Might Be a Bad Idea*, *HAISA*.

Ghazvini, A. and Shukur, Z. (2016), "Awareness training transfer and information security content development for healthcare industry", *International Journal of Advanced Computer Science and Applications)*, Vol. 7 No. 5.

Ghazvini, A. and Shukur, Z. (2017), "Information security content development for awareness training programs in healthcare", *International Journal of Security and Its Applications*, Vol. 11 No. 7, pp. 875-896.

Gregor, S. and Jones, D. (2007), "The anatomy of a design theory", *Journal of the Association for Information Systems*, Vol. 8, pp. 312-335.

Gritzalis, D. (1997), "A baseline security policy for distributed healthcare information systems", *Computers and Security*, Vol. 16 No. 8, pp. 709-719.

Guo, K.H. (2013), "Security-related behavior in using information systems in the workplace: a review and synthesis", *Computers and Security*, Vol. 32, pp. 242-251.

Guo, K.H. and Yuan, Y. (2012), "The effects of multilevel sanctions on information security violations: a mediating model", *Information and Management*, Vol. 49, pp. 320-326.

Harmsen, A.F. (1997), "Situational method engineering", Doctorial Dissertation, University of Twente.

Hedström, K., Karlsson, F. and Kolkowska, E. (2013), "Social action theory for understanding information security non-compliance in hospitals", *Information Management and Computer Security*, Vol. 21, pp. 266-287.

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

Herath, T. and Rao, H.R. (2009), "Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Vol. 47 No. 2, pp. 154-165.

Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004), "Design science in information systems research", *MIS Quarterly*, Vol. 28, pp. 75-105.

Höne, K. and Eloff, J.H.P. (2002a), "Information security policy – what do international information security standards say?", *Computers and Security*, Vol. 21 No. 5, pp. 402-409.

Höne, K. and Eloff, J.H.P. (2002b), "What makes an effective information security policy?", *Network Security*, Vol. 2002 No. 6, pp. 14-16.

Hong, K.S., Chi, Y.P., Chao, L.R. and Tang, J.H. (2006), "An empirical study of information security policy on information security elevation in Taiwan", *Information Management and Computer Security*, Vol. 14, pp. 104-115.

Hoppe, O.A., Van Niekerk, J. and Von Solms, R. (2002), "The effective implementation of information security in organizations", *Security in the Information Society*, Springer, Boston, MA, pp. 1-18.

Hou, Y., Gao, P. and Heeks, R. (2011), *The Influence of Institutional Forces on Employee Compliance with Information Security Policies*, WOSIS.

Howard, P.D. (2007), "The security policy life cycle: functions and responsibilities", in Tipon, H.F. and Krause, M. (Eds), *Information Security Managemeng Handbook*, Auerback Publications, Boca Raton, pp. 377-388.

Hsu, J.S.-C., Shih, S.-P., Hung, Y.W. and Lowry, P.B. (2015), "The role of extra-role behaviors and social controls in information security policy effectiveness", *Information Systems Research*, Vol. 26 No. 2, pp. 282-300.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012), "Managing employee compliance with information security policies: the critical role of top management and organizational culture", *Decision Sciences*, Vol. 43 No. 4, pp. 615-660.

Huang, H.W., Parolia, N. and Cheng, K.T. (2016), *Willingness and Ability to Perform Information Security Compliance Behavior: Psychological Ownership and Self-Efficacy Perspective*, PACIS.

Humaidi, N. and Balakrishnan, V. (2015a), "The moderating effect of working experience on health information system security policies compliance behaviour", *Malaysian Journal of Computer Science*, Vol. 28 No. 2, pp. 70-92.

Humaidi, N. and Balakrishnan, V. (2015b), "Leadership styles and information security compliance behavior: the mediator effect of information security awareness", *International Journal of Information and Education Technology*, Vol. 5 No. 4, p. 311.

Ifinedo, P. (2012), "Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory", *Computers and Security*, Vol. 31, pp. 83-95.

Ifinedo, P. (2014), "Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition", *Information and Management*, Vol. 51, pp. 69-79.

Ifinedo, P. (2016), "Critical times for organizations: what should be done to curb workers' noncompliance with is security policy guidelines?", *Information Systems Management*, Vol. 33 No. 1, pp. 30-41.

Ismail, W.H.B.W. and Widyarto, S.A. (2016), "Formulation and development process of information security policy in higher education", Paper presented at the 1st International Conference on Engineering Technology and Applied Sciences, Afyonkarahisar.

Ismail, Z., Masrom, M., Sidek, Z. and Hamzah, D. (2010), "Examining information security concerns: case study of malaysian academic setting", *14th International-Business-Information-Management-Association Conference*, *Istanbul*.

Jaafari, A. and Manivong, K. (1998), "Towards a smart project management information system", *International Journal of Project Management*, Vol. 16 No. 4, pp. 249-265.

Järveläinen, J. (2016), "Integrated business continuity planning and information security policy development approach".

Johnston, A.C., Warkentin, M. and Siponen, M. (2015), "An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric", *MIS Quarterly*, Vol. 39 No. 1, pp. 113-134.

Johnston, A.C., Wech, B. and Jack, E. (2013), "Engaging remote employees: the moderating role of 'remote' status in determining employee information security policy awareness", *Journal of Organizational and End User Computing (Computing)*, Vol. 25 No. 1, pp. 1-23.

Johnston, A.C., Warkentin, M., Mcbride, M. and Carter, L. (2016), "Dispositional and situational factors: influences on information security policy violations", *European Journal of Information Systems*, Vol. 25 No. 3, pp. 231-251.

Jürjens, J. and Shabalin, P. (2007), "Tools for secure systems development with UML", *International Journal on Software Tools for Technology Transfer*, Vol. 9 Nos 5/6, pp. 527-544.

