Received 30 May 2014
Revised 25 August 2014
23 September 2014
Accepted 2 October 2014

Information security culture – state-of-the-art review between 2000 and 2013

Fredrik Karlsson
CERIS, Department of Informatics, Örebro University, Örebro, Sweden, and
Joachim Åström and Martin Karlsson
Political Science Department, Örebro University, Örebro, Sweden

Abstract

Purpose – The aim of this paper is to survey existing information security culture research to scrutinise the kind of knowledge that has been developed and the way in which this knowledge has been brought about.

Design/methodology/approach – Results are based on a literature review of information security culture research published between 2000 and 2013 (December).

Findings – This paper can conclude that existing research has focused on a broad set of research topics, but with limited depth. It is striking that the effects of different information security cultures have not been part of that focus. Moreover, existing research has used a small repertoire of research methods, a repertoire that is more limited than in information systems research in general. Furthermore, an extensive part of the research is descriptive, philosophical or theoretical – lacking a structured use of empirical data – which means that it is quite immature.

Research limitations/implications – Findings call for future research that: addresses the effects of different information security cultures; addresses the identified research topics with greater depth; focuses more on generating theories or testing theories to increase the maturity of this subfield of information security research; and uses a broader set of research methods. It would be particularly interesting to see future studies that use intervening or ethnographic approaches because, to date, these have been completely lacking in existing research.

Practical implications – Findings show that existing research is, to a large extent, descriptive, philosophical or theoretical. Hence, it is difficult for practitioners to adopt these research results, such as frameworks for cultivating or assessment tools, which have not been empirically validated.

Originality/value – Few state-of-the-art reviews have sought to assess the maturity of existing research on information security culture. Findings on types of research methods used in information security culture research extend beyond the existing knowledge base, which allows for a critical discussion about existing research in this sub-discipline of information security.

Keywords Information security, Literature review, Organizational culture, Information security climate, Information security culture, State-of-the-art review

Paper type Literature review

1. Introduction

Organisations are coming to rely more and more on information and information systems; little wonder then, that information security has made it to the top of the

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

Information & Computer Security
Vol. 23 No. 3, 2015
pp. 246-285
© Emerald Group Publishing Limited
2056-4961
DOI 10.1108/ICS-05-2014-0033

agenda for practitioners. Information security breaches can lead to economic losses as well as negative effects on an organisation's reputation, goodwill and trust (Hoffer and Straub, 1989). Extensive research has been carried out into the development of top-class technology tools to secure and safeguard critical information assets (Siponen and Willison, 2007; Siponen and Oinas-Kukkonen, 2007). However, as technologies evolve, these tools may not be enough (Siponen *et al.*, 2008). There is, however, information security research that concentrates specifically on understanding and improving the use of administrative procedures to safeguard information assets (Dhillon and Torkzadeh, 2006; Stanton *et al.*, 2005; Bulgurcu *et al.*, 2010; Hedström *et al.*, 2011; Siponen *et al.*, 2007). Currently, organisations face an uphill battle in attempting to define administrative procedures for every possible security risk situation. Hence, there is a need to consider the mindset of employees with regard to information security.

Information security cultures in organisations have been on the research agenda since the start of this century (Schlienger and Teufel, 2002; Kolkowska, 2011; Vroom and von Solms, 2004; Da Viega and Eloff, 2010; Furnell, 2007; Connolly, 2000; von Solms, 2000). Even though scholars within the information security field have defined "information security culture" in slightly different ways (Dhillon, 1997; Da Viega and Eloff, 2010; Ilvonen, 2011; Schlienger and Teufel, 2002), there seems to be a common understanding that it consists of a shared pattern of values, mental models and activities that are traded among an organisation's employees over time, affecting information security. Despite the importance of this topic, there is a lack of critical discussion on the maturity of state-of-the-art information security culture research. Maturity can be assessed by charting the nature of research (Grönlund, 2001). A scientific field or subfield such as information security culture usually has a shared study object, as well as "a set of theories that can be used to understand the general conditions of the field" (Grönlund and Andersson, 2006). Hence, research that focuses on theory generating and testing would indicate a more mature field. On the other hand, an emphasis on pure description and case storytelling would signal a less mature field.

Against this backdrop, the aim of this paper is to survey existing information security culture research to scrutinise the kind of knowledge that has been developed, and the way in which this knowledge has been brought about. To the best of our knowledge, few studies have investigated existing research on information security culture (Connolly and Lang, 2013, 2012; Chang and Lin, 2007; Malcolmson, 2009). Furthermore, these reviews have had a specific focus; for example, to integrate models of national, organisational and security cultures. Hence, they do not contribute to the critical discussion on the maturity of information security culture research. We therefore pose the following research questions (RQs):

RQ1. What kinds of topics relating to information security culture have been investigated?

RQ2. Which theories have an influence on information security culture research?

RQ3. What types of information security culture research have been undertaken?

RQ4. What kinds of research methods dominate information security culture research?

Our results are based on a literature review of information security culture research published between 2000 and 2013. The study is based on a gross list of articles that initially consisted of 367 research papers (including duplicates), of which, finally, 72 papers were chosen for analysis (more details follows in the Research section). Our up-to-date and systematic literature review complements existing literature studies of information security culture. We have also been able to discuss the focus of earlier research efforts and to reference the disciplines that have influenced research on information security culture. Moreover, we have discussed the maturity of this research by assessing the different types of research that have been carried out to date and the types of research methods that are most prominent in existing studies.

This paper is structured as follows. Following this introduction, Section 2 describes existing literature reviews on information security culture. The Section 3 presents the research method adopted for our literature review. In Section 4, we present the results of our review. We first identify the topics relating to information security culture that are investigated in existing research. We also present the theories that have influenced research on these topics. Second, we present our findings on the types of information security culture research that have been carried out and the research methods used. This information forms the basis for a discussion of their impact on information security culture research and practice. We end the paper with a short conclusion.

2. Related research

Despite the fact that information security culture has been on the research agenda for quite some time, relatively few literature reviews have offered an overview of existing research (Connolly and Lang, 2013, 2012; Chang and Lin, 2007; Malcolmson, 2009). Of course, it is possible to find other literature reviews in the field of information security (Dhillon and Backhouse, 2001; Martins and Dos Santos, 2010; Abraham, 2011; Siponen and Willison, 2007). However, these studies have not focused on information security culture, in particular. For example, Martins and Dos Santos (2010) focused on methods designed to create information security, and Abraham (2011) addressed factors that influence employees' information security behaviour in organisations. Dhillon and Backhouse (2001) assessed information security research, in general, by using the framework put forward by Burrell and Morgan (1979) for their analysis. They concluded that, overall, information security literature was dominated by a "technical and functionalist preconception". Siponen and Willison (2007) analysed 1,280 information security papers published between 1990 and 2004 in terms of theories, research methods and research topics. They concluded that approximately 81 per cent of the investigated papers contained no theory, and that approximately 78 per cent of the papers could be categorised as subjective-argumentative in terms of the research method. In addition, although they identified a broad range of research topics, 14 of these topics made up 71 per cent of all the articles. As a result, they argued that information security research was theoretically underdeveloped and that there was a "need for theoretically grounded research that uses empirical methods including, for example, surveys, case studies and actions research". Consequently, one can conclude that, at that time, researchers rarely exploited the concepts of information security culture.

Chang and Lin (2007) presented a literature review as part of their work to develop a model of how organisational culture influences the effectiveness of information security management. Consequently, they focused more on the concept of organisational culture, directing their review towards organisational science literature. They did not attempt to provide a broad perspective on current research directions and research methods. In addition, they provided few details on how their review of existing research was carried out.

Malcolmson (2009) explored existing definitions of (information) security culture and ways of measuring culture. She concluded that there is no accepted definition of (information) security culture or an accepted way of measuring it. However, it is difficult to assess how these conclusions were reached because, again, few details about the literature review were revealed.

A literature review by Connolly and Lang (2013) aimed to integrate models of national, organisational and information security culture as well as behavioural theories to "identify factors that promote security-cautious behaviour of employees within organisational settings". As a result, their study had a narrow scope, not attempting to identify a broader set of research topics in the area of information security culture. Concretely, they investigated existing definitions of information security culture, and the theories used to discuss the relationship between national and organisational culture and information security culture. They identified different frameworks for fostering an information security culture, such as those put forward by Schlienger and Teufel (2002) and Zakaria *et al.* (2003), and noted that these frameworks make an important contribution to existing research. A second research theme includes the frameworks for understanding information security cultures such as that put forward by Kraemer and Carayon (2005). In addition, Connolly and Lang (2013) concluded that it is common to use influences from organisational science to study information security culture. In particular, "Schein's (1985) Model of Organisational Culture dominates this trend of research".

Connolly and Lang (2012) did not attempt to identify a set of research themes; instead, they focused on theories that underlie existing models of information security culture. They concluded that existing research on information security culture uses theories adapted from "various disciplines including psychology, economics, behavioural sciences and management". Again, they concluded that Schein's (1985) model of organisational culture has influenced existing research greatly, as has Detert *et al.*'s (2000) general framework of organisational culture.

We can conclude that there is no existing literature review on information security culture that systematically assesses current research directions and the underlying theories used. We have also been unable to find literature reviews that assess the maturity of existing research and identify the types of research methods that are predominant in this research. Consequently, very little is known about the frontline of research on information security culture, even though it has been on the research agenda since the start of this century.

3. Research method

Although the general research method of this study is straightforward, it was not a mechanical process; thus, several issues arose, which are detailed below. The general outline of the research process was as follows:

- Elsevier's database SCOPUS was used to search for potential papers.
- The abstract of each paper was read and an initial decision was made as to whether the research related to information security culture.
- 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 the purpose was classified according to Grönlund's (2001) research purpose framework (see below).
- The theoretical section of each paper was read (if such a section was found). The theoretical frameworks used in the paper were noted.
- Based on the large number of original descriptions of research questions, a classification set was created (see below). All papers were then assigned to their appropriate class(es).
- 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 Minger's (2003) research method framework (see below).

The result of the detailed analysis is found in Appendix 2 (Table AII), and a summary is presented in the Results section.

3.1 Selection of papers

Information security culture research appears both in conference proceedings and in international journals. The search for papers was carried out using the SCOPUS database to get a broad coverage of both international journals and conference proceedings. For example, the SCOPUS covers 88 per cent of the journals on the Association of Information Systems' journal ranking list. At the same time, it includes information security journals and conferences, such as information management and computer security, computer and security and IFIP TC 11 International Information Security Conference. Consequently, the database provides good coverage of the information systems field; it provided us with a good sample of papers to show existing research patterns on information security culture. The search included papers published on the database between 2000 and 2013 (December) because Ruighaver *et al.* (2007) has shown that researchers began to recognise information security at the start of this century.

