Information & Computer Security

Inter-organisational information security: a systematic literature review

Fredrik Karlsson Ella Kolkowska Frans Prenkert

1. Introduction

Today's business environment is becoming more and more competitive. Both national and international organisations are therefore moving away from operating as individual businesses to become strategic alliances (Tomkins, 2001, Gomes et al., In press). Collaboration through more integrated business processes is often enabled through the use of information technology. PriceWatherhouseCoopers (2010) has shown that information flows between organisations have increased in recent years. Kunz et al. (2011) also concluded that, "[w]ith this intensified exchange, information security becomes a major issue".

Information security risks certainly exist in individual businesses; however, inter-organisational collaboration introduces new forms of risks by opening opportunities for intrusion, non-compliance and exposure (Goodman and Ramer, 2007). Suddenly, information security risks cross boundaries, so that organisations become dependent on their partners to create information security (ISO 27010, 2012). For example, Thomas (2012) argued that "supplier information security breaches have the potential to cause greater harm that would other types of supplier disruption". Consequently, it is hardly surprising that inter-organisational information security is on the agenda of most practitioners (e.g. Vlissidis, 2012, Flinders, 2013, Ashford, 2015). From a research point of view, calls have been made to carry out more research in this area. For example, in their study on security architectures in networked environments Cherdanstseva et al. (2011) claimed that there is "an important gap in the current literature in addressing peculiarities of this environment". Similarly, Kunnathur and Vaithianathan (2008) concluded that, "[c]learly there is a significant gap in the research literature on inter-organizational information security".

Despite the practical demands and the calls for more research, there is still a lack of overview and critical discussion on the research topics in state-of-the-art inter-organisational information security research as well as concerning the maturity of this area. The study by

McLaughlin and Gogan (2014) is a notable exception. In their study, they identified existing literature on the inter-organisational aspects of information security. However, they limited their search to relatively few research outlets, thus providing us with only a superficial knowledge of existing research. Consequently, at present it is difficult to pinpoint gaps in existing research and highlight any future research directions.

Against this background, the aim of this paper is to survey existing inter-organisational information security research in order to scrutinise the kind of knowledge that is currently available, and the way in which this knowledge has been brought about. We therefore pose the following research questions:

Q1: What *kinds of primary research topics* related to inter-organisational information security have been investigated in prior research?

Q2: *How mature is prior research* on inter-organisational information security research?

Q3: What *kinds of research methods* dominate inter-organisational information security research?

Our results are based on a review of inter-organisational information security research literature published between 1990 and 2014. The study is based on a gross list of papers that initially consisted of 877 research papers (including duplicates). Of these, 66 papers were singled out for further analysis (more details are given in the Research method section). Our systematic review provides valuable insights into the topics researched, as well as those areas addressed less frequently. We have also been able to discuss the maturity of this research by assessing its purposes to date and the types of research methods most commonly used in existing studies. This paper thus contributes with an assessment of the character of current inter-organisational information security research and the methods used. Moreover, it pinpoints areas for future research based on areas of information security that are clearly under-researched.

The rest of this paper is organised as follows. The second section discusses the concept of inter-organisational information security. It also describes existing literature reviews on information security research, and in particular their focus on inter-organisational aspects, research methods and research maturity. The third section presents the research method adopted for our literature review. In the fourth section, we present the results of our review by first presenting the identified topics that relate to inter-organisational information security. We then present our findings on the maturity of inter-organisational information security research. Finally, in this section, we provide an overview of the research methods used to make this knowledge available. This information forms the basis for a discussion of their impact on inter-organisational information security research and practice. We end the paper with a short conclusion.

2. Related Research

2.1 Inter-organisational information security

Inter-organisational collaboration is characterised by voluntary agreements between organisations for the “exchange, sharing or codevelopment of products, technologies, or service” (Li et al., 2013). These kinds of collaboration are strategic decisions that relate to organisational design; they also give inter-organisational information security its key characteristic. Inter-organisational information security means that the collaborating organisations have to open their boundaries by sharing “information that in an intra-organisational setting is considered an organisation’s own property” (Karlsson et al., 2015) in order to achieve *shared business goals* (Cheng, 2011).

Consequently, the traditional security perimeter of an organisation is dissolved and the organisation has to allow non-staff access to information assets; the term non-staff includes "service providers, collaborators, authorities and customers" (Cherdantseva et al., 2011). Access is also given to other organisations' information systems. Having said that, only some parts of the collaborating organisations are able to access the sensitive information shared (ISO, 2012). This means that information security dependencies are created between selected parts of two or more information security systems (Kiely and Benzel, 2006). Hence, inter-organisational information security needs to focus on the *dependencies* between these systems or parts thereof. These dependencies add an extra layer of complexity to intra-organisational information security.

2.2 Inter-organisational information security in existing literature reviews

Although literature reviews on information security have been published periodically (e.g. Baskerville, 1993, Dhillon and Backhouse, 2001, Siponen and Willison, 2007, Abraham, 2011), relatively few of them have addressed existing inter-organisational information security research (McLaughlin and Gogan, 2014). For example, several studies have reviewed information systems security methods, classifying them into different generations (Baskerville, 1993, Siponen, 2005a, Siponen, 2005b). Abraham (2011) and Lebek et al. (2013) focused on employees' information security behaviour in organisations, reviewing different aspects of this topic. The former study focused on factors that influence employees' information security behaviour in organisations; the latter addressed the sorts of theories used to explain employees' security awareness and behaviour. Whilst all these studies offer a valuable overview of information security research, none of them refer to inter-organisational information security.

Dhillon and Backhouse (2001) employed the framework put forward by Burell and Morgan (1979) to assess information security research in general. According to their study, information security research is dominated by a "technical and functionalist preconception". They did not, however, pay any attention to the inter-organisational aspect of information security. Siponen and Willison (2007) carried out an extensive review of existing information security research published between 1990 and 2004. In all, they analysed 1,280 studies in terms of the theories and research methods used, and the research topics covered. Although they identified a broad range of research topics, 14 of these topics made up 71% of all the studies. Inter-organisational information security was not among the research topics listed. The authors also concluded that the most frequently used research method was subjective-argumentative, with approximately 78% of the papers falling into this category. Consequently, one can conclude that information security research at that time had a bias towards conceptual papers; empirical inquiries were not as frequent. As a result, they argued that more research was needed "that uses empirical methods including, for example, surveys, case studies and actions research". These two studies have given us a general overview of the most prominent research in information security research. However, they tell us little about the development of research on inter-organisational information security over time.

McLaugklin and Gogan (2014) included "inter-organisational" as a category in their review of information security research published in the AIS Senior Scholars' Basket of Eight between 2004 and 2013. It should be noted, however, that they focused on collaboration between organisations with information security as an end (such as sharing security information (Gal-Or and Ghose, 2005) and organisations' participation in the development of international information security standards (Backhouse et al., 2006)). We are interested in information security as a means to support the achievement of *shared business goals* in inter-organisational collaboration. Although the authors identified five publications (from 85 papers) that addressed inter-organisational information security, this was not a large enough set of publications to create a clear pattern of research methods used. When discussing research methods used on a general level, they found fewer subjective-argumentative studies than Siponen and Willison (2007). Nonetheless, they concluded that qualitative methods are under-represented. In their literature review, McLaugklin and Gogan (2014) explicitly categorised inter-organisational studies as a type of information security research. That said, their study still offers limited knowledge about this sub-field. This is mainly because their search was limited to the Basket of Eight.

We conclude that there is no existing literature review on inter-organisational information security that systematically assesses current research directions in depth across a large base of publication outlets. We have also been unable to find literature reviews that assess the maturity of existing research and identify the types of research methods that dominate this research. Consequently, there is a paucity of knowledge about the frontline of research on inter-organisational information security.

3. Research method

The research method used in this study consists of five steps that are quite straightforward on a general level. However, their implementation was far from mechanical. During the selection and classification of papers several issues arose, which are detailed below. The general outline of the research method used is as follows:

1. The ABI/Inform, EBSCO, SCOPUS and Web of Science databases were used to search for potential papers.
2. The abstract of each paper was read and an initial decision was made as to whether or not the research related to inter-organisational information security, i.e. whether a study primarily addressed the way in which two or more organisations open up their boundaries by sharing what they otherwise consider proprietary business information in order to achieve shared business goals.
3. The introduction of each paper was read. The research questions and purpose of each paper were noted in the terms used in the paper, and classified using Kiely and Benzel's (2006) framework of an information security system (see Section 3.3). All

papers were assigned to one or several parts of the system in order to pinpoint existing research topics.

4. The original descriptions of research purpose were also classified according to Grönlund's (2001) research purpose framework (see Section 3.4) in order to assess the maturity of existing research.
5. The research method section of each paper was read (if such a section was found). The research methods used were noted and classified using an extended version of Mingers' (2003) research method framework (see Section 3.5).

The result of the detailed analysis is found in Appendix C (Table C1); a summary is presented in the Results section.

3.1 Selection of papers

Information security research appears both in conference proceedings and in international journals. Thus, it is reasonable to assume that research which addresses inter-organisational aspects on this topic will also be found in these publications. Thus, our search for papers was carried out using the ABI/Inform, EBSCO, SCOPUS and Web of Science databases in order to get a broad coverage of both international journals and conference proceedings. All in all, the databases offer a good coverage of the information systems field; certainly, they provide us with a good sample of papers that show existing patterns of inter-organisational information security research. The search included papers published on the databases between 1990 and 2014.

Table A1 in Appendix A shows the combination of search criteria that were used when searching in the databases; search fields included paper title, abstract and keywords. In order to capture inter-organisational aspects of information security we used a large set of keywords that are commonly used in business administration research to highlight inter-organisational research. The use of multiple search queries resulted in a gross list of 877 research papers, including duplicates. After eliminating duplicates and papers that did not primarily focus on inter-organisational information security, we ended up with a net list of 66 papers, of which we were able to analyse 64. The two papers we were unable to analyse are listed in Table C2, Appendix C. This reduction in relevant papers was due to the fact that papers were included in the first dataset if they contained *either* information security *or* inter-organisational issues. For the second dataset, we then singled out papers that *combine* the two. We chose this method to ensure we would not miss any papers by setting search parameters that are too narrow.

3.2 Analytical framework and classification of papers

It has been suggested that research fields, or sub-fields, fall along a continuum, from emergent to mature, which can be measured empirically (e.g. Grönlund, 2003, McLaughlin and Gogan, 2014). The basic principle behind this suggestion is straightforward: the stage of development of the research literature at one point in time usually influences the type of research that is undertaken at a second point in time. Thus, the less known about a specific topic, the more effort is put into explorative research. As a topic is researched more, researchers can build on prior studies; they can identify critical variables in order to explain the general mechanisms that underlie the researched phenomenon, and they can use existing wisdom to propose new or modified designs. In relatively mature research fields, a variety of research topics and methods are often present, whereas emerging fields tend to have a more limited repertoire of research methods (Cheon and Grover, 1993).