Kabay, M. (1994), "Psychosocial factors in the implementation of information security policy", *EDPACS*, Vol. 21 No. 10, pp. 1-10.

Kadam, A.W. (2007), "Information security policy development and implementation", *Information Systems Security*, Vol. 16 No. 5, pp. 246-256.

Kadir, M.R.A., Norman, S.N.S., Rahman, S.A., Ahmad, A.R. and Bunawan, A.A. (2016), "Innovation management, development sustainability, and competitive economic growth information security policies compliance among employees in cybersecurity Malaysia", *28th International Business Information Management Association Conference-Vision 2020*, *International Business Information Management Association, IBIMA*.

Kajtazi, M. and Bulgurcu, B. (2013), "Information security policy compliance: an empirical study on escalation of commitment, an empirical study on escalation of commitment".

Karlsson, F. and Ågerfalk, P.J. (2012), "MC sandbox: devising a tool for method-user-centered method configuration", *Information and Software Technology*, Vol. 54 No. 5, pp. 501-516.

Karlsson, F., Åström, J. and Karlsson, M. (2015), "Information security culture–state-of-the-art review between 2000 and 2013", *Information and Computer Security*, Vol. 23 No. 3, pp. 246-285.

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

Karyda, M., Kokolakis, S. and Kiountouzis, E. (2003), "Content, context, process analysis of is security policy formation", *IFIP International Information Security Conference Springer*, *Boston, MA*.

Karyda, M., Kiountouzis, E. and Kokolakis, S. (2005), "Information systems security policies: a contextual perspective", *Computers and Security*, Vol. 24, pp. 246-260.

Kelion, L. (2013), "Cryptolocker ransomware has'infected about 250,000 PCs' [online]", BBC, available at: www.bbc.com/news/technology-25506020 (accessed 1 May 2018).

Kim, S.H., Yang, K.H. and Park, S. (2014), "An integrative behavioral model of information security policy compliance", *The Scientific World Journal*, Vol. 2014, pp. 1-12.

Knapp, K.J., Franklin Morris, R., Marshall, T.E. and Byrd, T.A. (2009), "Information security policy: an organizational-level process model", *Computers and Security*, Vol. 28, pp. 493-508.

Kolkowska, E. and De Decker, B. (2012), "Analyzing value conflicts for a work-friendly ISS policy implementation", *FIP International Information Security Conference*, *Springer*, *Berlin, Heidelberg*.

Kolkowska, E., Karlsson, F. and Hedström, K. (2017), "Towards analysing the rationale of information security non-compliance: devising a value-based compliance analysis method", *The Journal of Strategic Information Systems*, Vol. 26 No. 1, pp. 39-57.

Koziel, G. (2011), "Information security policy creating", *Actual Problems of Economics*, Vol. 12, p. 126.

Kretzer, M. and Mädche, A. (2015), "Which are the most effective measures for improving employees' security compliance?".

Kurtel, K. (2008), "Information security policy: positioning the technological components of information security services under the perspective of electronic business", *Security of Information and Networks: Proceedings of the First International Conference on Security of Information and Networks (SIN 2007)*, *Trafford Publishing*.

Kyobe, M. (2010), "Towards a framework to guide compliance with is security policies and regulations in a university", *2010 Information Security for South Africa, IEEE*.

Lapke, M. and Dhillon, G. (2015), "Disassociations in security policy lifecycles", *International Journal of Information Security and Privacy*, Vol. 9 No. 1, pp. 62-77.

Lebek, B., Uffen, J., Breitner, M.H., Neumann, M. and Hohler, B. (2013), "Employees' information security awareness and behavior: a literature review", *2013 46th HI International Conference on System Sciences*, *IEEE*, *Piscataway, NJ*, pp. 2978-2987.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. and H. Breitner, M. (2014), "Information security awareness and behavior: a theory-based literature review", *Management Research Review*, Vol. 37 No. 12, pp. 1049-1092.

Lee, C.K., Park, G.Y., Kwon, K.C., Hahn, D.H. and Cho, S.H. (2009), "Cyber security design requirements based on a risk assessment", *Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies*, pp. 1638-1646.

Levy, Y. and Ellis, T.J. (2006), "A systems approach to conduct an effective literature review in support of information systems research", *Informing Science*, Vol. 9.

Lindup, K.R. (1995), "A new model for information security policies", *Computers and Security*, Vol. 14 No. 8, pp. 691-695.

Lopes, I. and Oliveira, P. (2015a), "Implementation of information systems security policies: a survey in small and medium sized enterprises", *New Contributions in Information Systems and Technologies*, Springer, Cham.

Lopes, I.M. and Oliveira, P. (2015b), "Evaluation of the adoption of an information systems security policy", *2015 10th Iberian Conference on Information Systems and Technologies (CISTI)*, *IEEE*, *Piscataway, NJ*.

Lopes, I. and Oliveira, P. (2015c), "Applying action research in the formulation of information security policies", *New Contributions in Information Systems and Technologies*, Springer, Cham.

Lopes, I. and Oliveira, P. (2016), "The security policy application process: action research", *New Advances in Information Systems and Technologies*, Springer, Cham, pp. 353-362.

Lowry, P.B. and Moody, G.D. (2015), "Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies", *Information Systems Journal*, Vol. 25 No. 5, pp. 433-463.

Mader, A. and Srinivasan, S. (2005), "Curriculum development related to information security policies and procedures", *Proceedings of the 2nd annual conference on Information security curriculum development*, *ACM*, *New York, NY*.

Mavetera, N., Moroke, N.D. and Sebetlele, A. (2015), "An empirical study of staff compliance to information security policy in a South African municipality", *Corporate Ownership and Control*, Vol. 13 No. 1.

Maynard, S.B. Ruighaver, A.B. and Ahmad, A. (2011), "Stakeholders in security policy development".

Merhi, M. and Ahluwalia, P. (2015), "Top management can lower resistance toward information security compliance".