Table I shows the combination of search criteria that were used when searching in SCOPUS; search fields included paper title, abstract and keywords. The table has two columns. The leftmost column contains the search criteria used. The next column shows the total number of papers resulting from each search. The use of multiple search queries resulted in a gross list of 367 research papers including duplicates. After eliminating duplicates and papers that did not focus on information security culture, we ended up with a net list of 77 information security culture papers, of which we were able to analyse 72. The five papers we were unable to analyse are listed in Table AIII, Appendix 2.

3.2 Analytical framework and classification of papers

When reviewing research, it is suggested that research fields fall along a continuum, from nascent to mature, which can be measured empirically. The guiding intuition is

Search criteria	No. of papers
Information security culture	48
Information security AND culture	191
Information security AND organisational culture	37
Information security AND organizational culture	37
Information security AND national culture	8
Information security culture AND employee behaviour	5
Information security culture AND employee behavior	5
Information security culture AND compliance	5
Information security culture AND awareness	14
Information security culture AND self efficacy	0
Information security climate	1
Information security AND climate	15
Information security AND information security culture	1

Table I. Search criteria and search results

simple and straightforward: the stage of development of the literature at one point in time usually influences the kind of research that is undertaken at a second point in time. In general, the less known about a specific topic, the more explorative research is conducted. In contrast, when a topic of interest has been studied extensively, researchers often use prior research to identify critical variables to explain the general mechanisms that underlie the phenomenon or to propose new or modified designs. Relatively mature research fields are also often characterised by a variety of research topics and methods, while nascent fields tend to have a limited repertoire of research methods (Cheon and Grover, 1993).

Characterisations of state-of-the-art research have a descriptive value; they also serve as a normative underpinning to the way in which research questions, types of research and research methods relate to prior theory and research. This is sometimes discussed in terms of "methodological fit" (Edmondson and McManus, 2007). Even though they are not intended as inflexible rules, it can be argued that "a poor fit" may lead to essential problems. Too many open-ended studies in a mature research field may lead to the problem of "reinventing the wheel", and a failure to build effectively on prior work to advance knowledge about a topic. Likewise, too many quantitative measures on a nascent field may be detrimental to chance findings of significant associations among novel constructs and measures; similarly, it may be difficult to suggest effective design solutions for a nascent field because there are few theories to build on.

From these points of departure, we find it important to describe four key elements in information security culture research:

(1) research questions;

(2) their theoretical foundation;

(3) type of research purpose; and

(4) research methods.

It is also necessary to discuss their pairings. Let us now turn, therefore, to the way in which these elements are measured.

3.3 Classification of research questions

To find out which questions are researched in this field and which are not, we have classified the papers according to four "meta-questions" (Inglehart and Welzer, 2005), which are important in relation to almost any phenomenon:

1. (1) What is information security culture? This meta-question covers research on understanding the content of information security culture.
2. (2) What are the roots of information security culture? This meta-question covers research that addresses the forces that shape an information security culture.
3. (3) What are the fruits of different information security cultures? This meta-question addresses consequences of different information security cultures.
4. (4) How do we cultivate information security culture? This meta-question includes research on how to develop cultures that are beneficial for information security in organisations.

Moreover, we have inductively tried to group papers with similar research questions/purposes into topics by using questions or purposes, depending on what the authors used to describe their endeavour. We did so to get a more detailed view of what is actually being researched in relation to each meta-question. First, for the 72 papers, we noted all original research questions. Second, after the initial recording of original questions, we created initial codes, trying to group papers together. Many papers used similar words to describe the questions/purposes; for example, "to propose a framework" (Da Viega and Eloff, 2010) and "the paper details the model" (Thomson *et al.*, 2006). Third, the initial codes were used to create themes to which the papers were assigned. Fourth, we assigned the research topics to our four meta-questions.

3.4 Classification of theoretical foundations

The classification of theories on which existing information security culture research is based was made inductively. Instead of using a predefined framework for classification, we noted all theories that had been used as a starting point for analysis, design solutions or data collection in the investigated papers. In other words, we only classified occurrences of theory when they had an impact on the research design or design product. Our classification of theories closely followed the researchers' descriptions, which meant that it involved a great deal of judgement. In some cases, we had to go to the original sources to understand the theoretical foundation of the research. We also noted papers that did not make explicit use of theoretical frameworks.

3.5 Classification of types of research purpose

A third important element for classifying research is type of research purpose. Often, three types of research purposes are used for classification: exploratory, descriptive and explanatory (Schutt, 2001). The framework used here builds on this classification, but has been extended to five categories, in line with work by Grönlund (2001), to better grasp nuances at the nascent end of the scale. The categories are defined in Table II. The table has three columns. The leftmost column indicates the maturity state of the research, the second column contains the five research purpose classes and the rightmost column shows the operational definitions. The general idea is that a

Table II. Types of research purpose, based on Grönlund (2001)

State of research	Research purpose	Operational definition
Nascent	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"
Mature	Theory generating	"Attempts to analyse/interpret quantitative or qualitative data in a systematic manner for the purpose of model building"
	Theory testing	"Attempts to test a theory using quantitative or qualitative data in a systematic manner, i.e. not just strict theory testing"

mature field would focus on the generation and testing of theories that either explain or design a phenomenon, while a less mature field would focus more on exploring, describing and reflecting upon a phenomenon.

3.6 Classification of research methods

A classification of research methods can be carried out in many ways, and sometimes the distinctions between research strategies, approaches and methods are not very clear. We used a modified version of Minger's (2003) framework, even though it adopts a rather broad definition of research method. The reason for this is that we benefit from the opportunity to make comparisons between research on information security culture and the broader information systems field. Mingers (2003) identified 13 types of research methods, to which we have added three. The first is design science, which has received increased attention during recent years; most notably, after Minger's (2003) framework was created. Moreover, Minger (2003) did not include argument or literature review in his list of research methods because he only analysed empirical papers. Hence, the modified framework contained 16 types of research methods:

(1) action research;

(2) case study;

(3) consultancy;

(4) critical theory;

(5) design science;

(6) ethnography;

(7) experiments;

(8) grounded theory;

(9) interviews;

(10) literature review;

(11) participant observation;

(12) passive observation and measurement;

(13) qualitative content analysis
(14) simulation;
(15) subjective/argumentative; and
(16) survey/questionnaire/instrument.

The detailed operational definitions of the research methods are found in Appendix 1.

Note that in our classification of research methods it was possible for a study to use more than one research method. Thus, research may have been carried out using mixed-methods (Ågerfalk, 2013).

4. Results

In this section, we present a summary of our literature review, structured according to our four research questions. The detailed analysis is found in Appendix 2, Table AII.

4.1 Research questions investigated in information security culture research

What is existing research about? The analysis presented in Table III suggests that three out of four meta-questions have been covered by the research community, and in relation to these, we have identified nine specific research topics on information security culture. In Table III, the leftmost column contains the meta-questions, the second column contains the research topics, the third column contains the number of papers and the rightmost column shows the relative frequency.

When it comes to the meta-questions, we found that 25 per cent of the papers deal with questions relating to the nature of information security culture and that an additional 43 per cent are searching for the roots of information security culture. The fact that the bulk of the papers has ended up in these categories, signals that this field of research is certainly at an early stage. We found it interesting that no papers have investigated *the fruits of* different information security cultures, i.e. what differences in information security do different information security cultures generate? This came as a

Meta-question	Research topic	*n*	(%)
What is information security culture?	Framework for understanding information security culture	8	11
	Approaches to assess information security culture	6	8
	Analysis of existing security cultures	4	6
What are the roots of information security culture?	The relation between (organisational) culture and information security	22	31
	Factors that contribute to information security culture	9	12
What are the fruits of different information security cultures?	–	–	–
How do we cultivate information security culture?	Framework for cultivating an information security culture	13	18
	Management challenges	6	8
	Existing practices	2	3
	Practical work with cultivating an information security culture	2	3

Table III.
Research topics investigated

surprise, bearing in mind that almost one-third of the papers are concerned with the meta-question of how to cultivate an information security culture.

We took a look at the three specific topics that are the focus of the first meta-question. First, we found frameworks for understanding information security culture (Harnesk and Lindström, 2011; Van Niekerk and Von Solms, 2010; Alfawaz *et al.*, 2010). These frameworks differ from those detailed in relation to the fourth meta-question, the purpose of which is to cultivate. For example, Harnesk and Lindström (2011) developed a typology to categorise the information security environment along two dimensions: discipline and agility. They ended up with four types of culture: motivation, avoidance, opportunism and compliance, which can be used to understand an existing information security culture. In addition, we found approaches to assess information security culture (Okere *et al.*, 2012; Ghernaouti-Hélie *et al.*, 2010; Gaunt, 1998). For example, Okere *et al.* (2012) analysed two approaches to assess information security culture. According to them, information security culture should be assessed on the following underlying levels: artefacts, espoused values, shared tacit assumptions and information security knowledge. However, none of the analysed approaches had data collection techniques that satisfied the need to assess all four levels. Finally, we found a few analyses of existing security cultures. We identified four papers in this category (Kolkowska, 2011; Ramachandran *et al.*, 2008). Kolkowska (2011), for example, identified the existence of subcultures in an organisation; these subcultures caused value conflicts, which in turn affect information security. The different subcultures originated from the employees' professional values. Kolkowska's findings corroborate the findings of Ramachandran *et al.* (2008), who carried out a comparative study of four professions. In their study, they identified "the existence of differences in security cultures across professions".

In relation to the second meta-question, two research topics dominate. The first refers to the relation between culture/organisational culture and information security (McCoy *et al.*, 2009; Goo *et al.*, 2013; Connolly and Lang, 2012). This category of papers sets out to test the basic assumption that culture affects information security in organisations. One example is a study by McCoy *et al.* (2009), who were unable to establish a relationship between organisational culture and information security attitudes and behaviours. Goo *et al.* (2013) on the other hand, used the climate concept, which strongly supported the view that "the information security climate has significant positive influence on the intention of the security policy compliance". Consequently, existing findings can be described as inconclusive at best. The second topic of interest concerns factors that contribute to information security culture (Knapp *et al.*, 2007; Shahibi *et al.*, 2012; Alnatheer and Nelson, 2009). For example, Knapp *et al.* (2007) concluded that top management support is a factor that positively impacts on information security culture. Hence, according to this study, it is important to have top management's support when implementing information security culture changes.