From this starting point, we considered it necessary to describe three key elements in inter-organisational information security research: (1) research questions, (2) maturity of research, and (3) research methods. We discuss the classification frameworks of each of these elements below. The frameworks were employed using triangulation between the authors. We individually analysed the papers in sets of 10 papers, and compared the results. When we came across differences in classifications, we discussed them in order to reach consensus. These steps were performed in an iterative pattern.

3.3 Classification of research topics

We used Kiely and Benzel's (2006) framework of an information security system to classify the research questions identified in the papers. This framework allowed us to capture research that is focused on either the technical, formal or informal aspects of information security (Dhillon, 2007). We were also able to identify research into the intersection between them.

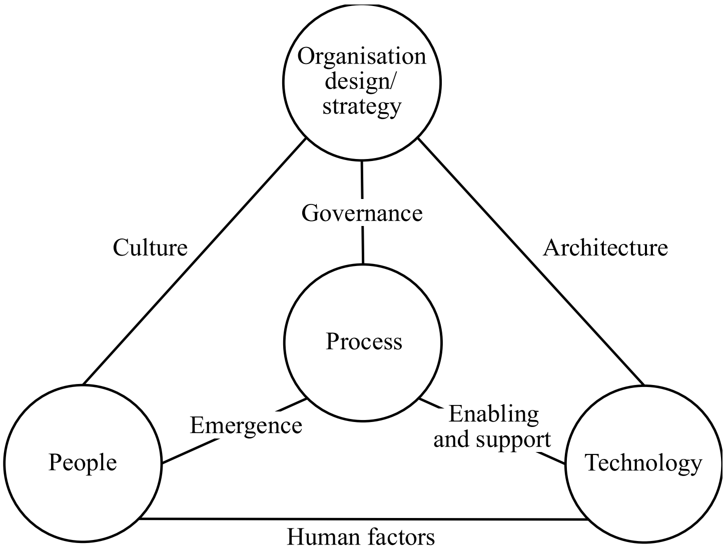

Figure 1. Information security system framework (Kiely and Benzel, 2006)

This framework consists of four nodes that are related to each other, as shown in Figure 1. Both the nodes and the relationships between them are important parts of an information security system. The four nodes are: technology, process, people, and organisation design/strategy. The technology node focuses on the development and implementation of technical solutions to prevent information security breaches; in our case, this takes place in an inter-organisational setting. Processes are about the operational policies and procedures that are used to keep inter-organisational collaboration secure. People represent the human resource aspect of the system, in this case employees and non-staff. This node focuses on their characteristics, such as skills and values, with regard to information security. The final node, organisation design/strategy, is about organisational structures and strategies, such as the decision to enter an inter-organisational collaboration and any decisions that lead to the provision of the conditions needed for the organisation to reach its goals.

Between these four nodes there are six relationships: culture, governance, architecture, enabling and support, emergence, and human factors. Culture is related to the people and organisation design/strategy nodes. It focuses on the shared pattern of values, and mental models that are traded among an organisation's employees over time, which affect inter-organisational information security. Governance relates to the organisation design/strategy and process nodes. It deals with the management and monitoring of operational processes to ensure that organisational objectives are met in an inter-organisational setting. Architecture is related to the organisation design/strategy and technology nodes. It addresses the frameworks through which an organisation aims to realise its role in the shared information security effort; it is also the framework into which processes are deployed. Enabling and support is related to the process and technology nodes. It highlights the fact that the implemented processes and technical solutions need to support each other. Emergence is related to the process and people nodes. It refers to the compliance of employees and non-staff to the information security processes. Finally, human factors connects the people and technology nodes. It addresses the extent to which the implemented technology can be used, given the skills of the employees and non-staff.

Overall, the framework provides us with ten different categories: technology, process, people, organisation design/strategy, culture, governance, architecture, enabling and support, emergence, and human factors. We organised each of the 64 papers into one or more of these categories, because a paper can cover more than one part of the framework.

3.4 Classification of maturity

Our second classification of research focuses on maturity. Maturity can be assessed by charting the nature of research (Grönlund, 2001). A scientific field or sub-field such as inter-organisational information security usually has a shared study object and a set of theories that are used to frame the general conditions of the field (Grönlund and Andersson, 2006). Thus, research aimed at pure description and case story telling signals a less mature field. On the other hand, research that focuses on theory generating and testing indicates a more mature field.

Often, three types of research purpose are used to characterise maturity of research: exploratory, descriptive and explanatory (Schutt, 2001). The framework we used builds on this classification, but was extended to include five categories, in line with the work put forward by Grönlund (2001). This allowed us to better grasp nuances at the emergent end of the scale. The categories are presented in Table 1, which has three columns. The leftmost column indicates the maturity state of the research, the second column contains the five research purpose categories, and the rightmost column shows our operational definitions. The general idea is that a less mature field would focus more on exploring, describing and reflecting upon a phenomenon, while a more mature field would focus on the generation and testing of theories that either explain or design a phenomenon.

Table 1. Types of research maturity, based on Grönlund (2001)

State of research	**Research purpose**	**Operational definition**
Emergent	Descriptive	"Describes a phenomenon in its appearance without any use of theory"
↕	Philosophical	"Reflects upon a phenomenon without data or reference to any theory"
	Theoretical	"Reflects upon a phenomenon based on some theory but without empirical data or with only anecdotal and particular such"
	Theory generating	"Attempts to analyse/interpret quantitative or qualitative data in a systematic manner for the purpose of model building"
Mature	Theory testing	"Attempts to test a theory using quantitative or qualitative data in a systematic manner, i.e. not just strict theory testing"

3.5 Classification of research methods

A third important element for classifying research is the type of research method used. Given that several frameworks exist for this purpose (e.g. Galliers, 1992, Mingers, 2003, Palvia et al., 2004, Dwivedi and Kuljis, 2008), it is inevitable that this type of classification can be carried out in slightly different ways. We used a modified version of Mingers' (2003) framework, even though it adopts a rather broad definition of research method. The main reason for this is that we can make comparisons between research on inter-organisational information security and the broader information systems field. Mingers (2003) included 13 types of research methods in his original framework, to which we have added four. The first is design science, which has received increased attention in recent years, most notably, after Mingers' (2003) framework was created. The second is systems engineering. During the classification work we found a need to acknowledge studies that constructed IT artefacts or parts thereof but did not employ an intervention approach such as action research and design science. Furthermore, Mingers (2003) only analysed empirical papers; thus, he did not include literature review or argument in his list of research methods. All in all, our modified framework contains 17 types of research method: action research, case study, consultancy, critical theory, design science, ethnography, experiments, grounded theory, interviews, literature review, participant observation, passive observation and measurement, qualitative content analysis, simulation, subjective/argumentative, survey/questionnaire/instrument, and systems engineering. The detailed operational definitions of these research methods are found in Appendix B. In our classification we acknowledged the possibility of studies employing a multi-method (Brewer and Hunter, 1989) or mixed-method (Creswell, 2003) approach, i.e. when a study is carried out using more than one research method.

4. Results

In this section we present a summary of our literature review, structured according to our three research questions. The detailed analysis is found in Appendix C.

4.1 Research topics investigated in inter-organisational information security research

Figure 2 shows how existing research is distributed in the information security system model; the actual number of papers is presented in brackets. The overview shows that most research has been devoted to topics in the upper and right-hand parts of the figure. The largest share of research has focused on organisation design/strategy, followed by governance. Technology has received significant attention together with related enabling and support. Whilst processes and architecture have received some attention, emergence has been barely touched on in this context. Finally, there is a complete lack of literature relating to cultural aspects, people and human factors. Below we take a closer look at the content of each of these categories.

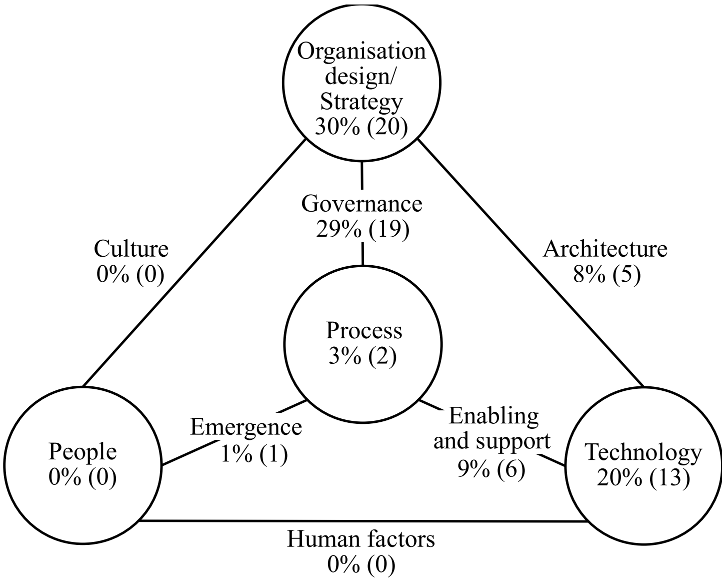

Figure 2. Research topics investigated

Research on organisation design/strategy focuses on information security related to different types of inter-organisational designs from a strategic point of view. Papers within this category often describe or assess risks in particular designs or propose frameworks to carry out risk assessments before an organisation makes any decisions about inter-organisational design. With regard to types of inter-organisational designs, supply-chain and outsourcing strategies are widely discussed. For example, several frameworks for risk propagation in supply chains have been suggested (Behara et al., 2007, Huang et al., 2008, Smith et al., 2007), meanwhile Deane et al. (2010) investigated the increased risks generated when medical companies connect in supply chains. Bandyopadhyay et al. (2010, 2005) and Vaidyanathan (2012) studied companies in supply chains and their investment strategies, together with the incentives to invest in information security. With regard to outsourcing, efforts have been made to identify different types of risks (Bahl et al., 2011, Khalfan, 2004, Pemble, 2004). Wei et al. (2010) also suggested safeguards in three categories (technical, data and human) to counter such risks. Khidzir et al. (2010b) stated that information security risk management is related to outsourcing strategies.

Governance focuses on the management of operational information security processes. Several scholars have sought to define tasks and critical activities relating to information security management in inter-organisational settings (Li and Chandra, 2008, Thalmann et al., 2012). Frameworks for management activities have aimed to: assess (Deane et al., 2009, Lu et al., 2013, Nassimbeni and Sartor, 2012), monitor (Shing et al., 2007) and mitigate (Su et al., 2012) risks in inter-organisational business processes. In addition, a framework for "achieving interoperability when multiple security policies are employed" (Kokolakis and Kiountouzis, 2000) in inter-organisational collaboration has been suggested. Research has also shown limitations in existing information security management systems and how they need to be extended to include cloud computing (Julisch and Hall, 2010), which is viewed as a specific type of outsourcing.

Technology research has addressed technical solutions to prevent information security incidents in inter-organisational settings. Often the technical solutions have targeted specific organisational designs. For example, in terms of cloud computing, Hao and Cai (2011) proposed a new cloud model to provide "a confidential and verifiable environment for each sensitive application". In terms of manufacturing outsourcing, Xue and Li (2005) focused on how to use 3D models to release the necessary engineering information for collaborative assembly design, whilst at the same time hiding sensitive information. We also identified more generic technical solutions; for example, Chen et al. (2007) and Santos-Pereira et al. (2013) presented access controls for inter-organisational settings and Yuan et al. (2009) proposed a virus propagation model.