Mingers, J. (2003a), "The paucity of multimethod research: a review of the information systems literature", *Information Systems Journal*, Vol. 13 No. 3, pp. 233-249.

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

Nash, K.S. and and Greenwood, D. (2008), "The global state of information security", CIO Magazine (reprinted by PriceWaterhouseCoopers).

Niemimaa, E. (2016), "Crafting an information security policy: insights from an ethnographic study".

Niemimaa, E. and Niemimaa, M. (2017), "Information systems security policy implementation in practice: from best practices to situated practices", *European Journal of Information Systems*, Vol. 26 No. 1, pp. 1-20.

Nowicki, A. Artur, R.O.T. and Szymanski, J. (2006), "The information system security management in the polish banking institutions", Case Study.

Orlikowski, W.J. (1993), "CASE tools as organizational change: investigating incremental and radical changes in systems development", *MIS Quarterly*, Vol. 17 No. 3, pp. 309-340.

Pahnila, S., Karjalainen, M. and Siponen, M.T. (2013), *Information Security Behavior: Towards Multi-Stage Models*, PACIS, p. 102.

Palmer, D. (2017), "Locky ransomware: why this menace keeps coming back. ZDNet: CBS interactive", available at: www.zdnet.com/article/locky-ransomware-why-this-menace-keeps-coming-back/ (accessed 1 May 2018).

Palmer, M.E., Robinson, C., Patilla, J.C. and Moser, E.P. (2001), "Information security policy framework: best practices for security policy in the E-commerce age", *Information Systems Security*, Vol. 10 No. 2, pp. 1-15.

Palvia, P., Leary, D., Mao, E., Midha, V., Pinjani, P. and Salam, A.F. (2004), "Research methodologies in MIS: an update", *Communications of the Association for Information Systems*, Vol. 14 No. 1, p. 58.

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

Pavlidis, M., Islam, S. and Mouratidis, H. (2011), "A CASE tool to support automated modelling and analysis of security requirements, based on secure tropos", *International Conference on Advanced Information Systems Engineering*, *Springer*, *Berlin, Heidelberg*, pp. 95-109.

Peltier, T.R. (2004), *Information Security Policies and Procedures – a Practitioner's Reference*, Auerbach publications, Boca Raton.

PWC (2014), "Managing cyber risks in an interconnected world - key findings from The Global State of Information Security Survey 2015", PriceWaterhouseCoopers.

Raymond, L. and Bergeron, F. (2008), "Project management information systems: an empirical study of their impact on project managers and project success", *International Journal of Project Management*, Vol. 26 No. 2, pp. 213-220.

Rees, J. and Allen, J. (2008), "The state of risk assessment practices in information security: an exploratory investigation", *Journal of Organizational Computing and Electronic Commerce*, Vol. 18 No. 4, pp. 255-277.

Rees, J., Bandyopadhyay, S. and Spafford, E.H. (2003), "A policy framework for information security", *Communications of the Acm*, Vol. 46 No. 7, pp. 101-106.

Reichard, A., Quirchmayr, G. and Wills, C.C. (2011), *Challenges in Implementing Information Security Policies*, HAISA, pp. 22-34.

Renaud, K. and Goucher, W. (2012), "Health service employees and information security policies: an uneasy partnership?", *Information Management and Computer Security*, Vol. 20, pp. 296-311.

Rossi, M., Ramesh, B., Lyytinen, K. and Tolvanen, J.P. (2004), "Managing evolutionary method engineering by method rationale", *The Association for Information Systems*, Vol. 5 No. 9, p. 12.

Sannicolas-Rocca, T., Schooley, B. and Spears, J.L. (2014), "Designing effective knowledge transfer practices to improve is security awareness and compliance", *2014 47th HI International Conference on System Sciences*, *IEEE*, *Piscataway, NJ*.

Saran, M. and Zavarsky, P. (2009), "A study of the methods for improving internet usage policy compliance", *2009 International Conference on Computational Science and Engineering*, *IEEE*, *Piscataway, NJ*.

Sharifa, H. Ismailb, Z. and Masromc, M. (2009), "Users' perception on the information security policy of the institutions of higher learning".

Shih, H.P., Guo, X., Lai, K.H. and Cheng, T.C.E. (2016), "Taking promotion and prevention mechanisms matter for information systems security policy in Chinese SMEs", *2016 2nd International Conference on Information Management (ICIM)*, *IEEE*, *Piscataway, NJ*.

Simms, D.J. (2009), "Information security optimization: from theory to practice", *2009 International Conference on Availability, Reliability and Security*, *IEEE*, *Piscataway, NJ*.

Siponen, M.T. and Iivari, J. (2006), "Six design theories for is security policies and guidelines", *Journal of the Association for Information Systems*, Vol. 7 No. 7, p. 19.

Siponen, M. and Vance, A. (2014), "Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations", *European Journal of Information Systems*, Vol. 23 No. 3, pp. 289-305.

Siponen, M.T. and Oinas-Kukkonen, H. (2007), "A review of information security issues and respective research contributions", *ACM SIGMIS Database*, Vol. 38 No. 1, pp. 60-80.

Siponen, M., Adam Mahmood, M. and Pahnila, S. (2014), "Employees' adherence to information security policies: an exploratory field study", *Information and Management*, Vol. 51, pp. 217-224.

Siponen, M., Mahmood, M.A. and Pahnila, S. (2009), "Technical opinionAre employees putting your company at risk by not following information security policies?", *Communications of the Acm*, Vol. 52 No. 12.

Siponen, M., Pahnila, S. and Mahmood, A.M. (2006), "A new model for understanding users' is security compliance", *PACIS 2006 Proceedings, PACIS*, p. 48.

Siponen, M., Willison, R. and Baskerville, R. (2008), "Power and practice in information systems security research", *ICIS 2008 Proceedings, ICIS*, p. 26.