In relation to the fourth meta-question, we found four main topics. First, there are studies that have addressed frameworks for cultivating an information security culture (Da Viega and Eloff, 2010; Thomson *et al.*, 2006; Williams, 2008, Nemati and Church, 2009). For example, Da Viega and Eloff (2010) stated that information security components "are implemented in the organisation", which influences employees' information security behaviour. In time, these behaviours evolve "as the way things are done in the organisation", which is the definition of culture used by Da Viega and Eloff (2010). In addition, they detailed the framework on three levels, identifying information security components such as security policies and security program management. Second, we found some papers on existing practices (von Solms, 2000, Lacey, 2010). von Solms (2000) divided the development of information security into three waves; he described the third wave as institutionalisation, of which cultivating an information security culture is one aspect. Lacey (2010) highlighted "failings and critical success factors in contemporary approaches to transform organisational culture"; these included managers' failure to understand the principles of psychology and a lack of experience of marketing campaigns. He concluded that more emphasis should be put on genuine engagement with employees rather than infrastructure and formal procedures. A related topic is practical work with cultivating an information security culture (Johnson and Goetz, 2007; Ashenden and Sasse, 2013). Based on empirical examples, Johnson and Goetz (2007) described information security culture work and the importance of personalising information security for employees and the creation of awareness. Ashenden and Sasse (2013) reported that, nowadays, Chief Information Security Officers (CISOs) are expected to contribute to organisational culture. CISOs, however, have struggled with "a perceived lack of power, confusion about their role identity and their inability to engage effectively with employees", making it difficult to fulfil this task. The final topic, management challenges (Ashenden, 2008; Ghernaouti-Hélie, 2009; Dojkovski *et al.*, 2007a; Gaunt, 2000; Johnsen *et al.*, 2006), represents 8 per cent of all investigated papers. All of these studies have typically addressed the challenges that managers face when "managing individuals in an organization" (Ashenden, 2008) to create a way of working. Examples of identified challenges are employees' awareness (Ghernaouti-Hélie, 2009), countering the *laissez-faire* attitude of employees (Dojkovski *et al.*, 2007a), finding enough resources to bring about any changes (Gaunt, 2000) and the training of employees (Gaunt, 2000). Dojkovski *et al.* (2007a), who focused on small- and medium-sized organisations, also identified business owner awareness as a challenge when creating an information security culture.

4.2 Theories underlying information security culture research

As shown in Table IV, a number of theories underlie the investigated papers on information security culture research. The table is structured into four columns; the leftmost column contains the four meta-questions, the second column contains the research topics we identified above, the third column contains the theories used and the rightmost column contains the identified reference disciplines.

Our analysis shows that seven reference disciplines have contributed with theories to information security culture research: anthropology, economics, knowledge management, organisational science, psychology, philosophy and sociology. Table IV shows that, of these disciplines, most theories have been borrowed from organisational science and psychology. It is not surprising that several of these theories are culture models/typologies of cultures (Schein, 1985; Hofstede, 1997; Westrum, 1993; Detert *et al.*, 2000). If we were to highlight single theories that have had an impact on several research topics, then we must include Schein's (1985) culture model and Hofstede's (1997) national culture framework; both originate from organisational science. For example, the culture model elaborated by Schein (1985) underlies research on three meta-questions and no fewer than six of our nine research topics, such as frameworks for cultivating and understanding information security culture. However, Table IV also shows that research on the meta-question how to cultivate information security culture use of the least number of theories. Indeed, the specific research topic "Existing practices" is not based on any theories. This is not surprising considering

Meta-question	Research topic	Theory	Reference discipline
What is information security culture?	Framework for understanding information security culture	Schein's (1985) culture model	Organisational science
		Elasticity theory (Acs and Gerlowski, 1996)	Economics
		Harrald's (2006) organisational typology	Organisational science
		Social exchange theory (Homans, 1958)	Sociology
	Approaches to assess information security culture	Hofstede's (1997) national culture framework	Organisational science
		Value-focused thinking (Keeney, 1992)	Organisational science
		Conscious competence learning matrix (Howell and Fleishman, 1982)	Psychology
	Analysis of existing security cultures	Schein's (1985) culture model	Organisational science
		Organisational culture framework (Detert *et al.*, 2000)	Organisational science
		Hall's (1959) classification of behavioural responses	Anthropology
		Hofstede's (1997) national culture framework	Organisational science
What are the roots of information security culture?	The relation between (organisational) culture and information security	Nine national culture dimensions (House *et al.*, 2004)	Organisational science
		Competing values framework (Quinn and Cameron, 1983)	Organisational science
		Hofstede's (1997) national culture framework	Organisational science
		Grid/group typology from cultural theory (Douglas, 1992, Douglas and Wildavsky, 1982)	Anthropology
		The four component model of moral development (Rest, 1986)	Psychology
		Theory of planned behaviour (Ajzen, 1991)	Psychology
		Psychological climate (Rousseau, 1988)	Psychology
		Ethical decision-making model (Thong and Yap, 1998)	Philosophy
		Schein's (1985) culture model	Organisational science
		Organisational culture framework (Detert *et al.*, 2000)	Organisational science

(*continued*)

Table IV. Research topics and underlying theories

Meta-question	Research topic	Theory	Reference discipline
	Factors that contribute to information security culture	Schein's (1985) culture model	Organisational science
		Competing values framework (Quinn and Cameron, 1983)	Organisational science
		Theory of planned behaviour (Ajzen, 1991)	Psychology
		Hofstede's (1997) national culture framework	Organisational science
		Lazarus' (1993) stress model	Psychology
What are the fruits of different information security cultures?	–	–	–
How do we cultivate information security culture?	Framework for cultivating an information security culture	Schein's (1985) culture model	Organisational science
		Three-tier organisational behaviour (Robbins, 2001)	Organisational science
		Goal-setting theory (Locke and Latham, 2002)	Psychology
		Conscious competence learning model (Flower, 1999)	Psychology
		Modes of knowledge creation (Nonaka, 1994)	Knowledge management
		Individual transition process (Bridges, 2003)	Organisational science
	Management challenges	Schein's (1985) culture model	Organisational science
		Westrum's (1993) typology of organisational cultures	Sociology
	Existing practices	–	–
	Practical work with cultivating an information security culture	Organisational discourse theory (Hardy, 2001)	Organisational science

Table IV.

that existing research in this category is mainly philosophical (Table V) and makes no claims to actively use theories.

To summarise, there are only a few reference disciplines that have substantially influenced information security culture research. Furthermore, many theories used are standard texts on organisational culture that cut across meta-questions and specific topics. Most of these theories are not current.

4.3 Types of research purpose in information security culture research

Table V shows our analysis of the types of information security culture research we have identified. The analysis is structured according to our meta-questions, the nine research topics discussed above and Grönlund's (2001) types of research purpose: descriptive, philosophical, theoretical, theory generating and theory testing.

Meta-question	Research topic	Descriptive	Philosophical	Theoretical	Theory generating	Theory testing	Sum
What is information security culture?	Framework for understanding information security culture	2	0	3	3	0	8
	Approaches to assess information security culture	3	0	2	0	1	6
	Analysis of existing security cultures	0	0	0	3	1	4
	The relation between (organisational) culture and information security	2	1	9	3	7	22
What are the roots of information security culture?	Factors that contribute to information security culture	1	0	5	0	3	9
What are the fruits of different information security cultures?	–	–	–	–	–	–	–
How do we cultivate information security culture?	Framework for cultivating an information security culture	2	0	8	2	1	13
	Existing practices	0	2	0	0	0	2
	Practical work with cultivating an information security culture	1	0	0	1	0	2
	Management challenges	1	2	1	2	0	6
Sum		12	5	28	14	13	72
%		17	7	39	19	18	100

Table V. Types of purpose in information security culture research

As is shown in the last row in Table V, almost 40 per cent of the papers are theoretical papers. Hence, these papers reflect on different aspects of information security culture; they are based on some theory but do not include empirical data. It is worth noting that several papers, which address the basic assumption that culture affects information security in organisations, are theoretical (Connolly and Lang, 2012; Furnell and Thomson, 2009; Ilvonen, 2011; Luo *et al.*, 2009; Thomson and von Solms, 2005). Moreover, we also found a considerable number of framework papers in this category; frameworks that are proposed for understanding (Rastogi and von Solms, 2012; Tsohou *et al.*, 2007), as well as cultivating information security culture (Ngo *et al.*, 2005; Thomson and Van Niekerk, 2012; Thomson *et al.*, 2006). This means that these frameworks are not empirically driven or tested.

One-fifth of all the papers are theory generating. The aim of these papers is to contribute to model building, through the use of either quantitative or qualitative data. We found that most attention is devoted to frameworks for understanding (Alfawaz *et al.*, 2010; Harnesk and Lindström, 2011) or cultivating (Dojkovski *et al.*, 2010, 2007b) information security. However, some papers also address basic assumptions by building models on the relationship between (organisational) culture and information security (Goo *et al.*, 2013; Lim *et al.*, 2010).

Theory testing papers constitute almost one-fifth of all papers. The papers that we identified are mostly related to investigating the relationship between (organisational) culture and information security (Chang and Lin, 2007; Chen *et al.*, 2008; Lowry *et al.*, 2013) and factors that contribute to information security (Hu *et al.*, 2012; Knapp *et al.*, 2007). These papers attempted to test theories on information security culture in a systematic manner using quantitative or qualitative data.

A little less than one-fifth of the investigated papers are descriptive; this means that they describe information security culture or different aspects of that phenomenon without any use of theory. Descriptions of different frameworks for understanding (Kraemer and Carayon, 2005; Malcolmson, 2009) and cultivating (Nemati and Church, 2009; Ruighaver *et al.*, 2010) information security make up the larger part of these papers. In this category, we also found papers that describe approaches to assessing information security cultures (Ghernaouti-Hélie *et al.*, 2010; Okere *et al.*, 2012).

Finally, a few papers are purely philosophical, which means that information security culture is reflected upon without the use of empirical data or reference to any theory. It is worth noting that the only papers on existing practices (Lacey, 2010; von Solms, 2000) are found in this category; these papers reflect on the work with information security culture on a general level.

The majority of the investigated papers are thus descriptive, philosophical or theoretical, which are the characteristics of a nascent field of research. However, looking at the distribution over time (Table VI), we did find some indications of change. Looking at the period from 2010 to 2013, it is clear that more papers had the purpose of generating and testing theories based on empirical work, compared with the period from 2000 to 2009. Hence, the table shows that scholars in this sub-field have increased efforts to *combine* theory and empirical data in their research work.

4.4 Research methods

Tables VII and VIII show our analysis of research methods used in existing research on information security culture. In Table VII, the analysis is structured according the meta-questions and the nine research topics identified above. The meta-questions are presented in the leftmost column. In the second column, we present the identified research topics. In the next nine columns, we present the research method that has been used in existing research. Hence, the table only contains a subset of our modified version of Mingers' (2003) framework. Table VIII presents our analysis, which has been structured according to the five types of research purpose. The types of research purpose are presented in the leftmost column and, again, the next nine columns present the types of research method used in existing research.