Research on enabling and support has investigated the way technology and processes align with each other in inter-organisational collaboration. We found that a great deal of attention has been given to access control systems and business processes (Kunz et al., 2011, Peng et al., 2014, Santos-Pereira et al., 2013, Gajanayake et al., 2011). Peng et al. (2014) proposed an access control theory based on organisational design. This theory suggests that authorisation management should "understand the detail responsibility and authorization of each individual or department in the organization" in order to support the business processes. Gajanayake, et al. (2011) proposed a framework for accessing information health care processes, a framework in which accountability is a key component.

Architectural research examines frameworks for the deployment of operational information security processes and technical implementations. We identified a small number of papers in this area (Djordjevic et al., 2007, Fabian et al., 2013, Moradian, 2008, Wangwe et al., 2012, Eigeles, 2006). For example, Wangwe et al. (2012) developed a framework for collaboration between government agencies. Djordjevic et al. (2007) summarised a novel security architecture that supports the Application Service Provision model; hence, they sought to target both commercial and government organisations.

Existing research has not devoted much attention to processes in inter-organisational collaboration, that is to say, the operational information security procedures, themselves. Gutiérrez et al. (2009) developed a tool for eliciting security requirements in inter-organisational information systems. Meanwhile, van Veenstra and Ramilli (2011) investigated the implementation of security patterns when creating access controls in a government organisation. Even fewer studies have been carried out in the area of emergence, which addresses compliance with information security processes and their inter-organisational effects. Johnson (2008) has carried out a study in this area. He examined the leakage of financial information in peer-to-peer networks and concluded that employees' use of such networks may result in the inadvertent disclosure of business information in financial supply chains.

4.2 The maturity of inter-organisational information security research

Figure 3 shows our maturity analysis of existing inter-organisational information security research. The analysis is structured according to Grönlund's (2001) types of research purpose: descriptive, philosophical, theoretical, theory generating and theory testing. Approaching these categories in descending order, Figure 3 shows that the largest category is made up of papers that are theoretical. Indeed, they account for 45% of research (30 papers). In other words, these papers reflect on different aspects of inter-organisational information security using some theory; however, they do not include empirical data. It is worth noting that this category constitutes 53% of research (10 papers) on governance (e.g. Gritzalis et al., 2007, Li and Chandra, 2008, Su et al., 2012, Kokolakis and Kiountouzis, 2000); an additional 16% (3 papers) can be classed as philosophical (Deane et al., 2009, Dommun, 2008, Julisch and Hall, 2010, Kling, 1977). Consequently, the majority of governance frameworks presented are not empirically driven or tested. Moreover, Figure 3 shows that 62% of research (8 papers) on technology (e.g. Chen et al., 2007, Cook et al., 2003, Denning, 1992, Zhang et al., 2005) and 83% of research (5 papers) on enabling and support (e.g. Kearney, 2005, Mao et al., 2008, Santos-Pereira et al., 2013) are theoretical. Thus, there is insufficient evidence on how well these solutions perform in practice.

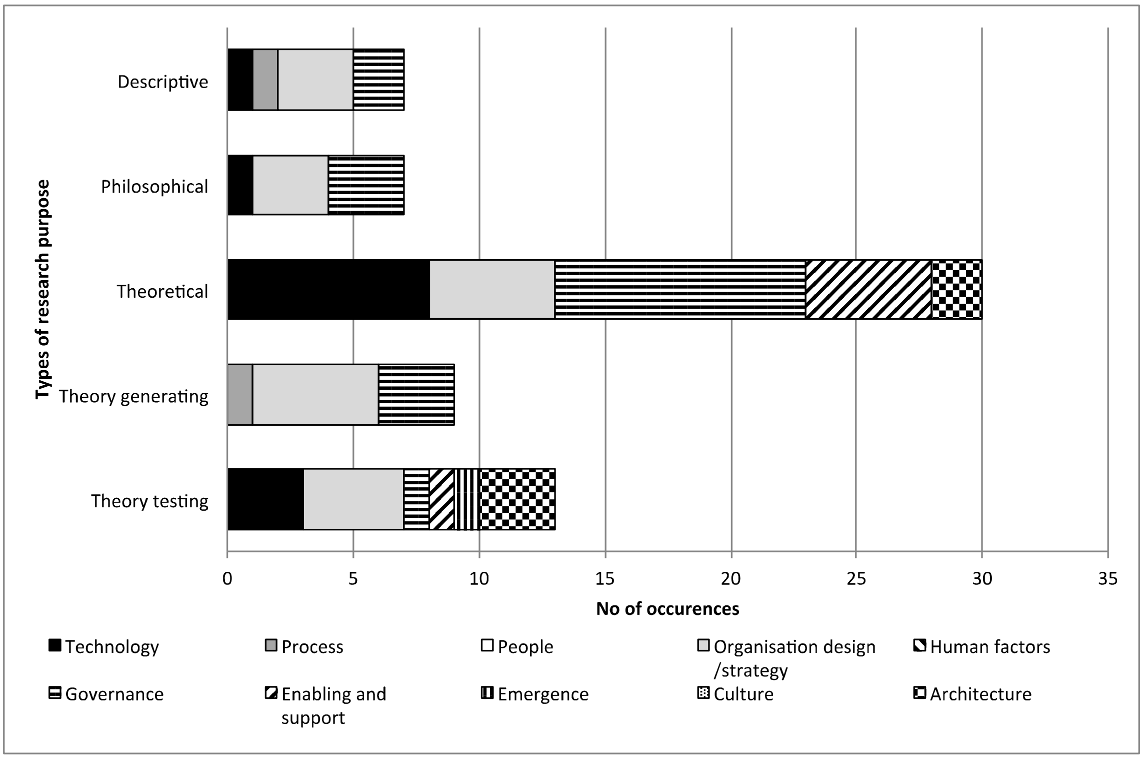

Figure 3. Maturity of inter-organisational information security research

We found that 20% of research is testing theory (13 papers), as is shown in Figure 3. These studies include both theory and empirical data; here, we interpret theory in a broad sense, as a model for understanding and predicting, or as a design principle. A closer analysis of Figure 3 shows that there are few papers in each research topic. The largest topics are technology (Kayem et al., 2011, Li and Ding, 2007, Yuan et al., 2009), organisational design/strategy (e.g. Khidzir et al., 2010a, Khidzir et al., 2010b, Robertson et al., 2010) and architecture (Djordjevic et al., 2007, Fabian et al., 2013, Wangwe et al., 2012). Together they constitute 77% of research on theory testing (10 papers). The remaining research is distributed between emergence (Johnson, 2008), enabling and support (Kunz et al., 2011) and governance (Nassimbeni and Sartor, 2012); one paper was found in each of these categories.

Theory generating papers constitute 14 percent (9 papers) of the identified research, and are the third largest set of papers in Figure 3. These papers contribute to the building of different types of models, which can be tested at a later stage. Some 88% of theory generating research (8 papers) is on management issues, with a focus on organisation design/strategy (e.g. Bahl et al., 2011, Berghmans and van Roy, 2011, Chen and Wang, 2010) and governance (Batten and Castleman, 2005, Schlaak et al., 2008, Shih and Wen, 2005), with 55 and 33% of research (5 and 3 papers), respectively. In addition, within theory generating research we identified one paper on processes (Gutiérrez et al., 2009).

In Figure 3, we identified an equal number of descriptive and philosophical papers, which amounts to approximately 11% of research (7 papers) in each category. With regard to the descriptive papers, inter-organisational information security or different aspects of that phenomenon are described without the use of theory. The largest set of papers relates to organisational design/strategy (Deane et al., 2010, Desai and McGee, 2010, Khalfan, 2004), closely followed by governance (Bartol, 2014, Thalmann et al., 2012). Together, these two categories constitute 71% of descriptive research (5 papers). In addition, we identified one descriptive study that focused on the technology (Xue and Li, 2005) and one paper on processes (van Veenstra and Ramilli, 2011).

In philosophical papers, inter-organisational information security is reflected upon without any reference to theory or the use of empirical data. On closer examination (see Figure 3), we found almost the same pattern as for descriptive papers. The two major sets of papers are found in organisation design/strategy (Davidson et al., 2013, Pemble, 2004, Power and Forte, 2005) and governance (Deane et al., 2009, Dommun, 2008, Julisch and Hall, 2010). Yet again, the focus on management issues is evident, in this case constituting 86% of philosophical research (6 papers). We also found one study on technology (Lanjuan, 2006). When compared with descriptive papers, there is a lack of papers on processes.

The majority of the investigated papers are descriptive, philosophical or theoretical. We can therefore conclude that inter-organisational information security research has the characteristics of a nascent sub-field. Nevertheless, we found some indications of change when assessing the distribution over time (see Table 2). A closer look at the period 2009 to

2014 shows that more papers were aimed at generating and testing theories based on empirical work compared with the period 1990 to 2008. Consequently, Table 2 shows that researchers in this sub-field have increased their efforts to combine empirical data and theory in their research work.

Table 2. Maturity of inter-organisational information security research, development over time

Type of research purpose	**1990-2008**	**2009-2014**	**Difference**
Descriptive	6.7% (2)	14.7% (5)	+8.0%
Philosophical	13.3% (4)	8.8% (3)	-4.5%
Theoretical	60.0% (18)	29.4% (10)	-30.6%
Sum Theoretical, Descriptive, Philosophical	*80.0% (24)*	*52.9% (18)*	*-27.1%*
Theory generating	10.0% (3)	17.7% (6)	+7.7%
Theory testing	10.0% (3)	29.4% (10)	+19.4%
Sum Theory testing, Theory generating	*20.0% (6)*	*47.1% (16)*	*+27,1%*
Total sum of papers	*30*	*34*	

Notes: The table displays shares (%) of studies with counts presented in parentheses. Time periods are divided after the median number of cases, creating time periods of unequal length but of equal size in terms of the number of studies.

4.3 Research methods used in inter-organisational information security research

Figures 4 and 5 show our analysis of research methods used in existing research on inter-organisational information security. As shown in Figure 4, our analysis was structured according to the research method *used* in existing research. Thus, the figure only contains a sub-set of our modified version of Mingers' (2003) framework. For each research method we also made a sub-categorisation based on Kiely and Benzel's (2006) framework of an information security system. Figure 5 has a similar structure, albeit we have used the five types of research purpose as sub-categories to capture the level of research maturity.

Assessing the research methods in descending order, Figure 4 shows that the subjective/argumentative research method is by far the most frequently used. It is employed in 44% of research (38 papers). The majority of these papers focuses on management issues. We found that 64% of all research (14 papers) on governance (e.g. Li and Chandra, 2008, Su et al., 2012, Yulin et al., 2006) can be found in this category, and 24% of research (8 papers) on organisational design/strategy (e.g. Bandyopadhyay et al., 2005, Davidson et al., 2013, Smith et al., 2007). In addition, some 67% of research (10 papers) on technology (e.g. Cook et al., 2003, Lanjuan, 2006, Zhang et al., 2005) is based on a subjective/argumentative method. When taking a closer look at Figure 5 we can also see that these papers are either philosophical or theoretical in nature. Consequently, these studies are not empirically grounded, i.e. they are not based on empirical data.