Sohrabi Safa, N., Von Solms, R. and Furnell, S. (2016), "Information security policy compliance model in organizations", *Computers and Security*, Vol. 56, pp. 70-82.

Sommestad, T., Karlzén, H. and Hallberg, J. (2015), "The sufficiency of the theory of planned behavior for explaining information security policy compliance", *Information and Computer Security*, Vol. 23 No. 2, pp. 200-217.

Sommestad, T., Hallberg, J., Lundholm, K. and Bengtsson, J. (2014), "Variables influencing information security policy compliance: a systematic review of quantitative studies", *Information Management and Computer Security*, Vol. 22 No. 1, pp. 42-75.

Son, J.-Y. (2011), "Out of fear or desire? Toward a better understanding of employees' motivation to follow is security policies", *Information and Management*, Vol. 48, pp. 296-302.

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016), "Information security management needs more holistic approach: a literature review", *International Journal of Information Management*, Vol. 36 No. 2, pp. 215-225.

Stahl, B.C., Doherty, N.F. and Shaw, M. (2012), "Information security policies in the UK healthcare sector: a critical evaluation", *Information Systems Journal*, Vol. 22 No. 1, pp. 77-94.

Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005), "Analysis of end user security behaviors", *Computers and Security*, Vol. 24, pp. 124-133.

Straub, D.W., Jr,. and Nance, W.D. (1990), "Discovering and disciplining computer abuse in organizations: a field study", *MIS Quarterly*, Vol. 14 No. 1, pp. 45-60.

Subramanian, V., Seker, R., Bian, J. and Kanaskar, N. (2011), "Collaborations, mergers, acquisitions, and security policy conflict analysis", *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research*, *ACM*, *New York, NY*.

Superdome, H.I.D. (2014), "27th international conference on computer applications in industry and engineering (CAINE-2014)".

Syamsuddin, I. and Hwang, J. (2010), "The use of AHP in security policy decision making: an open office calc application", *Journal of Software*, Vol. 5 No. 10.

Talbot, S. and Woodward, A. (2009), "Improving an organisations existing information technology policy to increase security".

Teixeira, L., Xambre, A.R., Figueiredo, J. and Alvelos, H. (2016), "Analysis and design of a project management information system: practical case in a consulting company", *Procedia Computer Science*, Vol. 100, pp. 171-178.

Tsohou, A., Karyda, M. and Kokolakis, S. (2015), "Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs", *Computers and Security*, Vol. 52, pp. 128-141.

Tuyikeze, T. and Flowerday, S. (2014), *Information Security Policy Development and Implementation: A Content Analysis Approach*, HAISA.

Tuyikeze, T. and Pottas, D. (2011), "An information security policy development life cycle", *Proceedings of the South African Information Security Multi-Conference (SAISMC)*, *SAISMC*, *Port Elizabeth*.

Van Niekerk, J.F. and Von Solms, R. (2010), "Information security culture: a management perspective", *Computers and Security*, Vol. 29 No. 4, pp. 476-486.

Vermeulen, C. and Von Solms, R. (2002), "The information security management toolbox – taking the pain out of security management", *Information Management and Computer Security*, Vol. 10, pp. 119-125.

Von Solms, R., Thomson, K.L. and Maninjwa, P.M. (2011), "Information security governance control through comprehensive policy architectures", *2011 Information Security for South Africa*, *IEEE*, *Piscataway, NJ*.

Vroom, C. and Von Solms, R. (2003), "Information security: auditing the behaviour of the employee", *IFIP International Information Security Conference*, *Springer*, *Boston, MA*, pp. 401-404.

Vroom, C. and Von Solms, R. (2004), "Towards information security behavioural compliance", *Computers and Security*, Vol. 23 No. 3, pp. 191-198.

Wall, J., Stahl, B.C. and Salam, A.F. (2015), *Critical Discourse Analysis as a Review Methodology: An Empirical Example*, Association for Information Systems.

Wang, X.L. and Li, W.L. (2015), "Using galois lattice to represent and analyze information security policy compliance", *Proceedings of the 5th International Asia Conference on Industrial Engineering and Management Innovation (IEMI2014)*, *Atlantis Press*, *Paris*, pp. 353-358.

Webster, J. and Watson, R.T. (2002), "Analyzing the past to prepare for the future: writing a literature review", *MIS Quarterly*, pp. 13-23.

Wiant, T.L. (2005), "Information security policy's impact on reporting security incidents", *Computers and Security*, Vol. 24, pp. 448-459.

Withman (2008), "Security policy: from design to maintenance", in Straub, D.W, Goodman, S.E. and Baskerville, R., (Eds), *Information Security: Policy, Processes, and Practices*, M. E. Sharpe, New York, NY, pp 123-151.

Yang, X., Yue, W.T. and Sia, C.L. (2011), "Cognitive elaboration on potential outcomes and its effects on employees' information security policy compliance intention – exploring the key antecedents", *Workshop on E-Business*, Springer, Berlin, Heidelberg.

Yaokumah, W., Brown, S. and Dawson, A.A. (2016), "Towards modelling the impact of security policy on compliance", *Journal of Information Technology Research (Research)*, Vol. 9 No. 2, pp. 1-16.

Yayla, A.A. (2011), *Enforcing Information Security Policies through Cultural Boundaries: A Multinational Company Approach*, ECIS.

Yusufovna, S.F. (2008), "Advanced security policy implementation for information systems", *2008 International Symposium on Ubiquitous Multimedia Computing*, *IEEE*, *Piscataway, NJ*.

Zafar, H. and Clark, J.G. (2009), "Current state of information security research in IS", *Communications of the Association for Information Systems*, Vol. 24.

Zhou, X. (2010), "The implementation of basic information security policy management framework using java", *2nd International Symposium on Electronic Business and Information System, Changsha City, SOUTH KOREA. AUSSINO ACAD PUBL HOUSE, PO BOX 893, MARRICKVILLE, NSW 2204 00000, AUSTRALIA*.