As shown in Table VII, the subjective/argumentative-category represents 35 per cent of all papers. Among this research, we found several papers that propose frameworks for cultivating (Ngo *et al.*, 2005; Thomson and Van Niekerk, 2012; Vroom and von Solms, 2004) and understanding (Tsohou *et al.*, 2007; Van Niekerk and Von Solms, 2010) information security culture, as well as papers that address the relationship between (organisational) culture and information security (Corriss, 2010; Furnell and Thomson, 2009; Warner, 2006). When looking at the subjective/argumentative-category in Table VIII, we see that these papers are either philosophical or theoretical in nature. Hence, these papers lack empirical data; in other words, they are not empirically grounded. An interesting aspect of these subjective/argumentative papers is that they often lack a description of the research method used.

Survey and case study methods are important methods for existing research on information security culture. Survey methods were used in almost one-fifth of the investigated studies. Indeed, this type of method was most prominent in studies that address the relation between (organisational) culture and information security (Alarifi *et al.*, 2012; Chang and Lin, 2007; Hovav and D'Arcy, 2012; McCoy *et al.*, 2009). These studies often aim to generate or test theory. Case study methods have mainly been used for studies of frameworks for cultivating (Dojkovski *et al.*, 2010; Nemati and Church, 2009), understanding (Alfawaz *et al.*, 2010; Harnesk and Lindström, 2011) or assessing information security culture (Ghernaouti-Hélie, 2009; Schlienger and Teufel, 2005), as well as investigating management challenges related to information security cultures (Dojkovski *et al.*, 2007a; Gaunt, 2000). Table VIII shows that these studies belong to two types of research: descriptive or theory generating.

Type of research purpose	2000-2009	2010-2013	Difference
Descriptive	15.0% (6)	18.8% (6)	+3.8%
Philosophical	7.5% (3)	6.2% (2)	−1.3%
Theoretical	50.0% (20)	25.0% (8)	−25.0%
Sum theoretical, descriptive, philosophical	72.5% (29)	50.0% (16)	−22.5%
Theory generating	12.5% (5)	28.1% (9)	+15.6%
Theory testing	15.0% (6)	21.9% (7)	+6.9%
Sum theory testing, theory generating	27.5% (11)	50.0% (16)	+22.5%
Total sum of papers	40	32	

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

Table VI. Type of purpose in information security culture research, development over time

Table VII.
Used types of research methods used and research topics

Meta-question	Research topic	Case study	Consultancy	Experiment	Grounded theory	Interviews	Literature review	Qualitative content analysis	Subjective/ argumentative	Survey
What is information security culture?	Framework for understanding information security culture	2	0	0	0	3	0	0	3	1
	Approaches to assess information security culture	3	0	0	0	0	1	1	2	0
	Analysis of existing security cultures	1	0	0	0	2	0	0	0	1
What are the roots of information security culture?	The relation between (organisational) culture and information security	2	0	1	0	1	1	0	9	9
	Factors that contribute to information security culture	0	0	1	1	0	1	0	4	3
What are the fruits of different information security cultures?	–	–	–	–	–	–	–	–	–	–
How do we cultivate information security culture?	Framework for cultivating an information security culture	5	0	0	0	1	3	0	5	1
	Existing practices	0	0	0	0	0	0	0	2	0
	Practical work with cultivating an information security culture	0	0	0	0	2	0	0	0	0
	Management challenges	2	1	0	0	1	1	0	2	0
Sum		15	1	2	1	10	7	1	27	15
%		19	1	3	1	13	9	1	35	18

Type of research purpose	Case study	Consultancy	Experiment	Grounded theory	Interviews	Literature review	Qualitative content analysis	Subjective/ argumentative	Survey
Descriptive	5	0	0	0	4	1	1	0	3
Philosophical	0	0	0	0	0	0	0	5	0
Theoretical	2	1	0	0	0	3	0	22	0
Theory generating	7	0	0	0	6	3	0	0	2
Theory testing	1	0	2	1	0	0	0	0	10
Sum	15	1	2	1	10	7	1	26	15
%	19	1	3	1	13	9	1	35	18

Table VIII. Used types of research methods used and types of research purpose

Interviews account for 13 per cent. This type of research method has been prominent in studies that focus on frameworks for understanding information security culture (Kraemer and Carayon, 2005, 2007; Malcolmson, 2009). In addition, interview studies are of two types: descriptive or theory generating. Consequently, the use of this research method shares similarities with the use of the case study method.

Almost one-tenth of the papers include literature reviews (Connolly and Lang, 2012; Okere *et al.*, 2012; Shahri *et al.*, 2012). However, few of the studies are pure literature reviews. Instead, this research method has often been used in combination with other types of research methods; the purpose is often to gather background information for the studies conducted. Table VIII shows that most of these papers are either theoretical or theory generating.

Table VII shows that such research methods as consultancy, experimentation, grounded theory and qualitative content analysis have not been widely used. In addition, we did not identify any papers that used the following research methods: action research, critical theory, design science, observation, participation observation and simulation.

To summarise, we can conclude that the research methods used in a considerable number of the investigated papers are subjective/argumentative. In addition, of the 15 types of research methods found in the modified version of Minger's (2003) framework, only 9 can be found in existing research; a closer investigation of these methods showed that only five of these methods (case study, interviews, literature review, subjective/argumentative and survey) have been used extensively.

5. Discussion

Despite the fact that information security culture has been on the research agenda for over a decade, there is no systematic literature review on existing research that focuses on the kind of knowledge that has been developed and how it has been developed. In this study, we have systematically investigated existing research on information security culture. Tables III–VIII show the patterns we found. Based on these findings, some notable lessons can be learned with regard to:

- topics investigated in information security culture research;
- theories that underlie information security culture research;
- types of research purpose in information security culture research; and
- types of research methods used.

5.1 Research topics investigated in information security culture research

Our findings show that a broad range of topics have been investigated in the area of information security culture; however, only a few topics account for most of the research carried out. A similar pattern was found when Siponen and Willison (2007) assessed information security research in general. Hence, as a pattern, we corroborate their findings; however, we were not able to compare the identified topics as such because our study focused on a particular part of the information security field.

Two of the research topics that we identified were also identified by Connolly and Lang (2013): "Framework for cultivating an information security culture" and "Framework for understanding information security culture". Thus, we can corroborate their findings, even though the two studies used slightly different strategies for selecting papers. Our study can also be said to complement that of Connolly and Lang (2013) because we have gone on to identify an additional seven research topics (Table III). This is an important contribution because the identification of these topics allows us to discuss where earlier research efforts have been focused.

We can conclude, therefore, that the most researched meta-question is What are the roots of information security culture and that only three of the four meta-questions have been addressed in research to date? In addition, the meta-question "What are the fruits of different information security cultures?" has not been addressed at any length. It is striking that no papers have, as yet, investigated the effects of different information security cultures. This indicates that the benefits of different cultures for performance are more or less taken for granted; in other words, they are seen as a point of departure rather than as something that needs to be empirically tested. However, it should be acknowledged that studying the effects of implementing or changing an information security culture or comparing the effects of different information security cultures are difficult empirical tasks. Such studies need to be able to access data from different cultures either over a long period of time or from different organisations or parts of organisations. Moreover, and what might be more difficult, it requires access to measures of actual information security such as incident reports.

We can conclude, then, that the most researched topics are *The relation between culture/organisational culture and information security* and *Framework for cultivating an information security culture*. However, although we have identified a rather broad range of topics, few studies have been carried out in each of these areas; indeed, several research topics have been studied only in a small number of papers. For example the research topic *Practical work with cultivating an information security culture* is only referred to in two papers. This means that our knowledge regarding these topics is quite limited. From a research point of view, it means that there are ample opportunities for future research in general, and on the meta-question "What are the fruits of different information security cultures and the less researched topics?" in particular. Consequently, there are implications for practice; it is difficult for practitioners to anchor their way of working in existing research because the number of studies is quite small.

5.2 Theories underlying information security culture research

Siponen and Willison (2007) have concluded that the majority of existing information security research generally lacks theory (81 per cent of the published papers between 1990 and 2004). We found that 24 per cent of the investigated papers in our study made no reference to theory. It is gratifying that we can see a higher degree of maturity in terms of theory compared with the findings by Siponen and Willison (2007).

According to Connolly and Lang (2013, 2012), the theories that underlie information security culture research originate from organisational science. They argued that Schein's (1985) model of organisational culture has had a major impact on information security culture research. In addition, Connolly and Lang (2012) identified Detert *et al.*'s (2000) general framework of organisational culture as another important theory that has been used in existing research.

Our findings show the same pattern as those presented above. Organisational science theories are predominant in all meta-questions and almost all research topics. Other reference disciplines that we have identified are anthropology, economics, knowledge management, philosophy, psychology and sociology. However, none of these reference disciplines has had the same impact on information security culture research as organisational science. We also identified that *Existing practices* is a topic for which no theories are used. To date, research on this topic has been philosophical; indeed, this type of research is not characterised by the explicit use of theories. It is also worth noting that almost one-fourth of the identified research is either descriptive or philosophical, which means there has been no active use of theories.

With regard to individual theories, we found that Schein's (1985) model of organisational culture has been the single most-used theory. It was used in three of the research meta-questions and in six of the nine research topics that we identified. The second most-used theory is Hofstede's (1997) national culture framework, which we found in four of the nine research topics. Otherwise, a spread of theories has been used. However, we have been unable to show the importance of Detert *et al.*'s (2000) general framework of organisational culture, a theory that Connolly and Lang (2012) pointed out as important.

Thus, we have found that existing research on information security culture has used theories from several reference disciplines. However, the distribution of reference disciplines is skewed. It is understandable that many studies have borrowed theories from organisational science because this discipline has carried out extensive research into the cultural aspects of organisations. Despite this fact, we believe that it would be beneficial for information security culture research if theories from other reference disciplines were considered to a larger extent, for example, theories from sociology, a discipline that has also researched culture at length (cf. Allan, 2010).

5.3 Types of research purpose in information security culture research

The opportunities for future research on information security culture was made even more specific when we added types of research purpose as an additional analytical layer (Table V). None of the existing literature reviews on information security culture (Connolly and Lang, 2013, 2012; Chang and Lin, 2007; Malcolmson, 2009) has studied this aspect; hence, we can contribute to the field by pinpointing the maturity of this subfield and the different research topics.