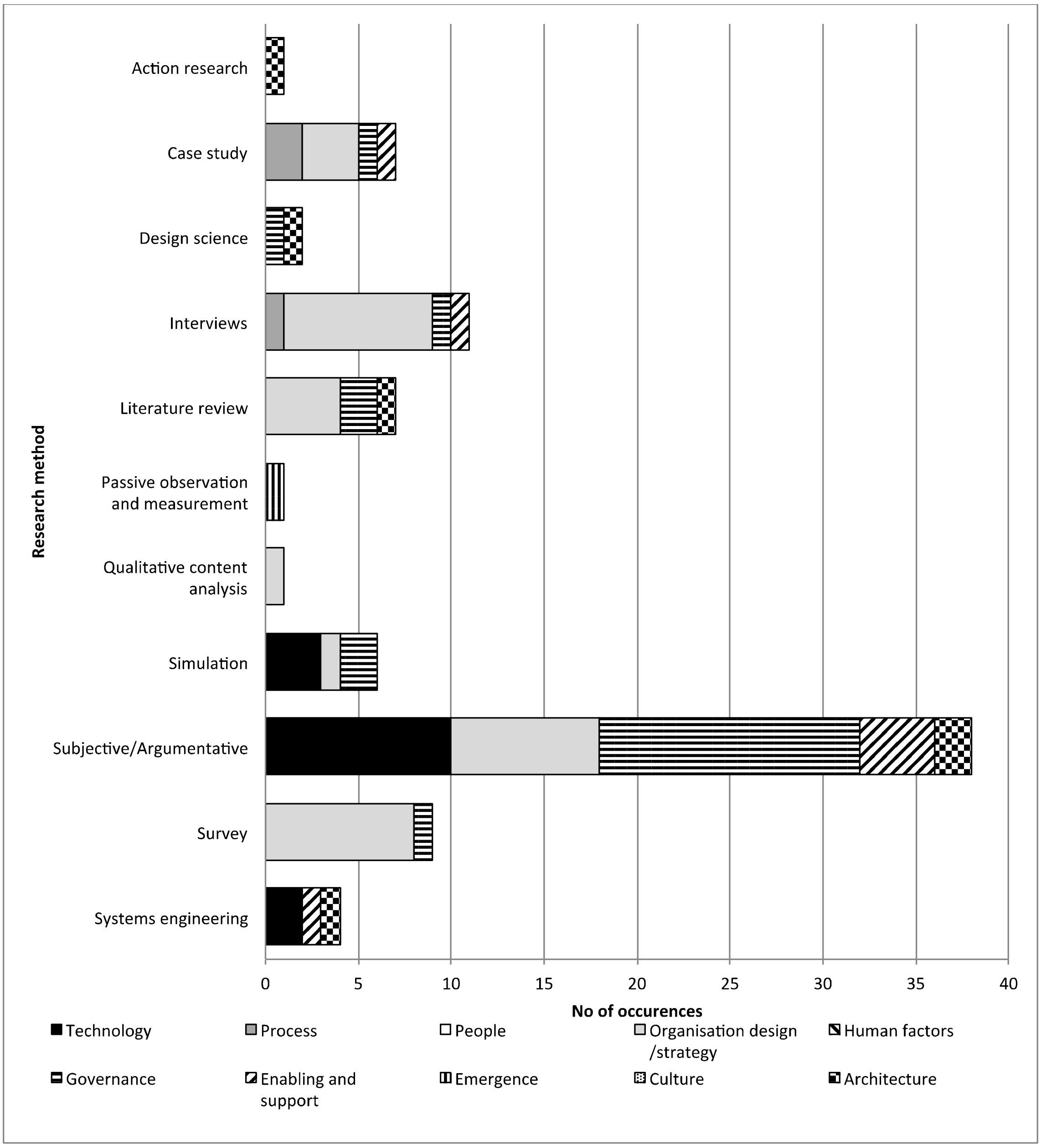

Figure 4. Types of research methods used and research topics covered

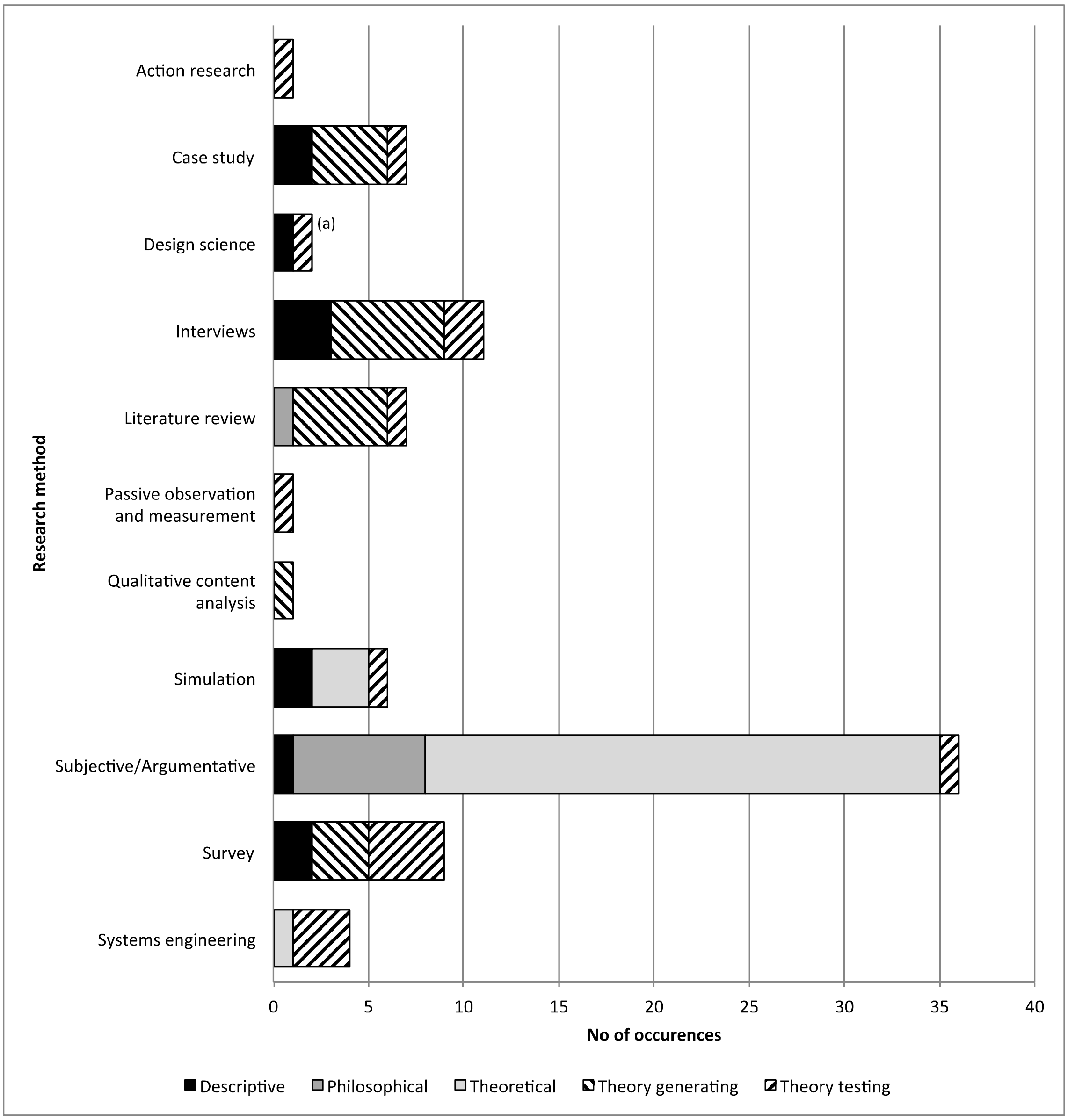

Figure 5. Types of research methods used and types of research purpose
[(a)] *Note: Includes a research-in-progress paper that only contains certain descriptive parts of the research project.*

Interviews and surveys account for 13 and 10% of research (11 and 9 papers), respectively. Based on Figures 4, we can see that interviews have been extensively used in investigations into organisation design/strategy (e.g. Berghmans and van Roy, 2011, Shittu et al., 2012, Wei et al., 2010). It should be noted that most of this research is aimed at either theory generating or theory testing. A similar pattern is evident for the use of surveys, which were used in studies on organisation design/strategy (e.g. Khalfan, 2004, Khidzir et al., 2010a, Robertson et al., 2010) and in one study on governance (Batten and Castleman, 2005). Thus, this method has been used solely for studying management issues. As Figure 5 shows, these papers are, to a large extent, either theory generating or theory testing studies.

Case studies and literature reviews each account for 8% of research methods used (7 papers). When it comes to case studies it is difficult to distinguish a clear pattern; in our study, we identified papers on organisation design/strategy (Berghmans and van Roy, 2011, Chen and Wang, 2010, Khalfan, 2004), governance (Shih and Wen, 2005), enabling and support (Kunz et al., 2011), and notably some of the few papers on processes (Gutiérrez et al., 2009, van Veenstra and Ramilli, 2011). As Figure 5 shows, most of these studies are theory generating. Literature reviews have mainly been used in studies on management issues, i.e. on organisation design/strategy (e.g. Berghmans and van Roy, 2011, Chen and Wang, 2010, Wei et al., 2010) and governance (Dommun, 2008). However, unlike many other methods, such as case studies, interviews and surveys, literature reviews have been used to provide a structured background analysis to the study at hand, rather than as a sole research method.

Figure 4 shows that simulations were used in 7% of studies (6 papers). These studies include governance (Cheng, 2012, Gritzalis et al., 2007), organisation design/strategy (Deane et al., 2010) and technology (Chen et al., 2007, Xue and Li, 2005, Yuan et al., 2009). With regard to maturity, our further analysis in Figure 5 reveals these papers are mainly descriptive or theoretical. Systems engineering accounts for 5% of studies (4 papers); these studies cover technology (Kayem et al., 2011, Li and Ding, 2007) or are related to this node in the information security system. One study was found for enabling and support (Peng et al., 2014) and one for architecture (Djordjevic et al., 2007). Most of these studies were theory testing.

Finally, we found a small number of studies that used action research (Wangwe et al., 2012), design science (Thalmann et al., 2012, Fabian et al., 2013), participation observation and measurement (Johnson, 2008), and qualitative content analysis (Bahl et al., 2011). For example, the action research study developed and tested an information security framework for collaboration between government agencies, whilst the case of qualitative content analysis was used in a theory generating study on risks in outsourcing.

To summarise, inter-organisational information security research is to a large extent based on a subjective/argumentative research method. Papers that have used this method are not empirically grounded. In addition, of the 17 types of research methods found in the modified version of Mingers' (2003) framework, we found that only 11 of them were represented in existing research. Furthermore, only six of them (case study, interviews, literature review, simulation, subjective/argumentative and survey) were used extensively.