Further reading

Turkey (2019), "Int business information management Assoc-Ibima", 34 E GERMANTOWN PIKE, NO. 327, NORRISTOWN, PA 19401 USA.

Corresponding author

Elham Rostami can be contacted at: elham.rostami@oru.se

Appendix 1. Search criteria with results

Table AI shows the search queries that were used for searching in Web of Science and Scopus, and the results from our searches. For searching in the databases, a combination of search query 1 and search query 2 was used. For example, as the second row in the table shows, the result of searching "Information security policy" and "management" in Web of Science was 74 papers while in Scopus it was 173 papers.

Table AI. Combinations of search criteria that generated search results

Search query 1	Search query 2	Web of Science	Scopus
"Information system security policy"	"management"	0	25
"Information security policy"	"management"	74	173
"Information system security policy"	"development"	0	5
"Information security policy"	"development"	24	84
"Information system security policy"	"implementation"	1	16
"Information security policy"	"implementation"	30	89
"Information system security policy"	"design"	1	5
"Information security policy"	"design"	27	65
"Information system security policy"	"requirement"	1	9
"Information security policy"	"requirement"	22	77
"Information security policy"	"deployment"	5	4
"Information system security policy"	"effectiveness"	0	1
"Information security policy"	"effectiveness"	9	46
"Information system security policy"	"planning"	1	3
"Information security policy"	"planning"	19	31
"Information security instruction"	–	0	1
"Information security rule"	"management"	2	4
"Information security rule"	"development"	0	1
"Information security rule"	"implementation"	2	2
"Information security rule"	"design"	2	2
"Information security rule"	"requirement"	0	3
"Information system security guideline"	"management"	0	1
"Information security guideline"	"management"	0	13
"Information security guideline"	"development"	0	6
"Information security guideline"	"implementation"	0	7
"Information security guideline"	"design"	0	2
"Information security guideline"	"requirement"	0	9
"Information security guideline"	"planning"	0	4
"Information security guideline"	–	0	17
"Cyber security policy"	"management"	0	11
"Cyber security policy"	"development"	4	13
"Cyber security policy"	"implementation"	2	8
"Cyber security policy"	"design"	2	6
"Cyber security policy"	"requirement"	1	10
"Cyber security policy"	"effectiveness"	0	4
"Cyber security policy"	"planning"	1	3
"Cyber security rule"	"management"	0	1
"Cyber security rule"	"design"	0	1
"Cyber security rule"	"requirement"	0	1
"IS security policy"	"management"	8	13
"IS security policies"	"management"	6	12

(*continued*)

Search query 1	Search query 2	Web of Science	Scopus
"IS security policy"	"development"	3	8
"IS security policies"	"development"	2	7
"IS security policy"	"implementation"	3	5
"IS security policies"	"implementation"	0	5
"IS security policy"	"design"	4	7
"IS security policies"	"design"	4	7
"IS security policy"	"requirement"	1	3
"IS security policies"	"requirement"	0	3
"IS security policy"	"effectiveness"	3	4
"IS security policies"	"effectiveness"	2	4
"IS security policy"	"planning"	2	0
"Information security"	"automation"	100	319
"Computer security"	"automation"	17	277
"Information security management"	"decision support system"	1	10
"Information security management"	"computer software"	0	34
"Information security policy"	"computer software"	0	7
"Information security policy"	"decision support system"	1	8
"Information security policy"	"automation"	0	4
"Cyber security policy"	"automation"	1	3
Total		388	1492

Table AI.

Appendix 2. Search criteria without results

Table AII illustrates the search criteria used in Web of Science and Scopus that did not return any results. The combination of search query 1 *and* search query 2 was used in searching the databases. For example, as the second row in the table shows, the combination of "Information system security instruction" *and* "management", or "Information system security instruction" *and* "development", or "Information system security instruction" *and* "implementation", or "Information system security instruction" *and* "design", or "Information system security instruction" *and* "requirement", or "Information system security instruction" *and* "deployment", or "Information system security instruction" *and* "effectiveness", or "Information system security instruction" *and* "planning" did not return any results in Web of Science or Scopus.

Table AII. Combinations of search criteria that did not generate search results

Search query 1	Search query 2
"Information system security policy"	"deployment"
"Information system security instruction"	"management" *or* "development" *or* "implementation" *or* "design" *or* "requirement" *or* "deployment" *or* "effectiveness" *or* "planning"
"Information security instruction"	"management" *or* "development" *or* "implementation" *or* "design" *or* "requirement" *or* "deployment" *or* "effectiveness" *or* "planning"
"Information system security rule"	"management" *or* "development" *or* "implementation" *or* "design" *or* "requirement" *or* "deployment" *or* "effectiveness" *or* "planning"
"Information security rule"	"deployment" *or* "effectiveness"
"Information system security formal control"	"management" *or* "development" *or* "planning" *or* "implementation" *or* "design" *or* "requirement" *or* "deployment" *or* "effectiveness"
"Information security formal control"	"management" *or* "development" *or* "planning" *or* "implementation" *or* "design" *or* "requirement" *or* "deployment" *or* "effectiveness"
"Information security formal control"	–
"Information system security guideline"	"development" *or* "implementation" *or* "design" *or* "requirement" *or* "deployment" *or* "effectiveness" *or* "planning"
"Information security guideline"	"deployment" *or* "effectiveness"
"Cyber security policy"	"deployment"
"Cyber security instruction"	"management" *or* "development" *or* "implementation" *or* "design" *or* "requirement" *or* "deployment" *or* "effectiveness" *or* "planning"
"Cyber security rule"	"development" *or* "implementation" *or* "deployment" *or* "effectiveness" *or* "planning"
"Cyber security formal control"	"management" *or* "development" *or* "implementation" *or* "design" *or* "requirement" *or* "deployment" *or* "effectiveness" *or* "planning"
"Cyber security guideline"	"management" *or* "development" *or* "implementation" *or* "design" "requirement" "deployment" "effectiveness" "planning"
"IS security policy"	"deployment" *or* "deployment" *or* "planning"
"IS security instruction"	"management" *or* "development" *or*