In general, we can conclude that the majority of the existing research is descriptive, philosophical or theoretical. Thus, existing research, irrespective of the meta-question it seeks to answer, is rather immature when measured according to Grönlund's (2001) framework. For example, one surprising finding is the large share of descriptive and theoretical research into the research topic *Framework for cultivating an information security culture*. Research in this area aims to contribute to the way in which information security culture is created. To some extent, these papers serve to prescribe the cultivating process. Nonetheless, most of these studies lack a structured analysis of the presented cases (descriptive) or empirical evidence (theoretical), and it is relevant to discuss on what basis these prescriptions were made. Much of the same conclusion can be drawn for the research topics *Existing practices* and *Approaches to assess information security culture*. The only topic that has produced a large share of research into theory generating and theory testing is *The relation between culture/organisational culture and information security*. This result shows that this research topic shows greater maturity than the other topics.

Our analysis showed that half of last years' studies on information security culture (2010-2013) are either theoretical, descriptive or philosophical. This shows a change from the period from 2000 to 2009, with an increase in the share of research devoted to theory generating and theory testing. Hence, with regard to the purpose of research in this subfield, there is a move towards greater maturity.

At least two implications for research can be identified. First, we can conclude that there is a need for more empirical research on all of the meta-questions and on most of the research topics that have been listed in Table III. Second, to increase the maturity of future research, there is also a need to combine empirical research with explicit use of theories (theory testing) or ensure that empirical research is used for the development of theories on information security culture (theory generating). The large share of descriptive and non-empirical research also has implications for practice. It is difficult for practitioners to adopt research results, such as frameworks or assessment tools, which have not been empirically validated. Consequently, with regard to several of the listed research topics, limited advice can be offered to practitioners.

5.4 Types of research methods used

Our findings on types of research methods used in information security culture research extend beyond the existing knowledge base. Existing studies (Connolly and Lang, 2013, 2012; Chang and Lin, 2007; Malcolmson, 2009) have not investigated this aspect of research carried out to date.

First, compared with the information systems field in general (Mingers, 2003), we found a different pattern of research method use in the subfield of information security culture. We can conclude that the spread of research methods used is smaller than in the information systems field in general. This is very similar to the findings of Siponen and Willison (2007), who investigated information security research in general. The most used research methods when researching information security culture are subjective/argumentative, case studies, surveys, interviews and literature reviews (often used as a background for arguing for a particular study). However, our study does not provide any answers as to why fewer types of research methods are used. Of course, some types of research methods might be more appropriate than others with regard to a research problem. Consequently, to some extent, the focus on certain research topics may provide one part of the explanation. But still it is interesting to see that such research methods as ethnography and participation observation, which are found in culture studies in other disciplines, are not present in existing research on information security culture.

Mingers (2003) argued that research methods have been developed "within a particular paradigm, but the relationship is far from clear". Similar arguments can be found in an analysis of information security research by Dhillon and Backhouse (2001), who used the framework put forward by Burrell and Morgan (1979). Thus, we can conclude that research methods come with a set of basic assumptions. When a small number of research methods have been used, only a limited number of perspectives have been used to address information security culture. For example, neither did we find any studies that used action research or design science, which belong to an intervention-oriented paradigm, nor did we find any studies that use critical theory. This is pretty much in line with the conclusion drawn by Dhillon and Backhouse (2001) on information security research in general, where intervening and critical research is rare.

Second, our findings show that a large number of the studies had a subjective/argumentative research method. In many cases, the research method had not been made explicit in these papers, which makes it difficult to assess the findings. Hence, we can conclude that researchers in the subfield of information security culture could be more explicit with their use of research methods or at least with the starting points for their logical arguments.

Third, we did not identify any strong patterns between meta-questions or research topics and the types of research methods used, except that many of the studies on *The relation between culture/organisational culture and information security* were carried out using surveys. Several of these papers construct hypotheses that are tested using different statistical analysis. These studies, more than others, are an example of the limited number of perspectives that have been used in the research of information security culture.

We believe that our findings should have implications for the types of research methods that are used in future research on information security culture. First, they call for a broader use of research methods to illustrate the phenomenon from several perspectives. Second, we believe that it would be beneficial to use mixed-methods (Ågerfalk, 2013) to gather empirical data. Today, the most frequent combination is a literature review in combination with another research method; this means that empirical data are often collected using just one research method.

5.5 The limitations of this study

In this paper, we have reported on the topics researched in the subfield of information security culture, as well as the underlying theories, types of research purpose and research method used. Obviously, our results depend on the search strategy and the selection of papers. We have been explicit with our selection of papers, which is based on searches of Elsevier's database SCOPUS. Of course, other search strategies are possible; for example, those used by Connolly and Lang (2012, 2013). Hence, we do not claim that we have identified all studies on information security culture, but we have used a sample of good size from relevant outlets.

Furthermore, the use of our analytical framework involves subjective judgement. It has not always been a straightforward task to classify papers into research topic categories or types of research methods. We have tried to make the analysis as explicit as possible by providing the complete classification of papers in Appendix 2; making it possible to scrutinise the analysis in detail.

6. Conclusion

The aim of this paper was to survey existing information security culture research to scrutinise the kind of knowledge that has been developed, and the way in which this knowledge has been brought about. For this purpose, we used Grönlund's (2001) framework on types of research purpose and an extended version of Minger's (2003) framework on research methods. We can conclude that, with regard to depth, existing research has focused on a limited set of research topics using a small repertoire of research methods; the repertoire is more limited than in information systems research in general. We categorised existing research in terms of four meta-questions:

(1) What is information security culture?

(2) What are the roots of information security culture?

(3) What are the fruits of different information security cultures?

(4) How do we cultivate information security culture?

We can conclude that research has been carried out for three of the four questions. However, research on the fruits of different information security cultures is lacking. Furthermore, we can conclude that an extensive part of research is descriptive, philosophical or theoretical. With regard to research methods only a limited set of research methods have been used, and the majority of the studies have used a subjective/argumentative method. Taken together, this means that research carried out to date is quite immature.

Our findings indicate that future information security culture research should:

- address a broader set of research topics;
- focus more on generating theories or testing theories to increase the maturity of this subfield of information security research; and
- use a broader set of research methods.

It would be particularly interesting to see future studies that use intervening or critical approaches which, so far, have been completely lacking in research.

References

Abraham, S. (2011), "Information security behaviour: factors and research directions", *Americas Conference on Information Systems*, AIS Electronic Library (AISeL), *Detroit, MI*.

Acs, Z.J. and Gerlowski, D.A. (1996), *Managerial Economics and Organization*, Prentice Hall, Upper Saddle River, NJ.

Ågerfalk, P.J. (2013), "Embracing diversity through mixed methods research", *European Journal of Information Systems*, Vol. 22, pp. 251-256.

Ajzen, I. (1991), "The theory of planned behavior", *Organizational Behavior and Human Decision Processes*, Vol. 50 No. 2, pp. 179-211.

Alarifi, A., Tootell, H. and Hyland, P. (2012), "A study of information security awareness and practices in Saudi Arabia", *2012 International Conference on Communications and Information Technology (ICCIT)*, IEEE Explore, Hammamet, pp. 6-12.

Alfawaz, S., Nelson, K. and Mohannak, K. (2010), "Information security culture: a behaviour compliance conceptual framework", *The Australasian Information Security Conference (AISC) 2010*, *Brisbane*, pp. 47-55.

Allan, K.D. (2010), *Explorations in Classical Sociological Theory: Seeing the Social World*, Pine Forge Press, Thousand Oaks, CA.

Alnatheer, M. and Nelson, K. (2009), "Proposed framework for understanding information security culture and practices in the Saudi context", *7th Australian Information Security Management Conference*, *Edith Cowan University, Perth*, 1-3 December, pp. 5-17.

Alshare, K.A. and Lane, P.L. (2008), "A conceptual model for explaining violations of the information security policy (ISP): a cross cultural perspective", *Americas Conference on Information Systems 2008*, *AIS Electronic Library*.

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

Ashenden, D. and Sasse, A. (2013), "CISOs and organisational culture: their own worst enemy?", *Computers & Security*, Vol. 39, pp. 396-405.

Bess, D. (2009), "Understanding information security culture for strategic use: a case study", *e15th Americas Conference on Information Systems (AMCIS 2009)*, AIS Electronic Library (AISeL).

Božić, G. (2012), "The role of a stress model in the development of information security culture", *35th International Convention of Information Communication Technology, Electronics and Microelectronics MIPRO 2012*, IEEE Xplore Digital Library, Opatija, pp. 1555-1559.

Bridges, W. (2003), *Managing Transitions: Making the Most of Change*, Perseus Books Group, Cambridge, MA.

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

Burrell, G. and Morgan, G. (1979), *Sociological Paradigms and Organisational Analysis: Elements of the Sociology of Corporate Life*, Heinemann, London.

Chang, S.E. and Lin, C.-S. (2007), "Exploring organizational culture for information security management", *Industrial Management & Data Systems*, Vol. 107 No. 3, pp. 438-458.

Chen, C.C., Medlin, B.D. and Shaw, R.S. (2008), "A cross-cultural investigation of situational information security awareness programs", *Information Management & Computer Security*, Vol. 16 No. 4, pp. 360-376.

Cheon, M.J. and Grover, V. (1993), "The evolution of empirical research in IS. A study in IS maturity", *Information & Management*, Vol. 24 No. 3, pp. 107-119.

Connolly, L. and Lang, M. (2012), "Investigation of cultural aspects within information systems security research", *The 7th International Conference for Internet Technology and Secured Transactions (ICITST 2012)*, *IEEE Digital Library, London*, pp. 105-111.

Connolly, L. and Lang, M. (2013), "Information systems security: the role of cultural aspects in organisational settings", *Workshop on Information Security and Privacy 2013 (WISP'13*), Milan.

Connolly, P.J. (2000), "Security starts from within", *InfoWorld*, Vol. 22, pp. 39-40.

Corriss, L. (2010), "Information security governance: integrating security into the organizational culture", *The 2010 Workshop on Governance of Technology, Information and Policies*, ACM Digital Library, Austin, TX, pp. 35-41.

Da Viega, A. and Eloff, J.H.P. (2010), "A framework and assessment instrument for information security culture", *Computer & Security*, Vol. 29 No. 2, pp. 196-207.

Detert, J.R., Schroeder, R.G. and Mauriel, J.J. (2000), "A framework for linking culture and improvement initiatives in organisations", *Academy of Management Review*, Vol. 25 No. 4, pp. 850-863.

Dhillon, G. (1997), *Managing Information System Security*, Macmillan, Basingstoke.

Dhillon, G. and Backhouse, J. (2001), "Current directions in IS security research: towards socio-organisational perspectives", *Information Systems Journal*, Vol. 11 No. 2, pp. 127-153.

Dhillon, G. and Torkzadeh, G. (2006), "Value-focused assessment of information security in organizations", *Information Systems Journal*, Vol. 16 No. 3, pp. 293-314.