5. Discussion

Inter-organisational collaboration is common in practice. Nonetheless, few systematic literature reviews on existing inter-organisational information security research have focused on the kind of knowledge that has been developed and how it has been brought about. The earlier study by McLaugklin and Gogan (2014) did not focus on inter-organisational information security research *per se*, although inter-organisational aspects were included in their survey of information security research in the Basket of Eight. On the other hand, our systematic literature review contributes with an explicit focus on inter-organisational information security research and a review of publications from a broader set of outlets. Figures 2 to 5 show the patterns we found and, based on these findings, some notable lessons that can be learned with regard to: (a) research topics investigated in inter-organisational information security research, (b) maturity of inter-organisational information security research, and (c) types of research methods used.

5.1 Research topics investigated in inter-organisational information security research

In our analysis of existing inter-organisational information security research we identified 66 studies, compared with the five studies identified by McLaugklin and Gogan (2014). This difference can be explained by the broader set of outlets reviewed in our study, which was not limited to the Basket of Eight. Siponen and Willison (2007) did not identify enough studies to classify inter-organisational information security as a topic in its own right. This may be explained by the fact that they surveyed papers *until* 2004, whilst the majority of the studies (94%) we identified appeared *after* 2004 (see Appendix C). However, taken together, our results show that research with an *explicit* focus on inter-organisational information security is, to date, not extensive.

The studies we identified are spread over a small number of research topics with regard to the categories found in Kiely and Benzel's (2006) framework of an information security system. Our analysis shows that the two categories: organisation design/strategy, and governance account for more than half of all the research carried out. Consequently, it is evident that inter-organisational information security has, so far, been approached as a management issue. Based on more detailed analysis we can see that the main focus has been on information security risks associated with inter-organisational designs and how to manage such risks. In addition, we have also been able to identify a larger set of research on technology, and a smaller number of papers related to the categories enable and support and architecture; in other words, research that is related to technology. Compared with earlier findings on information security research in general (Siponen and Willison, 2007), it is surprising to see that formal aspects of information security (organisation design/strategy and governance) have received more attention than technical ones (technology, architecture and enable and support). Research on technical aspects is normally the dominating strand of information security research.

It is not possible to compare our findings on research topics with those put forward by McLaugklin and Gogan (2014), because they did not give a close characterisation of the research topics found. This serves to emphasise the important contribution made by our study; in particular, the categorisation of research questions allowed us to discuss the focus of earlier research efforts. We identified that most research carried out has had a management focus. Although many of these papers address risks with inter-organisational settings, few such studies have been carried out on the categories related to process, people, emergence, culture, and human factors. This means that we have limited knowledge on how these risks appear in day-to-day practice. From a practitioner's point of view, it means that limited findings are available on actual information security risks in inter-organisational collaboration, as well as proven safeguards. Consequently, more research is needed in the above-mentioned categories.

5.2 Maturity of inter-organisational information security research

The avenues for future research on inter-organisational information security were made even more specific when we added maturity as an analytical layer (Figure 3). Whilst the literature review presented by McLaugklin and Gogan (2014) did address inter-organisational information security research, it did not attempt to classify the maturity of information security research. Therefore, we can contribute to the field by pinpointing the maturity of this sub-field in relation to the research topics.

On a general level, we can conclude that most of the existing research on inter-organisational information security is descriptive, philosophical or theoretical. When measured using Grönlund's (2001) framework, this sub-field can be seen to be rather immature. For example, one surprising finding is the large share of descriptive, philosophical and theoretical research related to organisation design/strategy and governance. Research in these two areas has sought to address strategic and management decisions on inter-organisational information security. As discussed above, many of these studies address different types of risks within inter-organisational settings. Nonetheless, most of these studies lack a structured analysis of the presented cases (descriptive) or empirical evidence (philosophical/theoretical). Consequently, it is relevant to discuss the basis on which these risks are identified and the management frameworks suggested. Moreover, in light of this it becomes even more relevant to investigate which risks are actually present in inter-organisational settings.

Our analysis showed that half of the studies on inter-organisational information security published between 2009 and 2014 are either theoretical, descriptive or philosophical. This shows a change from papers published between 1990 and 2008, with an increase in the share of research devoted to theory generating and theory testing. Such a change can be attributed to a move towards greater maturity. Still, the proliferation of descriptive and non-empirical research has implications for both research and practice. From a research point of view we can conclude that, in addition to the research depicted on the left-hand side and bottom parts of Figure 2 (culture, people, emergence and human factors), there is a need to increase the maturity of research on organisation design/strategy and governance. In order to accomplish this, researchers need to combine empirical research with the explicit use of theories (theory testing) or ensure that empirical research is used for the development of theories on inter-organisational information security (theory generating). From a practical point of view, it is difficult to consider existing research results, such as management frameworks, because they have not been empirically validated. Consequently, we can offer less advice to practitioners than was the case in the previous section.

5.3 Types of research methods used

Our findings on types of research methods used in inter-organisational information security research extend the existing knowledge base. McLaugklin and Gogan (2014) presented an analysis of the research methods used in a small set of studies based on the Basket of Eight.

They found that a very limited number of research methods were employed. In principle, all inter-organisational studies identified were based on case studies or surveys; often they were used in combination in a mixed-method approach. As discussed above, our study is based on a broader set of papers, making it possible to provide a more detailed pattern of the research methods used. Our analysis shows that case studies and surveys are not the only research methods used; indeed, they are not even the most frequently used methods.

In total, we found that 11 different research methods were used for inter-organisational information security investigations and that the subjective/argumentative method is by far the most frequently used. For example, it has been the dominating research method in the study of governance and technology. This confirms our finding that a large part of inter-organisational information security research lacks empirical grounding. Whilst anecdotal data may be used, a subjective/argumentative research method does not make use of empirical data in a structured way. Based on our detailed analysis (see Appendix C), we can conclude that only a small number of studies have employed multi-method approaches (Brewer and Hunter, 1989); often these studies combined literature reviews with a research method for collecting empirical data. Even fewer studies used a mixed-method approach (Creswell, 2003). Hence, in this sub-field today, empirical data is often collected using just one research method.

When comparing our results with the information systems field in general (Mingers, 2003), we found both similarities and differences. We can conclude that, on an overall level, the number of research methods used is similar to that found in the information systems field in general. The most common research methods in the information systems field are case studies, interviews, observations and surveys. Similarly, we found that case studies, interviews and surveys are the most frequently used research methods for *empirical* investigations into inter-organisational information security. However, we only identified one study that was based on observations; in this case, it used quantitative data (passive observation and measurement). Siponen and Williams (2007) have put forward similar results when reviewing general information security research; however, they did not offer any evidence on the use of observation.

We cannot compare our findings of the widespread use of subjective/argumentative research methods with those put forward by Mingers (2003), because he did not include non-empirical research methods in his study. Yet again, our findings are similar to those presented by Siponen and Williams (2007); in both reviews, subjective/argumentative methods were found to be most frequently used. That said, we identified a smaller number than Siponen and Williams (2007) (44% compared with their 78%). With regard to this type of research method it is also worth noting that the method was often not made explicit, which makes it problematic to assess the research results. Thus, we can conclude that researchers in the sub-field of inter-organisational information security could be more explicit in their use of this type of research method, or at least in stating the point of departure for their logical arguments.

Mingers (2003) argued that research methods belong to certain paradigms, although the relationships are not always clear-cut. Dhillon and Backhouse (2001) argued along similar lines when using the framework put forward by Burell and Morgan (1979) to evaluate information security research. We can therefore conclude that a research method is based on a set of basic assumptions. Furthermore, given the skewed frequency of the research methods used, only a limited number of perspectives have been used to address inter-organisational information security. For example, we did not find any enquires that used critical theory and few studies appear to have used action research or design science. Consequently, critical and intervening research is rare. These findings are similar to the results put forward by Dhillon and Backhouse (2001) and Siponen and Williams (2007) on information security research in general.

We believe that our results have implications for the types of research methods that are used in future research on inter-organisational information security. They call for a broader use of research methods in order to approach the phenomenon from several perspectives. Moreover, we believe that it would be beneficial to increase the use of mixed-method (Creswell, 2003) or multi-method (Brewer and Hunter, 1989) approaches. Using more than one research method would allow us to acknowledge several perspectives through data triangulation when collecting empirical data.

5.4 The limitations of this study

In this study we have reported on the topics researched in the sub-field of inter-organisational information security, as well as the maturity of existing research and the research methods used. Naturally, the findings depend on our search strategy and on our selection of papers. We have been explicit with our selection of papers, which is based on searches in the ABI/Inform, EBSCO, SCOPUS and Web of Science databases. Of course, other search strategies are possible, such as that used by McLaugklin and Gogan (2014). Hence, we do not claim that we have identified all studies on inter-organisational information security; rather, we have used a good-sized sample from the relevant outlets.

The use of our analytical framework involves subjective judgment. It has not always been a straightforward task to classify papers into research topics or types of research methods. However, we have triangulated all of our classifications based on the individual analyses of the authors, which strengthens our findings. In addition, we have tried to make our analysis as explicit as possible by providing the complete classification of papers in Appendix C making it possible to scrutinise the analysis in detail.

6. Conclusion

The aim of this paper was to survey existing inter-organisational information security research in order to scrutinise the kind of knowledge that is currently available, and the way in which this knowledge has been brought about. To this end, we used the framework on information security system put forward by Kiely and Benzel (2006), the framework on types of research purpose by Grönlund (2001), together with an extended version of the framework on research methods laid out by Mingers (2003). We conclude that, with regard to scope, existing research has focused on a limited set of research topics; the main part of existing research has focused on management issues and technical solutions. This is an unwarranted omission on behalf of the research community and we call for more research into:

(a) how the characteristics of employees and non-staff affect inter-organisational information security (e.g. how employees'/non-staff's skills/awareness affect inter-organisational information security? What kind of additional information security skills/awareness are needed in an inter-organisational setting?)

(b) existing processes and how they are carried out in inter-organisational settings (e.g. is existing information security policies useable with regard to inter-organisational settings? How is employees'/non-staff's compliance with information security policies affected by inter-organisational collaborations?)

(c) how well technology supports employees and non-staff (e.g. is existing technology suitable for solving information security tasks in an inter-organisational setting? Do employees/non-staff carry out workarounds due to improper technological support?)

(d) the role that multiple cultures play in inter-organisational information security (e.g. what kind of imprints does inter-organisational collaboration make on an organisation's information security culture? What kind of conflicts occurs when different information security cultures meet in an inter-organisational collaboration?)

Furthermore, we conclude that an extensive part of research is descriptive, philosophical or theoretical. Thus, few studies combine theoretical work and empirical data. Thus, there is a need for more integrative studies that are empirically relevant; in other words, studies that employ sound theories as well as empirical data to investigate issues relating to inter-organisational information security or to develop theory based on empirical data. With regard to research methods, only a small repertoire of research methods has been extensively employed. The majority of the studies have employed a subjective/argumentative method, whilst a few cases have used a multi-method or mixed-method approach. Thus, we are in need of more methodologically ambitious studies that seek to explain, understand and predict inter-organisational information security issues. Taken together, this means that many topics have been researched to a limited extent and from a limited set of perspectives, if at all. This leads us to conclude that current inter-organisational information security research is quite immature.