(*continued*)

Search query 1	Search query 2
	"implementation" *or* "design" "requirement" *or* "deployment" *or* "effectiveness" *or* "planning"
"IS security rule"	"management" *or* "development" *or* "implementation" *or* "design" "requirement" *or* "deployment" *or* "effectiveness" *or* "planning"
"IS security formal control"	"management" *or* "development" *or*
	"implementation" *or* "design" *or* "requirement" *or* "deployment" *or* "effectiveness" *or* "planning"
"IS security guideline"	"management" *or* "development" *or* "implementation" *or* "design" "requirement" *or* "deployment" *or* "effectiveness" *or* "planning"

Table AII.

Appendix 3. Identified papers with no access

Table AIII lists the identified papers that we were not able to access.

ID	Author (s)	Papers' titles	Type
1	Gaigole and Khere (2012)	Web-based group decision support system for information security decision-making in case of Indian e-government systems	Proceeding paper
2	Ismail *et al.* (2010)	Examining information security concerns: Case study of Malaysian academic setting	Proceeding paper
3	Kabay (1994)	Psychosocial factors in the implementation of information security policy	Journal
4	Lee *et al.* (2009)	Cyber security design requirements based on a risk assessment	Conference
5	Superdome (2014)	Perturbing information security policy statements using deviational analysis	Conference
6	Yaokumah *et al.* (2016)	Towards modelling the impact of security policy on compliance	Journal
7	Zhou (2010)	The implementation of basic information security policy management framework using Java	Proceeding paper

Table AIII.
Papers that we were unable to analyse

Appendix 4. Definitions of the different research methods used in our classification framework

Table AIV provides operational definitions of the types of research methods that we used in the classification framework.

Table AIV. Operational definitions of research methods

Research method	Operational definition
Action research	This category refers to the contribution of knowledge whilst at the same time solving organisational problems through intervention. Action research can be distinguished from consultancy in that the researcher uses particular theoretical tools to solve the organisational problems and uses the results of the interventions to evaluate and improve existing theory
Case study	This category refers to the contribution of knowledge through in-depth enquiries into a phenomenon within its real-life context, where the boundaries between phenomenon and context are not clearly apparent
Consultancy	This category refers to the provision of an expert service for a client in return for a fee. Hence, it might be argued that this is not research at all; however, it is possible to learn from such projects
Critical theory	This category refers to the contribution of knowledge through the articulation of assumptions that keep people from a full understanding of how the world works
Design science	This category refers to the contribution to knowledge through the design of novel or innovative artefacts (Hevner *et al.*, 2004). Such research consists of build-and-evaluate loops, and the developed knowledge ranges from design principles, construction methods and tools to basic assumptions about the context in which the artefact is to function (Gregor and Jones, 2007)
Ethnography	This category refers to the contribution of knowledge through an understanding of a phenomenon from the perspective of the people involved; in other words, understanding their values, language and practices. Ethnography has its roots in anthropology and the researcher spends a considerable amount of time in a particular (sub)organisation. This category shades into participant observation
Experiments	This category refers to the contribution of knowledge through the provision of insights into cause-and-effect. This is carried out by deliberately manipulating certain factors in artificially generated situations. This category includes both laboratory and field experiments
Grounded theory	This category refers to the contribution to knowledge through the marking of key points in the collected data with a series of codes. These codes are grouped into similar concepts from which the categories are formed. Finally, a theory can be constructed
Interviews	This category refers to the contribution to knowledge through a conversation in which a researcher elicits information from a respondent. Different types of interview techniques are included in this category, ranging from unstructured interviews (open-ended discussions) to structured interviews (a pre-structured set of questions). Moreover, interviews with one or more interviewees can be held at the same time (e.g. focus groups)
No method	This category is a placeholder for capturing when researchers have not explicitly stated or described the research method(s) they have used. This does not mean that they have not used any research method; however, the researchers do not give any account of it
Participant observation	This category refers to the contribution to knowledge through active participation in a situation. The people in the situation do not need to be aware

(*continued*)

Research method	Operational definition
	of the researcher. This category is an extension of ethnography (Mingers, 2003 b).
Passive observation and measurement	This category refers to the contribution to knowledge through the direct observation, recording and measurement of phenomena that result in quantitative data. Such knowledge is developed through statistical analysis
Qualitative content analysis	This category refers to the contribution to knowledge through the analysis of texts or pictures to identify "the occurrence of specific categories or terms" (Mingers, 2003 b). The analysis can either be carried out using predefined categories or in an "interpretive manner, recognizing the role of the analyst in doing this" (Mingers, 2003 b)
Simulation	This category refers to the contribution to knowledge through the recreation of situations and data in such a way that they are, to some extent, representative of a relevant real-world situation.
Survey, questionnaire, or instrument	This category refers to the contribution to knowledge through a pre- structured set of questions, regardless of the technique used for the administration and circulation of these questions. Data is collected through the sampling of individual units from a wider population and the analysis includes any type of statistical method

Table AIV.

Appendix 5. Detailed information on the analysed papers based on their type of coverage

Table AV shows the coverage of ISP management phases in existing research and how these phases have been combined.