Dojkovski, S., Lichtenstein, S. and Warren, M. (2006), "Challenges in fostering an information security culture in Australian small and medium sized enterprises", in Remenyi, D. (Ed.), *The 5th European Conference on Information Warfare and Security (ECIW 2006)*, *Academic Conferences Limited, Reading*, pp. 31-40.

Dojkovski, S., Lichtenstein, S. and Warren, M. (2007a), "Developing information security culture in small and medium size enterprises: Australian case studies", *6th European Conference on*

Information Warfare and Security (ECIW 2007), *Academic Conferences Limited, Shrivenham*, 2-3 July, pp. 55-65.

Dojkovski, S., Lichtenstein, S. and Warren, M. (2010), "Enabling information security culture: influences and challenges for Australian SMEs", *The 21st Australasian Conference on Information Systems (ACIS 2010), AIS Electronic Library (AISeL)*, *Brisbane*.

Dojkovski, S., Lichtenstein, S. and Warren, M.J. (2007b), "Fostering information security culture in small and medium size enterprises: an interpretive study in Australia", *15th European Conference on Information Systems (ECIS 2007)*, AIS Electronic Library (AISeL), St. Gallen.

Douglas, M. (1992), *Risk and Blame: Essays in Cultural Theory*, Routledge, London.

Douglas, M. and Wildavsky, A. (1982), *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers*, University of California Press, Berkeley, CA.

Edmondson, A.C. and Mcmanus, S.E. (2007), "Methodological fit in management field research", *Academy of Management Review*, Vol. 32 No. 4, pp. 1155-1179.

Fernando, S. and Asai, T. (2011), "Human-related information security problems faced by British companies in economically rising countries", *Australian Information Security Management Conference 2011*, *Edith Cowan University, Perth*, 5-7 December, pp. 76-86.

Flower, J. (1999), "In the mush", *Physician Executive Journal*, Vol. 25 No. 1, pp. 64-66.

Furnell, S. (2007), "IFIP workshop – information security culture", *Computer & Security*, Vol. 26 No. 1, p. 35.

Furnell, S. and Thomson, K.-L. (2009), "From culture to disobedience: recognising the varying user acceptance of IT security", *Computer Fraud & Security*, No. 2, pp. 5-10.

Gattiker, U.E. (2008), "Early warning system for home users and small- and medium-sized enterprises: eight lessons learned", *International Journal of System of Systems Engineering*, Vol. 1 Nos 1/2, pp. 149-170.

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

Gaunt, N. (2000), "Practical approaches to creating a security culture", *International Journal of Medical Informatics*, Vol. 60 No. 2, pp. 151-157.

Ghernaouti-Hélie, S. (2009), "An inclusive information society needs a global approach of information security", *2009 International Conference on Availability, Reliability and Security*, *IEEE Computer Society*, pp. 658-662.

Ghernaouti-Hélie, S., Tashi, I. and Simms, D. (2010), "A multi-stage methodology for ensuring appropriate security culture and governance", *2010 International Conference on Availability, Reliability and Security*, *IEEE Computer Society, Krakow*, pp. 353-359.

Goo, J., Yim, M.-S. and Kim, D.J. (2013), "A path way to successful management of individual intention to security compliance: a role of organizational security climate", *46th Hawaii International Conference on System Sciences (HICSS 2013)*, *IEEE Computer Society, Wailea, HI*, 7-10 January, pp. 2959-2968.

Gregor, S. and Jones, D. (2007), "The anatomy of a design theory", *Journal of the Association of Information Systems*, Vol. 8 No. 5, pp. 312-335.

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. and 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.

Hall, E.T. (1959), *The Silent Language*, Anchor Books, Garden City, NY.

Hardy, C. (2001), "Researching organizational discourse", *International Studies of Management and Organization*, Vol. 31 No. 3, pp. 25-47.

Harnesk, D. and Lindström, J. (2011), "Shaping security behaviour through discipline and agility – implications for information security management", *Information Management & Computer Security*, Vol. 19 No. 4, pp. 262-276.

Harrald, J.R. (2006), "Agility and discipline: critical success factors for disaster response", *The ANNALS of the American Academy of Political and Social Science*, Vol. 604 No. 1, pp. 256-272.

Harris, A.L., Yates, D., Harris, J.M. and Quaresma, R. (2010), "Information system ethical attitudes: a cultural comparison of the United States, Spain, and Portugal", *16th Americas Conference on Information Systems (AMCIS 2010)*, AIS Electronic Library (AISeL), *Lima, Peru*, 12-15 August, p. 234.

Hedström, K., Kolkowlska, E., Karlsson, F. and Allen, J.P. (2011), "A values-based compliance model: integrating information systems security into health care", *Journal of Association of Information Systems*, Vol. 20, pp. 373-384.

Helokunnas, T. and Kuusisto, R. (2003), "Information security culture in a value net", *International Engineering Management Conference 2003 (IEMC '03)*, *IEEE Xplore Digital Library, Albany, NY*, 2-4 November, pp. 190-194.

Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004), "Design science in information systems research", *MIS Quarterly*, Vol. 28 No. 1, pp. 75-105.

Hoffer, J.A. and Straub, D.W. (1989), "The 9 to 5 underground: are you policing computer crimes?", *Sloan Management Review*, Vol. 30 No. 4, pp. 35-44.

Hofstede, G. (1997), *Culture and Organizations: Software of the Mind*, McGraw-Hill, New York, NY.

Homans, G.C. (1958), "Social behavior as exchange", *American Journal of Sociology*, Vol. 63 No. 6, pp. 597-606.

House, R.J., Hanges, P.J., Javidan, M., Dorfman, P.W. and Vipin, G. (2004), *Culture, Leadership, and Organizations: The GLOBE Study of 62 Societies*, Sage, Thousand Oaks, CA.

Hovav, A. and D'arcy, J. (2012), "Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the US and South Korea", *Information & Management*, Vol. 49 No. 2, pp. 99-110.

Howell, W.C. and Fleishman, E.A. (1982), *Human Performance and Productivity, Vol. 2: Information Processing and Decision Making*, Erlbaum, Hillsdale, NJ.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2008), "Top management championship and individual behaviour towards information security: an integrative model", *16th European Conference on Information Systems (ECIS 2008), AIS Electronic Library (AISeL)*, *Galway*, p. 54.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012), "Managing employee compliance with information security policies: the critical role of top management and organizational culture", *Decision Sciences Journal*, Vol. 43 No. 4, pp. 615-659.

Ilvonen, I. (2011), "Information security culture or information safety culture: what do words convey?", in Ottis, R. (Ed.), *The European Conference on Informations Warfare 2011*, *Academic Publishing, Reading*, pp. 148-154.

Inglehart, R. and Welzer, C. (2005), *Modernization, Cultural Change, and Democracy: The Human Development Sequence*, Cambridge University Press, Cambridge.

Johnsen, S.O., Hansen, C.W., Nordby, Y. and Dahl, M.B. (2006), "Measurement and improvement of information security culture", *Measurement and Control*, Vol. 39 No. 2, pp. 52-56.

Johnson, E.M. and Goetz, E. (2007), "Embedding information security into the organization", *Journal of Security and Privacy*, Vol. 5 No. 3, pp. 16-24.

Keeney, R.L. (1992), *Value-Focused Thinking*, Harvard University Press, Cambridge, MA.

Knapp, K.J., Marshall, T.E., Rainer, R.K. and Ford, F.N. (2007), "Information security: management's effect on culture and policy", *Information Management & Computer Security*, Vol. 14 No 1, pp. 24-36.

Kolkowska, E. (2005), "Value sensitive approach to information system security", *Americas Conference on Information Systems 2005*, *Omaha, NE*, 11-14 August.

Kolkowska, E. (2011), "Security subcultures in an organization-exploring value conflicts", *19th European Conference on Information Systems (ECIS 2011)*, *AIS Electronic Library, Helsinki*, p. 237.

Koskosas, I.V. (2012), "Cultural and organisational commitment in the context of e-banking", *International Journal of Internet Technology and Secured Transactions*, Vol. 4 No. 1, pp. 26-41.

Koskosas, I.V. and Massalas, C. (2008), "Internet banking security in the contexts of goal setting, culture and risk communication", *International Journal of Risk Assessment and Management*, Vol. 10, pp. 186-205.

Kraemer, S. and Carayon, P. (2005), "Computer and information security culture: findings from two studies", *The Human Factors and Ergonomics Society 49th Annual Meeting*, Orlando, FL, 26-30 September, pp. 1483-1487.

Kraemer, S. and Carayon, P. (2007), "Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists", *Applied Ergonomics*, Vol. 38 No. 2, pp. 143-154.

Lacey, D. (2010), "Understanding and transforming organizational security culture", *Information Management & Computer Security*, Vol. 18 No. 1, pp. 4-13.

Lazarus, R.S. (1993), "From psychological stress to the motions: a history of changing outlooks", *Annual Review of Psychology*, Vol. 44, pp. 1-22.

Lim, J.S., Ahmad, A., Chang, S. and Maynard, S. (2010), "Embedding information security culture emerging concerns and challenges", *Pacific Asia Conference on Information Systems 2010*, AIS Electronic Library (AISeL), *Taipei*, p. 43.

Lim, J.S., Chang, S., Maynard, S. and Ahmad, A. (2009), "Exploring the relationship between organizational culture and information security culture", *The 7th Australian Information Security Management Conference*, *Edith Cowan University, Perth*, pp. 88-97.

Locke, E.A. and Latham, G.P. (2002), "Building a practically useful theory of goal setting and task motivation: a 35-year odyssey", *American Psychologist*, Vol. 57 No. 9, pp. 705-717.

Lowry, P.B., Posey, C., Roberts, T.L. and Bennett, R.J. (2013), "Is your banker leaking your personal information? The roles of ethics and individual-level cultural characteristics in predicting organizational computer abuse", *Journal of Business Ethics*, Vol. 121 No. 3, pp. 385-401.

Luo, X., Warkentin, M. and Johnston, A.C. (2009), "The impact of national culture on workplace privacy expectations in the context of information security assurance", *15th American Conference on Information Systems (AMCIS 2009)*, AIS Electronic Library (AISeL), *San Francisco, CA*.

Malcolmson, J. (2009), "What is security culture? Does it differ in content from general organisational culture?", in Sanson, L.D. and Steiner-Koller, S.M. (Eds), *43rd Annual International Carnahan Conference on Security Technology*, *IEEE Xplore Digital Library, Zurich*, 5-8 October, pp. 361-366.