Our findings suggest that future inter-organisational information security research should: (a) address a broader set of research topics, focusing especially on employees/non-staff and their use of processes and technology in inter-organisational settings, as well as on cultural aspects, which are lacking today; (b) focus more on theory generation or theory testing in order to increase the maturity of this sub-field; and (c) use a broader set of research methods as well as multi-method or mixed-method approaches. It would be particularly interesting to see future investigations that use critical or intervening approaches. So far, they have been used to a limited extent in inter-organisational information security research.

Acknowledgments
This research has been funded by the Swedish Civil Contingencies Agency

References

Abraham, S. "Information security behaviour: factors and research directions", *Americas Conference on Information Systems* 2011 Detriot, Michigan. AIS Electronic Library (AISeL), pp. Paper 462.

Al Kattan, I., Al Nunu, A. & Saleh, K. (2009), "A Stochastic Model for Improving Information Security in Supply Chain Systems", *International Journal of Information Systems and Supply Chain Management,* 2**,** pp. 35-50.

Ashford, W. (2015), "Supply chain an important part of information security, say experts" *ComputerWeekly.com.*

Backhouse, J., Hsu, C. W. & Silva, L. (2006), "Circuits of power in creating de jur standards: shaping an international information systems security standard", *MIS Quarterly,* 30**,** pp. 413-438.

Bahl, S., Wali, O. P. & Kumaraguru, P. "Information Security Practices Followed in the Indian Software Services Industry: An Exploratory Study", *Second Worldwide Cybersecurity Summit (WCS 2011)* 2011 London, UK. IEEE, pp. 1-2 June, 2011.

Bandyopadhyay, T., Jacob, V. & Raghunathan, S. (2010), "Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest", *Information Technology and Management,* 11**,** pp. 7-23.

Bandyopadhyay, T., Jacob, V. S. & Raghunathan, S. "Information Security Investment Strategies in Supply Chain Firms: Interplay Between Breach Propagation, Shared Information Assets and Chain Topology", *11th Americas Conference on Information Systems (AMCIS 2005)*, August 11-14, 2005 2005 Omaha, Nebraska, USA. AIS Electronic Library (AISeL), pp. Paper 456.

Bartol, N. (2014), "Cyber supply chain security practices DNA – Filling in the puzzle using a diverse set of disciplines", *Technovation,* 34**,** pp. 354-361.

Baskerville, R. (1993), "Information systems security design methods: Implications for information systems development ", *ACM Computing Surveys,* 25**,** pp.

Batten, L. & Castleman, T. "Securing Small Business - The Role of Information Technology Policy", *Australasian Conference on Information Systems 2005 (ACIS 2005)*, 2005 Sydney, Australia. AIS Electronic Library, pp. Paper 79.

Behara, R., Huang, C. D. & Hu, Q. "Extended-Enterprise Information Security: A Risk Propagation Framework for Information Supply Chains", *13th Americas Conference on Information Systems (AMCIS 2007)*, 2007 Keystone, Colorado. AIS Electronic Library (AISeL), pp. Paper 270.

Berghmans, P. & Van Roy, K. (2011), "Information Security Risks in Enabling e-Government: The Impact of IT Vendors", *Information Systems Management,* 28**,** pp. 284-293.

Brewer, J. D. & Hunter, A. (1989), *Multimethod Research: A Synthesis of Styles,* SAGE Publication, Newbury Park.

Burell, G. & Morgan, G. (1979), *Sociological paradigms and organisational analysis : elements of the sociology of corporate life,* Heinemann, London.

Chen, M.-K. & Wang, S.-C. (2010), "A hybrid Delphi-Bayesian method to establish business data integrity policy - A benchmark data center case study", *Kybernetes,* 39**,** pp. 800-824.

Chen, T.-Y., Chen, Y.-M., Wang, C.-B., Chu, H.-C. & Yang, H. (2007), "Secure resource sharing on cross-organization collaboration using a novel trust method", *Robotics and Computer-Integrated Manufacturing,* 23**,** pp. 421-435.

Cheng, J.-H. (2011), "Inter-organizational relationships and information sharing in supply chains", *International Journal of Information Management,* 31**,** pp. 374-384.

Cheng, Y. "Information Security Risk Assessment Model of IT Outsourcing Managed Service", *2012 International Conference on Management of e-Commerce and e-Government*, 20-21 October, 2012 2012 Beihing, China. IEEE Xplore, pp. 116-121.

Cheon, M. J. & Grover, V. (1993), "The evolution of empirical research in IS. A Study in IS maturity", *Information & Management,* 24**,** pp. 107-119.

Cherdantseva, Y., Rana, O. & Hilton, J. (2011), "Security Architecture in a Collaborative De-Perimeterised Environment: Factors of Success" *ISSE Securing Electronic Business Processes 2011.* Prague.

Cook, N., Shrivastava, S. & Wheater, S. (2003), "Middleware Support for Non-repudiable Transactional Information Sharing between Enterprises", in Stefani, J.-B., Demeure, I. and Hagimont, D. (eds.) *Distributed Applications and Interoperable Systems - 4th IFIP WG6.1 International Conference, DAIS 2003, Paris, France, November 17-21, 2003.* Springer, Berlin, pp 125-132.

Creswell, J. W. (2003), *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches,* Sage Publications, London.

Cunha, C. R., Gomes, J. P. & Morais, E. P. (2013), "An agent-based security framework for cooperative business networks" *20th International Business Information Management Association Conference.* Kuala Lumpur, Malaysia.

Davidson, D., Shankles, S. & Hamilton, B. A. (2013), "We Cannot Blindly Reap the Benefits of a Globalized ICT Supply Chain!", *Crosstalk,* March/April**,** pp. 4-7.

Deane, J. K., Ragsdale, C. T., Rakes, T. R. & Rees, L. P. (2009), "Managing supply chain risk and disruption from IT security incidents", *Operations Management Research,* 2**,** pp. 4-12.

Deane, J. K., Rees, C. & Baker, W. H. (2010), "Assessing the information technology security risk in medical supply chains", *International Journal of Electronic Marketing and Retailing,* 3**,** pp. 145-155.

Denning, P. J. (1992), ""Passwords"", *American Scientist,* 80**,** pp. 117-120.

Desai, R. & Mcgee, R. W. (2010), "Is Outscourced Data Secure?", *The CPA Journal,* January**,** pp. 8-11.

Dhillon, G. (2007), *Principles of information systems security: text and cases,* Wiley Inc, Hoboken, NJ.

Dhillon, G. & Backhouse, J. (2001), "Current directions in IS security research: towards socio-organisational perspectives", *Information Systems Journal,* 11**,** pp.

Djordjevic, I., Dimitrakos, T., Romano, N., Mac Randal, D. & Ritrovato, P. (2007), "Dynamic security perimeters for inter-enterprise service integration", *Future Generation Computer Systems,* 23**,** pp. 633-657.

Dommun, M. R. (2008), "Multi-level information system security in outsourcing domain", *Business Process Management Journal,* 14**,** pp. 849-857.

Doomun, M. R. (2008), "Multi-level information system security in outsourcing domain", *Business Process Management Journal,* 14**,** pp. 849-857.

Durowoju, O. A., Chan, H. K. & Wang, X. (2011), "The impact of security and scalability of cloud service on supply chain performance", *Journal of Electronic Commerce Research,* 12**,** pp. 243-256.

Dwivedi, Y. K. & Kuljis, J. (2008), "Profile of IS research published in the European Journal of Information Systems", *European Journal of Information Systems,* 17**,** pp. 678-693.

Eigeles, D. (2006), "Intelligent authentication, authorization, and administration (I3A)", *Information Management & Computer Security,* 14**,** pp. 5-23.

Fabian, B., Kunz, S., Müller, S. & Günther, O. (2013), "Secure federation of semantic information services", *Decision Support Systems,* 55**,** pp. 385-398.

Flinders, K. 2013. The lawyer, the supplier and the consultant on outsourcing security. *ComputerWeekly.com*, 20 February, 2013.

Gajanayake, R., Iannella, R. & Sahama, T. (2011), "Sharing with Care - An Information Accountability Perspective", *IEEE Internet Computing,* 15**,** pp. 31-38.

Gal-Or, E. & Ghose, A. (2005), "The Economic Incentives for Sharing Security Information", *Information Systems Research,* 16**,** pp. 186-208.

Galliers, R. (1992), *Information Systems Research: Issues, Methods and Practical Guidelines,* Blackwell Scientific Publications, Oxford.

Gomes, E., Barnes, B. R. & Mahmood, T. (In press), "A 22 year review of strategic alliance research in the leading management journals", *International Business Review,* Available online 13 April 2014**,** pp.

Goodman, S. E. & Ramer, R. (2007), "Identify and Mitigate the Risks of Global IT Outsourcing", *Journal of Global Information Technology Management,* 10**,** pp. 1-6.

Gregor, S. & Jones, D. (2007), "The Anatomy of a Design Theory", *Journal of the Association of Information Systems,* 8**,** pp. 312-335.

Gritzalis, S., Yannacopoulos, A. N., Lambrinoudakis, C., Hatzopoulos, P. & Katsikas, S. K. (2007), "A probabilistic model for optimal insurance contracts against security risks and privacy violation in IT outsourcing environments", *International Journal of Information Security,* 6**,** pp. 197-211.

Grönlund, Å. (2001), "State of the art in e-Gov research - a survey", in Traunmüller, R. (ed.) *Electronic Government - Third International Conference, EGOV 2004.* Springer, Berlin Heidelberg, pp 178-185.

Grönlund, Å. (2003), "Emerging Electronic Infrastructures - Exploring Democratic Components", *Social Science Computer Review,* 21**,** pp. 55-72.

Grönlund, Å. & Andersson, A. (2006), "e-Gov Research Quality Improvements Since 2003: More Rigor, but Research (Perhaps) Redefined", in *Electronic Government - 5th International Conference, EGOV 2006.* Springer, Berlin, pp 1-12.

Gutiérrez, C., Rosado, D. G. & Fernández-Medina, E. (2009), "The practical application of a process for eliciting and designing security in web service systems", *Information and Software Technology,* 51**,** pp. 1712-1738.

Hao, J. & Cai, W. "Trusted Block as a Service: Towards Sensitive Applications on the Cloud", *IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2011)*, 16-18 November, 2011 2011 Changsha. IEEE, pp. 73-82.

Hevner, A. R., March, S. T., Park, J. & Ram, S. (2004), "Design Science in Information Systems Research", *MIS Quarterly,* 28**,** pp. 75-105.

Huang, C. D., Behara, R. S. & Hu, Q. (2008), "Managing Risk Propagation in Extended Enterprise Networks", *IT Professional,* 10**,** pp. 14-19.

ISO 27010 (2012), "ISO/IEC 27010:2012, Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications". International Organization for Standardization (ISO).

Johnson, E. M. (2008), "Information Risk of Inadvertent Disclosure: An Analysis of File-Sharing Risk in the Financial Supply Chain", *Journal of Management Information Systems,* 25**,** pp. 97-123.