Type of coverage	Phases	Type of focus		
		Manual	Computerised	Total
Low	Risk management	1	–	1
	Construction	11	–	11
	Implementation	14	–	14
	Compliance	47	2	49
	Monitoring	3	1	4
	Total	*76*	*3*	*79*
Medium	Risk Management, Construction	1	2	3
	Construction, Implementation	5	–	5
	Construction, Compliance	3	–	3
	Construction, Monitoring	2	–	2
	Implementation, Compliance	6	1	7
	Risk assessment, Construction, Implementation	2	–	2
	Construction, Implementation, Compliance	5	–	5
	Construction, Implementation, Monitoring	5	0	5
	Construction, Compliance, Monitoring	1	–	1
	Implementation, Compliance, Monitoring	1	–	1
	Risk assessment, Construction, Compliance, Monitoring	–	1	1
	Risk assessment, Construction, Implementation, Monitoring	7	–	7
	Construction, Implementation, Compliance, Monitoring	1	–	1
	Total	*39*	*4*	*43*
High	Risk Management, Construction, Implementation, Compliance, Monitoring	2	–	2
	Total	*2*	–	*2*
Total		*117*	*7*	*124*

Table AV. Coverage and combinations of ISP management phases

Note: Please note that papers can address both manual and computerised support, which means that the total number of papers exceeds the actual number of papers

Appendix 6. Papers included in the research

Table AVI presents a detailed analysis of the papers that we could access.

ID	Author(s)	Type of focus		Phases					Research method
		Manual	Computerised	Risk assessment	Construction	Implementation	Compliance	Monitoring	
1	Abdelwahed *et al.* (2016)	Yes	No	*	*	*		*	Survey
2	Abed *et al.* (2016)	Yes	No				*		Survey
3	Al-Izki and Weir (2016)	Yes	No				*		Survey
4	Abraham and Chengalur-Smith (2011)	Yes	No		*	*			Case study, Interview
5	Al-Hamdani and Dixie (2009)	Yes	No	*	*	*			No method
6	Al-Mukahal and Alshare (2015)	Yes	No		*	*	*		Survey
7	Almusharraf *et al.* (2015)	Yes	No		*		*		Case study, Interview
8	Arif (2011)	Yes	No				*		Survey
9	Asai and Hakizabera (2010)	Yes	No			*			Interview
10	Aurigemma and Mattson (2014)	Yes	No				*		Survey
11	Aurigemma and Mattson (2017a)	Yes	No				*		Survey
12	Aurigemma and Mattson (2017b)	Yes	No				*		Survey
13	Balozian and Leidner (2016)	Yes	No				*		Interview, Grounded theory
14	Bauer and Bernroider (2017)	Yes	No				*		Survey, Interview, Case study
15	Bauer *et al.* (2017)	Yes	No			*	*		Case study, Interview, Qualitative content analysis
16	Bernik (2016)	Yes	No				*		Survey
17	Bhardwaj *et al.* (2016)	Yes	No	*	*	*		*	No method
18	Bulgurcu *et al.* (2009a)	Yes	No				*		Survey
19	Bulgurcu *et al.* (2009b)	Yes	No				*		Survey
20	Bulgurcu *et al.* (2010)	Yes	No				*		Survey
21	Busch *et al.* (2016)	No	Yes			*	*		Survey, Experiment, Participant observation
22	Buthelezi *et al.* (2016)	Yes	No		*		*		Case study, Qualitative content analysis
23	Chen *et al.* (2012)	Yes	No				*		Survey, Participant observation
24	Cheng *et al.* (2013)	Yes	No				*		Survey

(*continued*)

Table AVI.
Detailed analysis

Table AVI.

ID	Author(s)	Type of focus		Phases					Research method
		Manual	Computerised	Risk assessment	Construction	Implementation	Compliance	Monitoring	
25	Cherdantseva and Hilton (2013)	Yes	No		*			*	Case study, Qualitative content analysis
26	Cheung (2014)	Yes	No		*	*			No method
27	Choi (2016)	Yes	No		*		*		Survey
28	Coertze and von Solms (2013)	No	Yes	*	*		*	*	Interview
29	Coertze *et al.* (2011)	No	Yes	*	*				Case study
30	Corpuz and Barnes (2010)	Yes	No	*	*	*		*	No method
31	Corpuz (2011a)	Yes	No					*	No method
32	Corpuz (2011b)	Yes	No	*	*	*		*	No method
33	Cosic and Boban (2010)	Yes	No		*				No method
34	Dinev *et al.* (2009)	Yes	No				*		Case study, Survey
35	D'Arcy *et al.* (2014)	Yes	No				*		Survey
36	Doherty and Fulford (2006)	Yes	No		*				Simulation
37	Doherty *et al.* (2009)	Yes	No					*	Survey
38	Fragos *et al.* (2007)	Yes	No			*			Case study, Interview
39	Fulford and Doherty (2003)	Yes	No			*			Survey
40	Gadzama *et al.* (2014)	Yes	No			*			Survey
41	Gaunt (1998)	Yes	No		*	*			Survey, Participant observation
42	Gerber *et al.* (2016)	Yes	No				*		Survey
43	Ghazvini and Shukur (2016)	Yes	No			*			Interview
44	Ghazvini and Shukur (2017)	Yes	No			*			Survey
45	Gritzalis (1997)	Yes	No		*				No method
46	Guo and Yuan (2012)	Yes	No				*		Survey
47	Hedström *et al.* (2011)	Yes	No				*		Interview, Case study, Qualitative content analysis, Passive observation
48	Hedström *et al.* (2013)	Yes	No				*		Interview, Case study, Qualitative content analysis, Passive observation
49	Herath and Rao (2009)	Yes	No				*		Survey
50	Höne and Eloff (2002a)	Yes	No		*			*	No method

(*continued*)

Table AVI.