Martins, J. and Dos Santos, H. (2010), "Methods of organizational information security (a literature review)", in Tenreiro De Magalhaes, S., Jahankhani, H. and Hessami, A.G. (Eds), *Global Security, Safety, and Sustainability – 6th International Conference, ICGS3 2010, Braga, Portugal, 1-3 September*, *Springer, Heidelberg*, pp. 120-130.

Mccoy, B., Stephens, G. and Stevens, K.J. (2009), "An investigation of the impact of corporate culture on employee information systems security behaviour", *20th Australasian Conference on Information Systems (ACIS 2009)*, *AIS Electronic Library, Melbourne*.

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

Nemati, H.R. and Church, M. (2009), "A human centered framework for information security management: a healthcare perspective", *Americas Conference on Information Systems 2009 (AMCIS 2009)*, *AIS Electronic Library*.

Ngo, L., Zhou, W. and Warren, M. (2005), "Understanding transition towards information security culture change", in Valli, C. and Woodward, A. (Eds), *3rd Australian Information Security Management Conference*, *Edith Cowan University, Perth*, pp. 67-73.

Nonaka, I. (1994), "A dynamic theory of organizational knowledge creation", *Organization Science*, Vol. 5 No. 1, pp. 14-37.

Okere, I., Van Niekerk, J. and Carroll, M. (2012), "Assessing information security culture: a critical analysis of current approaches", *ISSA 2012*, IEEE Xplore Digital Library, pp. 1-8.

Quinn, R.E. and Cameron, K. (1983), "Organizational life cycles and shifting criteria of effectiveness: some preliminary evidence", *Management Science*, Vol. 29 No. 1, pp. 33-51.

Ramachandran, S., Rao, C., Goles, T. and Dhillon, G. (2013), "Variations in information security cultures across professions: a qualitative study", *Communications of the Association for Information Systems*, Vol. 33, pp. 163-204.

Ramachandran, S., Rao, S.V. and Goles, T. (2008), "Information security cultures of four professions: a comparative study", *The 41st Annual Hawaii International Conference on System Sciences*, Big Island, HI, 7-10 January, pp. 454-464.

Rastogi, R. and von Solms, R. (2012), "Information security service culture – information security for end-users", *Journal of Universal Computer Science*, Vol. 18 No. 12, pp. 1628-1642.

Rest, J.R. (1986), *Moral Development: Advances in Research and Theory*, Praeger, New York, NY.

Robbins, S. (2001), *Organisational Behaviour*, Prentice Hall, NJ.

Rousseau, D. (1988), "The construction of climate in organizational research", in Cooper, C.L. and Robertson, I. (Eds), *International Review of Industrial and Organizational Psychology*, Wiley, Chichester, pp. 139-158.

Ruighaver, A.B., Maynard, S.B. and Chang, S. (2007), "Organisational security culture: extending the end-user perspective", *Computers & Security*, Vol. 26 No. 1, pp. 56-62.

Ruighaver, A.B., Maynard, S.B. and Warren, M. (2010), "Ethical decision making: improving the quality of acceptable use policies", *Computer & Security*, Vol. 29 No. 7, pp. 731-736.

Sabbagh, B.A. and Kowalski, S. (2012), "Developing social metrics for security modeling the security culture of it workers individuals (case study)", in Mosharka, J.M. (Ed.), *5th International Conference on Communications, Computers and Applications, MIC-CCA 2012*, *IEEE Xplore Digital Library*, pp. 112-118.

Sánchez, L.E., Santos-Olmo, A., Fernández-Medina, E. and Piatinni, M. (2010), "Security culture in small and medium-size enterprise". *ENTERprise Information Systems – International Conference, CENTERIS 2010, Viana do Castelo, Portugal*, *Springer, Berlin*, 20-22 October.

Schein, E.H. (1985), *Organizational Culture and Leadership*, Jossey-Bass, San Francisco, CA, pp. 315-324.

Schlienger, T. and Teufel, S. (2002), "Information security culture – the socio- cultural dimension in information security management", in Adeeb Ghonaimy, M., El-Hadidi, M.T. and Aslan, H.K. (Eds), *Security in the Information Society: Visions and Perspectives*, Kluwer Academic Publishers, Dordrecht, pp. 191-201.

Schlienger, T. and Teufel, S. (2005), "Tool supported management of information security culture application in a private bank", in Sasaki, R., Qing, S., Okamoto, E. and Yoshiura, H. (Eds), *Security and Privacy in the Age of Ubiquitous Computing – IFIP TC11 20th International Information Security Conference, 30 May-1 June, Chiba*, *Springer*, *NY*, pp. 65-77.

Schutt, R.K. (2001), *Investigating the Social World: The Process and Practice of Research*, Pine Forge Press, Thousand Oaks, CA.

Shaaban, H. and Conrad, M. (2012), "Democracy, culture and information security: a case study in Zanzibar", *Information Management & Computer Security*, Vol. 21 No. 3, pp. 191-201.

Shahibi, M.S., Rashid, R.M., Fakeh, S.K.W., Dollah, W.A.K.W. and Ali, J. (2012), "Determining factors influencing information security culture among ICT librarians", *Journal of Theoretical and Applied Information Technology*, Vol. 37 No. 1, pp. 132-140.

Shahri, A.B., Ismail, Z. and Rahim, N.Z.A. (2012), "Security effectiveness in health information system: through improving the human factors by education and training", *Australian Journal of Basic and Applied Sciences*, Vol. 6 No. 2, pp. 226-233.

Siponen, M., Pahnila, S. and Mahmood, A. (2007), "Employees' adherence to information security policies: an empirical study", in Venter, H., Eloff, M., Labuschagne, L., Eloff, J. and Von Solms, R. (Eds), *IFIP International Federation for Information Processing, New Approaches for Security, Privacy and Trust in Complex Environments*, Springer, Boston, MA, pp. 133-144.

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

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

Siponen, M., Wilson, R. and Baskerville, R. (2008), "Power and practice in information systems security research" *International Conference on Information Systems (ICIS*), Paris.

Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005), "Analysis of end user security behaviors", *Computers & Security*, Vol. 24 No. 2, pp. 124-133.

Thomson, K. and Van Niekerk, J. (2012), "Combating information security apathy by encouraging prosocial organisational behaviour", *Information Management & Computer Security*, Vol. 20, pp. 39-46.

Thomson, K.-L. and Von Solms, R. (2005), "Information security obedience: a definition", *Computer & Security*, Vol. 24, pp. 69-75.

Thomson, K.-L. and Von Solms, R. (2006), "Towards an information security competence maturity model", *Computer Fraud & Security*, No. 5, pp. 11-15.

Thomson, K.-L., Von Solms, R. and Louw, L. (2006), "Cultivating an organizational information security culture", *Computer Fraud & Security*, No. 10, pp. 7-11.

Thong, J.Y.L. and Yap, C.-S. (1998), "Testing an ethical decision-making theory: the case of softlifting", *Journal of Management Information Systems*, Vol. 15 No. 1, pp. 213-237.

Tsohou, A., Karyda, M., Kokolakis, S. and Kiountouzis, E. (2006), "Formulating information systems risk management strategies through cultural theory", *Information Management & Computer Security*, Vol. 14 No. 3, pp. 198-217.

Tsohou, A., Theoharidou, M., Kokolakis, S. and Gritzalis, D. (2007), "Addressing cultural dissimilarity in the information security management outsourcing relationship", in Lambrinoudakis, C., Pernul, G. and Tjoa, A.M. (Eds), *Trust, Privacy and Security in Digital Business*, Springer, pp. 24-33.

Van Niekerk, J.F. and Von Solms, R. (2010), "Information security culture: a management perspective", *Computer & Security*, Vol. 29, pp. 476-486.

Van Niekerk, J. and Von Solms, R. (2013), "A theory based approach to information security culture change", *Information (Japan)*, Vol. 16, pp. 3907-3930.

Von Solms, B. (2000), "Information security – the third wave?", *Computers and Security*, Vol. 19, pp. 615-620.

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

Warner, J. (2006), "Towards understanding user behavioral intentions to use IT security: examining the impact of IT security psychological climate and individual beliefs", *12th Americas Conference on Information Systems (AMCIS)*, AIS Electronic Library (AISeL), Acapulco, 4-6 August.

Westrum, R.J. (1993), "Cultures with requisite imagination", in Wise, J.A., Hopkin, V.D. and Stager, P. (Eds), *Verification and Validation of Complex Systems: Human Factors Issues*, Springer, Heidelberg, pp. 401-416.

Williams, P.A. (2009), "What does security culture look like for small organizations?", *7th Australian Information Security Management Conference*, *Edith Cowan University, Perth*, 1-3 December, pp. 48-54.

Williams, P.A.H. (2008), "In a 'trusting' environment, everyone is responsible for information security", *Information Security Technical Report*, Vol. 13 No. 4, pp. 207-215.

Woodhouse, S. (2007), "Information security: end user behavior and corporate culture", *Seventh International Conference on Computer and Information Technology*, *IEEE Xplore Digital Library, Aizu-Wakamatsu, Fukushima*, 16-19 October, pp. 767-774.

Zakaria, O. (2005a), "Employee security perception in cultivating information security culture", in Dowland, P., Furnell, S., Thuraisingham, B. and Wang, S.X. (Eds), *IFIP TC-11 WG 11.1 and WG 11.5 Joint Working Conference on Security Management, Integrity, and Internal Control in Information Systems*. Springer-Verlag, New York, NY, pp. 83-92.

Zakaria, O. (2005b), "Information security culture and leadership", *4th European Conference on Information Warfare and Security 2005, ECIW 2005*, *Academic Conferences Limited*, Glamorgan, pp. 415-420.

Zakaria, O. (2006), "Internalisation of information security culture amongst employees through basic security knowledge", in Fischer-Hübner, S., Lindskog, S., Lassous, G. and Yngström, L. (Eds), *Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006) on Security and Privacy in Dynamic Environments*, *Springer, New York, NY*, pp. 437-441.

Zakaria, O., Jarupunphol, P. and Gani, A. (2003), "Paradigm mapping for information security culture approach", in Slay, J. (Ed.), *4th Australian Conference on Information Warfare and IT Security*, *Adelaide*, 20-21 November, pp. 417-426.

Appendix 1

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 the people's values, language and practices. Ethnography has its rotes 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. It is not necessary that the people in the situation are aware of the researcher. This category is an extension of ethnography (Mingers, 2003)

(*continued*)

Table AI. Operational definitions of research methods

Research method	Operational definition
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

Table AI.