Julisch, K. & Hall, M. (2010), "Security and Control in the Cloud", *Information Security Journal: A Global Perspective,* 19**,** pp. 299-309.

Karlsson, F., Kolkowska, E., Hedström, K. & Frostenson, M. (2015), "Inter-organisational information sharing – between a rock and a hard place" *HAISA 2015.*

Kayem, A. V. D. M., Martin, P. & Akl, S. G. "Efficient Enforcement of Dynamic Cryptographic Access Control Policies for Outsourced Data", *Information Security South Africa (ISSA), 2011*, 15-17 August, 2011 2011 Johannesburg, South Africa. IEEE Xplore, pp. 1-8.

Kearney, P. (2005), "Message level security for web services", *Information Security Technical Report,* 10**,** pp. 41-50.

Khalfan, A. M. (2004), "Information security considerations in IS/IT outsourcing projects:a descriptive case study of two sectors", *International Journal of Information Management,* 24**,** pp. 29-42.

Khidzir, N. Z., Arshad, N. H. H. & Mohamed, A. "Information Security Risk Management: An Empirical Study on the Importance and Practices in ICT Outsourcing", *International Symposium in Information Technology (ITSim), 2010* 15-17 June, 2010 2010a Kuala Lumpur. IEEE, pp. 1610-1615.

Khidzir, N. Z., Mohamed, A. & Arshad, N. H. "Information Security Risk Factors: Critical Threats and Vulnerabilities in ICT Outsourcing", *International Conference on Information Retrieval & Knowledge Management, (CAMP 2010)*, 17-18 March, 2010 2010b Shah Alam, Selangor. IEEE, pp. 194-199.

Kiely, L. & Benzel, T. V. (2006), "Systemic Security Management", *IEEE Secuirty & Privacy,* 4**,** pp. 74-77.

Kling, R. (1977), "The Organizational Context of User-Centered Software Designs", *MIS Quarterly,* 1**,** pp. 41.

Kokolakis, S. A. & Kiountouzis, E. A. (2000), "Achieving Interoperability in a Multiple-Security-Policies Environment", *Computers & Security,* 19**,** pp. 267-281.

Kunnathur, A. S. & Vaithainathan, S. "Information Security Issues In Global Supply Chain", *IMR Conference 2008*, December 22-24, 2008 2008 Bangalore, India. pp.

Kunz, S., Fabian, B., Marx, D. & Müller, S. "Engineering Policies for Secure Interorganizational Information Flow", *15th IEEE International Enterprise Distributed Object Computing Conference Workshops*, 29 August-2 September, 2011 2011 Helsinki, Finland. IEEE Xplore, pp. 438-447.

Lanjuan, L. "SCM Security Solution Based on SSL Protocol", *IEEE International Conference on Service Operations and Logistics, and Informatics, 2006 (SOLI '06)* 21-23 June, 2006 2006 Shanghai, China. IEEE, pp. 814-817.

Lebek, B., Uffen, J. & Breitner, M. H. "Employees' Information Security Awareness and Behavior: A Literature Review", *The 46th Annual Hawaii International Conference on System Sciences (HICSS 2013)*, 2013 Grand Wailea, Maui, Hawaii. IEEE Xplore, pp.

Li, L., Qian, G. & Qian, Z. (2013), "Do partners in international strategic alliances share resources, costs, and risks?", *Journal of Business Research,* 66**,** pp. 489-498.

Li, X. & Chandra, C. (2008), "Toward a secure supply chain: A system's perspective", *Human Systems Management,* 27**,** pp. 73-86.

Li, Y. & Ding, X. "Protecting RFID Communications in Supply Chains", in Deng, R. and Samarati, P., eds. *2nd ACM symposium on Information, computer and communications security (ASIACCS '07)*, 2007. ACM Digital Library, pp. 234-241.

Lu, T., Guo, X., Xu, B., Zhao, L., Peng, Y. & Yang, H. (2013), "Next Big Thing in Big Data: the Security of the ICT Supply Chain" *International Conference on Social Computing (SocialCom), 2013.* Wasinghton DC, USA: IEEE Xplore Digital Library.

Mao, T., Williams, J. & Sanchez, A. "Interoperable Internet Scale Security Framework for RFID Networks", *24th International Conference on Conference: Data Engineering Workshop*, 2008. IEEE Xplore, pp. 94-99.

Mclaughlin, M.-D. & Gogan, J. "INFOSEC in a Basket, 2004-2013", *The 20th Americas Conference on Information Systems (AMCIS 2014)*, 2014 Savannah, Georgia, USA. AIS Electronic Library (AISeL), pp. ISSecutity paper 6.

Mingers, J. (2003), "The paucity of multimethod research: a review of the information systems literature", *Information Systems Journal,* 13**,** pp. 233-249.

Moradian, E. (2008), "Integrating Web Services and Intelligent Agents in Supply Chain for Securing Sensitive Messages", in Lovrek, I., Howlett, R. J. and Jain, L. C. (eds.) *Knowledge-Based Intelligent Information and Engineering Systems - 12th International Conference, KES 2008, Zagreb, Croatia, September 3-5, 2008, Proceedings, Part III.* Springer, Berlin, pp 771-778.

Nassimbeni, G. & Sartor, M. (2012), "Security risks in service offshoring and outsourcing", *Industrial Management & Data Systems,* 112**,** pp. 405-440.

Palvia, P., Leary, D., Mao, E., Midha, V. & Pinjani, P. (2004), "Research Methodologies in MIS: An Update", *Communications of the Association for Information Systems,* 14**,** pp. Paper 24.

Pemble, M. (2004), "Transferring business and support functions: the information security risks of outsourcing and off-shoring", *Computer Fraud & Security,* 2004**,** pp. 5-9.

Peng, Y., Song, Y., Ju, H. & Wang, Y. (2014), "OB4LAC: An Organization-based Access Control Model for E-government System", *Applied Mathematics & Information Sciences,* 8**,** pp. 1467-1474.

Power, R. & Forte, D. (2005), "Outsourced or Outsmarted?", *Computer Fraud & Security,* 2005**,** pp. 17-19.

Pricewaterhousecoopers (2010), "Information Security Breaches Survey 2010 - Technical Report". PriceWaterhouseCoopers.

Robertson, C. J., Lamin, A. & Livanis, G. (2010), "Stakeholder Perceptions of Offshoring and Outsourcing: The Role of Embedded Issues", *Journal of Business Ethics,* 95**,** pp. 167-189.

Sandhu, R., Ranganathan, K. & Zhang, X. "Secure Information Sharing Enabled by Trusted Computing and PEI Models", *2006 ACM Symposium on Information, computer and communications security*, 2006 Taipei, Taiwan. ACM, pp. 2-12.

Santos-Pereira, C., Augusto, A. B., Cruz-Correia, R. & Correia, M. E. (2013), "A secure RBAC mobile agent access control model for Healthcare Institutions", in Rodrigues, P. P., Pechenizkiy, M., Gama, J., Correia, R. C., Liu, J., Traina, A., Lucas, P. and Soda, P. (eds.) *2013 IEEE 26th International Symposium on Computer-Based Medical Systems (CBMS).* IEEE Xplore Digital Library, Porto, Portugal, pp 349-354.

Schlaak, B., Dynes, S., Kolbe, L. M. & Schierholz, R. "Managing of Information Systems Risks in Extended Enterprises: The Case of Outsourcing", *14th Americas Conference on Information Systems (AMCIS 2008)*, 2008 Toronto, Ontario, Canada. AIS Electronic Library (AISeL), pp. Paper 280.

Schutt, R. K. (2001), *Investigating the social world: The process and practice of research,* Pine Forge Press, Thousand Oaks, CA.

Shih, S. C. & Wen, H. J. (2005), "Integrated e-enterprise security design and implementation: a case study of e-service in supply chain management", *International Journal of Electronic Business,* 3**,** pp. 154-173.

Shing, M.-L., Shing, C.-C., Chen, H. L. & Lee, H. (2007), "Security Modeling on the Supply Chain Networks", *Systems, Cybernetics and Informatics,* 5**,** pp. 53-58.

Shittu, A. J. K., Ahlan, A. R. & Osman, W. R. S. (2012), "Information security and mutual trust as determining factors for information technology outsourcing success", *African Journal of Business Management,* 6**,** pp. 103-110.

Shu, T., Maccarthy, B. L., Wang, S., Lai, K. K. & Xie, C. (2007), "AVE-based collaboration and information transmission security" *The Sixth Wuhan International Conference on E-Business.* Wuhan, China.

Siponen, M. (2005a), "Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods", *Information and Organization,* 15**,** pp. 339-375.

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

Siponen, M. & Willison, R. "A critical assessment of IS security research between 1990–2004", *The 15th European Conference on Information Systems (ECIS 2007)*, 2007 St. Gallen; Switzerland. AIS Electronic Library (AISeL), pp. 1551–1559.

Smith, G. E., Watson, K. J., Baker, W. H. & Pokorski Ii, J. A. (2007), "A critical balance: collaboration and security in the IT-enabled supply chain", *International Journal of Production Research,* 45**,** pp. 2595-2613.

Su, Z., Biennier, F. & Ouedraogo, W. F. (2012), "A governance framework for mitigating risks and uncertainty in collaborative business processes", in Camarinha-Matos, L. M., Xu, L. and Afsarmanesh, H. (eds.) *Collaborative Networks in the Internet of Services - 13th IFIP WG 5.5 Working Conference on Virtual Enterprises, PRO-VE 2012, Bournemouth, UK, October 1-3, 2012.* Springer, Berlin, pp 667-674.

Thalmann, S., Bachlechner, D. & Maier, R. "Security management in cross-organizational settings: a design science approach", *33rd International Conference on Information*

Systems (ICIS 2012), 2012 Orlando, FL, USA. AIS Electronic Library (AISeL), pp. Paper 41.

Thomas, C. (2012), "Practical approaches to supply chain continuity: new challenges and timeless principles", in Khan, O. and Zsidisin, G. A. (eds.) *Handbook for supply chain management: case studies, effective practices and emerging trends.* J. Ross Publishing, Fort Lauderdale, pp

Tomkins, C. (2001), "Interdependencies, trust and information in relationships, alliances and networks", *Accounting, Organizations and Society,* 26**,** pp. 161-191.

Vaidyanathan, G., Devaraj, S. & D'arcy, J. (2012), "Does Security Impact E-procurement Performance? Testing a Model of Direct and Moderated Effects", *Decision Sciences Journal,* 43**,** pp. 437-458.

Van Veenstra, A. F. & Ramilli, M. (2011), "Exploring Information Security Issues in Public Sector Inter-organizational Collaboration", in Janssen, M., Scholl, H. J., Wimmer, M. A. and Tan, Y.-H. (eds.) *Electronic Government - 10th IFIP WG 8.5 International Conference, EGOV 2011, Delft, The Netherlands, August 28 – September 2, 2011. Proceedings.* Springer, Berlin, pp 355-366.

Vlissidis, P. (2012), "The security risk of the supply chain", *SC Magazine***,** pp.