ID	Author(s)	Type of focus		Phases					Research method
		Manual	Computerised	Risk assessment	Construction	Implementation	Compliance	Monitoring	
51	HöNe and Eloff (2002b)	Yes	No		*	*			No method
52	Hong *et al.* (2006)	Yes	No		*	*		*	Survey
53	Hou *et al.* (2011)	Yes	No				*		Survey, Case study
54	Hsu *et al.* (2015)	Yes	No				*		Survey
55	Hu *et al.* (2012)	Yes	No				*		Survey
56	Huang *et al.* (2016)	Yes	No				*		Survey
57	Humaidi and Balakrishnan (2015a)	Yes	No		*	*	*		Survey
58	Humaidi and Balakrishnan (2015b)	Yes	No				*		Survey
59	Ifinedo (2012)	Yes	No				*		Survey
60	Ifinedo (2014)	Yes	No				*		Survey
61	Ifinedo (2016)	Yes	No				*		Survey
62	Ismail and Widyarto (2016)	Yes	No	*	*	*		*	Case study, Qualitative content analysis
63	Johnston *et al.* (2013)	Yes	No			*	*		Survey
64	Johnston *et al.* (2015)	Yes	No				*		Survey, Interview
65	Kadam (2007)	Yes	No	*	*	*			No method
66	Kadir *et al.* (2016)	Yes	No				*		Survey
67	Kajtazi and Bulgurcu (2013)	Yes	No				*		Survey
68	Karlsson *et al.* (2017)	Yes	No		*		*	*	Interview, Case study, Qualitative content analysis, Passive observation
69	Karyda *et al.* (2003)	Yes	No		*	*		*	Interview
70	Karyda *et al.* (2005)	Yes	No		*	*		*	Case study, Interview
71	Kim *et al.* (2014)	Yes	No				*		Survey
72	Knapp *et al.* (2009)	Yes	No	*	*	*	*	*	Survey, Interview, Qualitative content analysis, Grounded theory
73	Kolkowska and De Decker (2012)	Yes	No		*	*	*		Case study, Interview
74	Kolkowska *et al.* (2017)	Yes	No				*		Interview, Passive observation, Design science

(*continued*)

Table AVI.

ID	Author(s)	Type of focus		Phases					Research method
		Manual	Computerised	Risk assessment	Construction	Implementation	Compliance	Monitoring	
75	Koziel (2011)	Yes	No		*				No method
76	Kretzer and Mädche (2015)	Yes	No				*		Survey
77	Kurtel (2008)	Yes	No		*				No method
78	Kyobe (2010)	Yes	No				*		No method
79	Lapke and Dhillon (2015)	Yes	No		*	*			Case study, Interview
80	Lindup (1995)	Yes	No		*				No method
81	Lopes and Oliveira (2015a)	Yes	No			*			Survey
82	Lopes and Oliveira (2015b)	Yes	No			*	*	*	Action research
83	Lopes and Oliveira (2015c)	Yes	No		*				Action research
84	Lopes and Oliveira (2016)	Yes	No		*	*	*		Action research
85	Lowry and Moody (2015)	Yes	No				*		Survey, Qualitative content analysis
86	Mader and Srinivasan (2005)	Yes	No		*	*		*	No method
87	Mavetera *et al.* (2015)	Yes	No			*	*		Survey
88	Maynard *et al.* (2011)	Yes	No		*				Interview
89	Merhi and Ahluwalia (2015)	Yes	No				*		Survey
90	Myyry *et al.* (2009)	Yes	No				*		Survey, Case study
91	Niemimaa (2016)	Yes	No		*				Ethnography, Participant observation
92	Niemimaa and Niemimaa (2017)	Yes	No			*			Ethnography, Participant observation
93	Nowicki *et al.* (2006)	Yes	No			*			Case study, Survey
94	Pahnila *et al.* (2013)	Yes	No				*		Survey, Interview
95	Palmer *et al.* (2001)	Yes	No	*	*	*		*	No method
96	Pathari and Sonar (2012)	Yes	No			*			Case study, Interview, Qualitative content analysis
97	Rees and Allen (2008)	Yes	No	*					Survey
98	Reichard *et al.* (2011)	Yes	No			*			Interview
99	Renaud and Goucher (2012)	Yes	No		*	*	*		Interview
100	SanNicolas-Rocca *et al.* (2014)	Yes	No				*		Survey, Case study, Experiment
101	Saran and Zavarsky (2009)	No	Yes				*		Case study
102	Sharifa *et al.* (2009)	Yes	No			*			Survey, Interview
103	Shih *et al.* (2016)	Yes	No			*	*		Survey

(*continued*)

ID	Author(s)	Type of focus		Phases					Research method
		Manual	Computerised	Risk assessment	Construction	Implementation	Compliance	Monitoring	
104	Simms (2009)	Yes	No	*	*	*		*	No method
105	Siponen *et al.* (2006)	Yes	No				*		Survey
106	Siponen *et al.* (2009)	Yes	No				*		Survey
107	Siponen *et al.* (2014)	Yes	No				*		Survey
108	Siponen and Iivari (2006)	Yes	No		*				No method
109	Sohrabi Safa *et al.* (2016)	Yes	No				*		Survey
110	Sommestad *et al.* (2015)	Yes	No				*		Survey
111	Son (2011)	Yes	No				*		Survey
112	Syamsuddin and Hwang (2010)	No	Yes					*	Survey
113	Talbot and Woodward (2009)	Yes	No		*	*	*	*	Consultancy
114	Tsohou *et al.* (2015)	Yes	No			*	*		No method
115	Tuyikeze and Pottas (2011)	Yes	No	*	*	*	*	*	No method
116	Vermeulen and Von Solms (2002)	Yes	Yes	*	*				No method
117	Von Solms *et al.* (2011)	Yes	No		*				No method
118	Vroom and Von Solms (2003)	Yes	No					*	No method
119	Wang and Li (2015)	No	Yes				*		Survey, Interview
120	Wiant (2005)	Yes	No			*			Survey
121	Yang *et al.* (2011)	Yes	No			*	*		Survey
122	Yayla (2011)	Yes	No			*			No method
123	Yusufovna (2008)	Yes	No		*	*		*	Survey, Interview, Case study

Table AVI.