Appendix 2

Table AII.
Detailed analysis

Authors	Classification of aim	Research type	Research method	Theories
Alarifi *et al.* (2012)	The relation between culture and information security	Descriptive	Survey	–
Alfawaz *et al.* (2010)	Framework for understanding information security culture	Theory generating	Case study	–
Alnatheer and Nelson (2009)	Factors that contribute to information security culture	Theoretical	Subjective/argumentative	Hofstede's (1997) national culture framework, Schein's (1985) culture model
Alshare and Lane (2008)	The relation between culture and information security	Theoretical	Subjective/argumentative	Hofstede's (1997) national culture framework
Ashenden (2008)	Management challenges	Philosophical	Subjective/argumentative	–
Ashenden and Sasse (2013)	Practical work with cultivating an information security culture	Theory generating	Interviews	Organisational discourse theory (Hardy, 2001)
Božić (2012)	Factors that contribute to information security culture	Theoretical	Subjective/argumentative	Lazarus' (1993) stress model
Chang and Lin (2007)	The relation between culture and information security	Theory testing	Survey	Competing values framework (Quinn and Cameron, 1983)
Chen *et al.* (2008)	The relation between culture and information security	Theory testing	Experiment	Hofstede's (1997) national culture framework
Connolly and Lang (2012)	The relation between culture and information security	Theoretical	Literature review	–
Corriss (2010)	The relation between culture and information security	Philosophical	Subjective/argumentative	–
Da Viega and Eloff (2010)	Framework for cultivating an information security culture	Theory testing	Survey	Schein's (1985) culture model
Dojkovski *et al.* (2006)	Management challenges	Theory generating	Literature review, interviews	–
Dojkovski *et al.* (2007a)	Management challenges	Theory generating	Case study	–
Dojkovski *et al.* (2007b)	Framework for cultivating an information security culture	Theory generating	Case study, literature review	–

(*continued*)

Table AII.

Authors	Classification of aim	Research type	Research method	Theories
Dojkovski *et al.* (2010)	Framework for cultivating an information security culture	Theory generating	Case study, literature review	–
Fernando and Asai (2011)	Analysis of existing security cultures	Theory testing	Survey	Hofstede's (1997) national culture framework
Furnell and Thomson (2009)	The relation between culture and information security	Theoretical	Subjective/argumentative	Schein's (1985) culture model
Gaunt (2000)	Management challenges	Descriptive	Case study	–
Ghernaouti-Hélie (2009)	Management challenges	Philosophical	Subjective/argumentative	–
Ghernaouti-Hélie *et al.* (2010)	Approaches to assess information security culture	Descriptive	Case study	–
Goo *et al.* (2013)	The relation between culture and information security	Theory generating	Survey	–
Harnesk and Lindström (2011)	Framework for understanding information security culture	Theory generating	Case study	Harrald's (2006) organisational typology
Harris *et al.* (2010)	The relation between culture and information security	Theory testing	Survey	Hofstede's (1997) national culture framework, the four component model of moral development (Rest, 1986)
Helokunnas and Kuusisto (2003)	Factors that contribute to information security culture	Theoretical	Subjective/argumentative	–
Hovav and D'Arcy (2012)	The relation between culture and information security	Theory testing	Survey	Hofstede's (1997) national culture framework
Hu *et al.* (2008)	The relation between culture and information security	Theory testing	Survey	Theory of planned behaviour (Ajzen, 1991)
Hu *et al.* (2012)	Factors that contribute to information security culture	Theory testing	Survey	Theory of planned behaviour (Ajzen, 1991), competing values framework (Quinn and Cameron, 1983)
Ilvonen (2011)	The relation between culture and information security	Theoretical	Subjective/argumentative	–

(*continued*)

Authors	Classification of aim	Research type	Research method	Theories
Johnsen *et al.* (2006)	Management challenges	Theoretical[a]	Consultancy	Schein's (1985) culture model, Westrum's (1993) typology of organizational cultures
Johnson and Goetz (2007)	Practical work with cultivating an information security culture	Descriptive	Interviews	–
Knapp *et al.* (2007)	Factors that contribute to information security culture	Theory testing	Grounded theory, survey	–
Kolkowska (2005)	Approaches to assess information security culture	Theoretical	Subjective/argumentative	Hofstede's (1997) national culture framework
Kolkowska (2011)	Analysis of existing security cultures	Theory generating	Case study	Schein's (1985) culture model, value-focused thinking (Keeney, 1992)
Koskosas (2012)	The relation between culture and information security	Descriptive	Case study	–
Kraemer and Carayon (2005)	Framework for understanding information security culture	Descriptive	Interviews	–
Kraemer and Carayon (2007)	Framework for understanding information security culture	Theory generating	Interviews	Schein's (1985) culture model
Lacey (2010)	Existing practices	Philosophical	Subjective/argumentative	–
Lim *et al.* (2009)	The relation between culture and information security	Theoretical	Subjective/argumentative	Organisational culture framework (Detert *et al.*, 2000)
Lim *et al.* (2010)	The relation between culture and information security	Theory generating	Case study	–
Lowry *et al.* (2013)	The relation between culture and information security	Theory testing	Survey	Ethical decision-making model (Thong and Yap, 1998)
Luo *et al.* (2009)	The relation between culture and information security	Theoretical	Subjective/argumentative	Hofstede's (1997) national culture framework
Malcolmson (2009)	Framework for understanding information security culture	Descriptive	Survey, interviews	–

(*continued*)

Table AII.

Table AII.

Authors	Classification of aim	Research type	Research method	Theories
McCoy *et al.* (2009)	The relation between culture and information security	Theory testing	Survey	Hofstede's (1997) national culture framework
Nemati and Church (2009)	Framework for cultivating an information security culture	Descriptive	Case study	–
Ngo *et al.* (2005)	Framework for cultivating an information security culture	Theoretical	Subjective/argumentative	Individual transition process (Bridges, 2003)
Okere *et al.* (2012)	Approaches to assess information security culture	Descriptive	Qualitative content analysis, literature review	–
Ramachandran *et al.* (2008)	Analysis of existing security cultures	Theory generating	Interviews	Organisational culture framework (Detert *et al.*, 2000)
Ramachandran *et al.* (2013)	Analysis of existing security cultures	Theory generating	Interviews	Organisational culture framework (Detert *et al.*, 2000), Hall's (1959) classification of behavioural responses
Rastogi and von Solms (2012)	Framework for understanding information security culture	Theoretical	Subjective/argumentative	Schein's (1985) culture model
Ruighaver *et al.* (2010)	Framework for cultivating an information security culture	Descriptive	Interviews	–
(Sabbagh and Kowalski, 2012)	Approaches to assess information security culture	Descriptive	Case study	–
(Sánchez *et al.*, 2010)	Framework for cultivating an information security culture	Theoretical	Subjective/argumentative	–
Schlienger and Teufel (2005)	Approaches to assess information security culture	Theory testing	Case study	–
Shaaban and Conrad (2012)	The relation between culture and information security	Theory generating	Survey, interviews	Nine national culture dimensions (House *et al.*, 2004), competing values framework (Quinn and Cameron, 1983)

(*continued*)

Authors	Classification of aim	Research type	Research method	Theories
Shahibi *et al.* (2012)	Factors that contribute to information security culture	Theory testing	Experiment	Schein's (1985) culture model
Shahri *et al.* (2012)	Factors that contribute to information security culture	Theoretical	Literature review	–
Thomson and Van Niekerk (2012)	Framework for cultivating an information security culture	Theoretical	Literature review, subjective/argumentative	Goal-setting theory (Locke and Latham, 2002)
Thomson and von Solms (2005)	The relation between culture and information security	Theoretical	Subjective/argumentative	Schein's (1985) culture model
Thomson and von Solms (2006)	Approaches to assess information security culture	Theoretical	Subjective/argumentative	Conscious competence learning matrix (Howell and Fleishman, 1982)
Thomson *et al.* (2006)	Framework for cultivating an information security culture	Theoretical	Subjective/argumentative	Conscious competence learning model (Flower, 1999), modes of knowledge creation (Nonaka, 1994)
Tsohou *et al.* (2007)	Framework for understanding information security culture	Theoretical	Subjective/argumentative	Schein's (1985) culture model
Tsohou *et al.* (2006)	The relation between culture and information security	Theoretical	Subjective/argumentative	Grid/group typology from cultural theory (Douglas, 1992, Douglas and Wildavsky, 1982)
Van Niekerk and Von Solms (2010)	Framework for understanding information security culture	Theoretical	Subjective/argumentative	Schein's (1985) culture model, elasticity theory (Acs and Gerlowski, 1996)
von Solms (2000)	Existing practices	Philosophical	Subjective/argumentative	–
Vroom and von Solms (2004)	Framework for cultivating an information security culture	Theoretical	Subjective/argumentative	Schein's (1985) culture model

(*continued*)

Table AII.

Table AII.

Authors	Classification of aim	Research type	Research method	Theories
Warner (2006)	The relation between culture and information security	Theoretical	Subjective/argumentative	Theory of planned behaviour (Ajzen, 1991), psychological climate (Rousseau, 1988)
Williams (2008)	Framework for cultivating an information security culture	Theoretical	Subjective/argumentative	–
Williams (2009)	Factors that contribute to information security culture	Theoretical	Subjective/argumentative	–
Woodhouse (2007)	Factors that contribute to information security culture	Descriptive	Survey	–
Zakaria (2005a)	Framework for cultivating an information security culture	Theoretical[b]	Case study	–
Zakaria (2006)	Practical work with cultivating an information security culture	Theoretical[b]	Case study	–

Notes: [a] The use of the empirical data from consultancy is anecdotal and fragmented; the paper has therefore been classified as theoretical; [b] The use of the empirical data from case study is anecdotal and fragmented; the paper has therefore been classified as theoretical

Table AIII. Papers that we have been unable to analyse

Author	Reason why the analysis was not carried out
Bess (2009)	Unable to get a copy of the paper
Van Niekerk and Von Solms (2013)	Unable to get a copy of the paper
Gattiker (2008)	Unable to get a copy of the paper
Zakaria (2005b)	Unable to get a copy of the paper
Koskosas and Massalas (2008)	Unable to get a copy of the paper

About the authors

Fredrik Karlsson is a Professor in Information Systems at Örebro University, Sweden. He has previously held a research position at University of Skövde. He received 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 the Deputy Head of the School of Business at Örebro University. He is also a research leader of the research environment Centre for Empirical Research on Information Systems (CERIS). Fredrik Karlsson is the corresponding author and can be contacted at: fredrik.karlsson@oru.se

Joachim Åström is a Professor in Political Science at Örebro University, Sweden. His research focuses on new modes of governance in general, and issues concerning information and communication technologies, power and democracy in particular.

Martin Karlsson is currently a Postdoctoral Researcher in political science at Örebro University. His research interests revolve around the interplay between information technology and organizational as well as political processes. Karlsson published research widely in the areas of E-government, E-democracy and E-campaigning.

This article has been cited by:

1. Adele Da VeigaA cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument 1006-1015. [CrossRef]