Wangwe, C. K., Eloff, M. M. & Venter, L. (2012), "A sustainable information security framework for e-Government – case of Tanzania", *Technological and Economic Development of Economy,* 18**,** pp. 117-131.

Wei, J., O'connell, J. & Loho-Noya, M. (2010), "Information Technology Offshore Outsourcing Security Risks and Safeguards", *Journal of Information Privacy & Security,* 6**,** pp. 29-46.

Xue, H. & Li, J. "A Method for Information Protection in Collaborative Assembly Design", *Ninth International Conference on Computer Aided Design and Computer Graphics (CAD/CG 2005)*, 7-10 December, 2005 2005 Hong Kong. IEEE, pp.

Yu, B., Yang, L., Chen, S. H. & Ma, L. R. (2013), "A Review of Information Flow Control in Composite Services", *Applied Mechanics and Materials,* 336-338**,** pp. 2348-2353.

Yuan, H., Chen, G., Wu, J. & Xiong, H. (2009), "Towards controlling virus propagation in information systems with point-to-group information sharing", *Decision Support Systems,* 48**,** pp. 57-68.

Yulin, D., Shiying, L. & Yi, L. "Information Relevance Management Model – A New Strategy in Information Security Management in the Outsourcing Industry", *5th IEEE/ACIS International Conference on Computer and Information Science*, 10-12 July, 2006 2006 Honolulu. IEEE, pp. 433-438.

Zhang, L., Zhou, H., Kong, R. & Yang, F. "An Improved Approach to Security and Privacy of RFID Application System", *2005 International Conference on Wireless Communications, Networking and Mobile Computing*, 23-26 September, 2005 2005. IEEE, pp. 1195-1198.

Biographical Details:

Fredrik Karlsson is Professor in Informatics at Örebro University, Sweden. He has previously held a research position at University of Skövde. He received his PhD in Information Systems Development from Linköping University. His research on information security, tailoring of systems development methods, system development methods as reusable assets, CAME-tools, method rationale and electronic government has appeared in a variety of information systems journals and conferences. He is currently research leader of the research environment Centre for Empirical Research on Information Systems (CERIS).

Ella Kokowska is Assistant Professor in Informatics at Örebro University. Her main area of interest is information security with focus on end-users' security behaviours. Especially she has studied how users' professional values influence their behaviours with respect to information security policies and guidelines. She has also studied how ISPs should be designed to reflect current professional practice. Recently Kolkowska has started to study privacy in the context of smart homes technologies and elderly care.

Frans Prenkert is Associate Professor in industrial marketing and member or the research group INTERORG at Örebro University School of Business. His research concerns inter-organizational processes and the networked economy. He has published in journals such as Journal of Business Research, Industrial Marketing Management, European Journal of Marketing and Journal of Cleaner Production.

Appendix A

Table A1. Search criteria and search results

	Number of papers			
Search criteria	**ABI/Inform**	**EBSCO**	**SCOPUS**	**Web of Science**
Information security AND Activity coordination	0	0	0	0
Information security AND Activity linking	0	0	0	0
Information security AND B2B	2	10	10	3
Information security AND Business collaboration	0	1	1	2
Information security AND Business relationships	1	3	3	0
Information security AND Buyer seller relationships	1	2	2	1
Information security AND Customer development	0	0	0	0
Information security AND Customer interaction	0	0	0	0
Information security AND Customer relationship management	4	9	9	4
Information security AND Enterprise collaboration	0	45	45	0
Information security AND Inter-enterprise	0	17	17	2
Information security AND Inter-organisational	2	9	9	1
Information security AND Interoperability	12	96	96	49
Information security AND Merge company	0	1	1	0
Information security AND Mutual adaptation	0	0	0	0
Information security AND Organisational collaboration	0	47	47	0
Information security AND Outsourcing	35	114	114	43
Information security AND Resource interaction	0	29	29	0
Information security AND Resource interfaces	0	0	0	0
Information security AND Resource integration	0	1	1	1
Information security AND Resource pooling	1	0	0	1
Information security AND Sourcing strategies	2	0	0	0
Information security AND Strategic alliances	0	1	1	1
Information security AND Supplier development	0	0	0	1
Information security AND Supplier re-organisation	0	0	0	0
Information security AND Supply chain	87	82	82	27
Information security AND Supply network	0	1	1	0
Sum	*147*	*126*	*468*	*136*

Appendix B

Table B1. 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 an insight 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).
Literature review	This category refers to the contribution to knowledge through a systematic account of existing research publications in a research area.
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 of the researcher. This category is an extension of ethnography (Mingers, 2003).
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 in order to identify “the occurrence of specific categories or terms” (Mingers, 2003). The analysis can either be carried out using predefined categories or in an “interpretive manner, recognizing the role of the analyst on doing this” (Mingers, 2003).
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.
Subjective/argumentative	This category refers to the contribution to knowledge through logical arguments based on: a) own experiences, and/or b) textual analysis to discover the underlying meaning of a body of text. The arguments may not necessarily be based on any particular theory or implicit theory.
Survey, questionnaire, or instrument	This category refers to the contribution to knowledge through a pre-structured set of questions, regardless of the technique 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.
Systems engineering	This category refers to the contribution to knowledge through developing an IT artefact or parts thereof. Such research consists of build-and-evaluate loops and the primary goal is system design. It sometimes overlaps with Action research and Design science but does not have an explicit use of design principles, and does not use organisational intervention to evaluate the artefact. Hence, this research does not contribute to organisational development.

Appendix C

Table C1. Detailed analysis

Author(s)	**Research topic**	**Type of research purpose**	**Research method**
Bahl et al. (2011)	Organisation design/strategy	Theory generating	Interviews, literature review, qualitative content analysis, survey
Bandyopadhyay et al. (2005)	Organisation design/strategy	Theoretical	Subjective/argumentative
Bandyopadhyay et al. (2010)	Organisation design/strategy	Theoretical	Subjective/argumentative
Bartol (2014)	Governance	Descriptive	Subjective/argumentative
Batten and Castleman (2005)	Governance	Theory generating	Survey
Behara et al. (2007)	Organisation design/strategy	Theoretical	Subjective/argumentative
Berghmans and van Roy (2011)	Organisation design/strategy	Theory generating	Case study, interviews, literature review, survey
Chen et al. (2007)	Technology	Theoretical	Subjective/argumentative, simulation
Chen and Wang (2010)	Organisation design/strategy	Theory generating	Case study, interviews, literature review
Cheng (2012)	Governance	Theoretical	Subjective/argumentative, simulation
Cook et al. (2003)	Technology	Theoretical	Subjective/argumentative
Davidson et al. (2013)	Organisation design/strategy	Philosophical	Subjective/argumentative
Deane et al.	Governance	Philosophical	Subjective/argumentative

(2009)			
Deane et al. (2010)	Organisation design/strategy	Descriptive	Simulation, survey
Desai and McGee (2010)	Organisation design/strategy	Descriptive	Interviews
Djordjevic et al. (2007)	Architecture	Theory testing	Systems engineering
Doomun (2008)	Governance	Philosophical	Literature review, subjective/argumentative
Durowoju et al. (2011)	Governance	Theoretical	Subjective/argumentative
Eigeles (2006)	Architecture	Theoretical	Subjective/argumentative
Fabian et al. (2013)	Architecture	Theory testing	Design science
Gajanayake et al. (2011)	Enabling and support	Theoretical	Subjective/argumentative
Gritzalis et al. (2007)	Governance	Theoretical	Subjective/argumentative, Simulation
Gutiérrez et al. (2009)	Process	Theory generating	Case study
Hao and Cai (2011)	Technology	Theoretical	Subjective/argumentative
Huang et al. (2008)	Organisation design/strategy	Theoretical	Subjective/argumentative
Johnson (2008)	Emergence	Theory testing	Passive observation and measurement
Julisch and Hall (2010)	Governance	Philosophical	Subjective/argumentative
Al Kattan et al. (2009)	Governance	Theoretical	Subjective/argumentative
Kayem et al. (2011)	Technology	Theory testing	Systems engineering
Kearney (2005)	Enabling and support	Theoretical	Subjective/argumentative
Khalfan (2004)	Organisation design/strategy	Descriptive	Case study, interviews, survey
Khidzir et al. (2010b)	Organisation design/strategy	Descriptive	Survey
Khidzir et al. (2010a)	Organisation design/strategy	Theory testing	Survey
Kokolakis and Kiountouzis (2000)	Governance	Theoretical	Subjective/argumentative
Kunz et al. (2011)	Enabling and support	Theory testing	Case study, interviews
Lanjuan (2006)	Technology	Philosophical	Subjective/argumentative
Li and Chandra (2008)	Governance	Theoretical	Subjective/argumentative
Li and Ding (2007)	Technology	Theory testing	Systems engineering
Lu et al. (2013)	Governance	Theoretical	Subjective/argumentative
Mao et al. (2008)	Technology	Theoretical	Subjective/argumentative
Moradian (2008)	Architecture	Theoretical	Subjective/argumentative
Nassimbeni and	Governance	Theory testing	Design science

Sartor (2012)			
Pemble (2004)	Organisation design/strategy	Philosophical	Subjective/argumentative
Peng et al. (2014)	Enabling and support	Theoretical	Systems engineering
Power and Forte (2005)	Organisation design/strategy	Philosophical	Subjective/argumentative
Robertson et al. (2010)	Organisation design/strategy	Theory testing	Survey
Sandhu et al. (2006)	Technology	Theoretical	Subjective/argumentative
Santos-Pereira et al. (2013)	Technology	Theoretical	Subjective/argumentative
Schlaak et al. (2008)	Governance	Theory generating	Interviews, literature review
Shih and Wen (2005)	Governance	Theory generating	Case study
Shing et al. (2007)	Governance	Theoretical	Subjective/argumentative
Shittu et al. (2012)	Organisation design/strategy	Theory generating	Interviews
Shu et al. (2007)	Technology	Theoretical	Subjective/argumentative
Smith et al. (2007)	Organisation design/strategy	Theoretical	Subjective/argumentative
Su et al. (2012)	Governance	Theoretical	Subjective/argumentative
Thalmann et al. (2012)	Governance	Descriptive	Design science [(a)]
Vaidyanathan et al. (2012)	Organisation design/strategy	Theory testing	Survey
van Veenstra and Ramilli (2011)	Process	Descriptive	Case study, interviews
Wangwe et al. (2012)	Architecture	Theory testing	Action research, literature review
Wei et al. (2010)	Organisation design/strategy	Theory generating	Literature review, interviews
Xue and Li (2005)	Technology	Descriptive	Simulation
Yuan et al. (2009)	Technology	Theory testing	Subjective/argumentative, simulation
Yulin et al. (2006)	Governance	Theoretical	Subjective/argumentative
Zhang et al. (2005)	Technology	Theoretical	Subjective/argumentative

[(a)] *This is a research-in-progress paper that only contains certain descriptive parts of the research project.*

Table C2. Papers that we have been unable to analyse

Author(s)	**Reason why the analysis was not carried out**
Cunha et al. (2013)	Unable to get a copy of the paper
Yu et al. (2013)	Unable to get a copy of the paper