Published in Computers & Security 92 (2020), https://doi.org/10.1016/j.cose.2020.101713

Defining organisational information security culture—Perspectives from academia and industry

Adéle da Veiga [a,*], Liudmila V. Astakhova [b], Adéle Botha [c], Marlien Herselman [c]

[a] School of Computing, College of Science, Engineering and Technology, University of South Africa (UNISA), Florida Campus, Johannesburg, South Africa
[b] Department of Information Security, School of Electronic Engineering and Computer Science, South Ural State University (National Research University), Chelyabinsk, Russia
[c] Next Generation Enterprises and Institutions, CSIR, Pretoria and School of Computing, College of Science, Engineering and Technology, University of South Africa (UNISA), Florida Campus, Johannesburg, South Africa

ABSTRACT

The ideal or strong information security culture can aid in minimising the threat of humans to information protection and thereby aid in reducing data breaches or incidents in organisations. This research sets out to understand how information security culture is defined from an academic and industry perspective using a mixed-method approach. The definition, factors necessary to instil the ideal information security culture and the potential impact of the ideal information security culture were investigated from both perspectives. A survey approach was implemented to obtain the views from industry and 512 respondents from organisations, many of which operate at an international level, participated in the survey. The research presents a description of information security culture, integrating the existing literature and expanding on it with the views of industry, thereby giving clarity to the concept. The ideal information security culture was identified with the top traits relating to aspects such as an aware and knowledgeable workforce implementing conscientious, caring behaviour to comply with policies as guided by management. The factors that could positively influence an information security culture were identified, consolidated and expanded to five external factors and twenty internal factors. Organisations that have a strong information security culture were identified as achieving mutual trust and integrity through the protection of their information. The description of an information security culture can be used as a baseline to define and understand the concept, identify a single, comprehensive set of factors to be implemented, comprehend the traits of such a culture, as well as what an organisation can achieve by having a strong information security culture. The analysis showed that scientific interpretations of the definitions and factors of information security culture are much wider than their understanding of the industry. Both the results from the scoping review of papers and the feedback from the industry experts are synthesised visually to provide an organisational information security culture model (OISCM). The definition, factors, and model that influence the organisational culture of information security, have prognostic value for industry. For scientists, this is an important topic of research on methods and forms of increasing the level of this knowledge.

Keywords

Information security culture, definition, factors, impact, human, key traits, model

1. Introduction

The focus on information security culture spans back many years and is still critical today. Academia and industry work to combat threats to information protection. Information security culture is important to combat risks from a human perspective as motivated in the early work conducted by the Organisation for Economic Co-operation and Development (OECD), which published the *Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security*, the United Nations' document entitled *Creation of a Global Culture of Cybersecurity* (United Nations General Assembly, 2003) and the Information Security Forum's work in 2002. While efforts have been underway to address the human element by focusing on information security culture, current employees are still

estimated as the highest source of security incidents, followed by former employees (PricewaterhouseCoopers, 2016), often related to carelessness or human error (Ponemon, 2018).

The OECD (2015) suggests that a culture of digital security should be established where stakeholders should address the risk of their own activities in the digital environment. The digital environment is also referred to as cyberspace where the concept of a cybersecurity culture is important. In an organisational context, the term "information security culture" is often used, cybersecurity culture being a subset (ENISA, 2017; Von Solms & Von Solms, 2018). Cybersecurity culture relates to the manner in which people perceive cybersecurity and the resultant behaviour in cyberspace that impacts on the protection of the digital information, systems and people (Da Veiga, 2016a; Von Solms & Van Niekerk, 2013). Information security culture can be understood as the way things are done by employees when processing information using organisational systems as well as cyberspace, which manifests in behaviour in an organisational context that impacts on the protection of information (Da Veiga & Eloff, 2010; Da Veiga & Martins, 2017).

Academia has worked on the concept of information security culture to define the term (AlHogail & Mirza, 2014; Astakhova, 2014; Da Veiga & Eloff, 2010; Schlienger & Teufel, 2002; Van Niekerk & Von Solms, 2005), to propose frameworks or models (Nel & Drevin 2019; AlHogail, 2015a; AlHogail, 2015b; Van Niekerk & Von Solms, 2005, 2006) to develop assessment methods (AlHogail, 2015a; AlHogail, 2015b; Da Veiga & Eloff, 2010; Da Veiga & Martins, 2015a; Da Veiga & Martins, 2015b; Geeling, Brown, & Weimann, 2016; Karlsson, Åström, & Karlsson, 2015; Ruighaver, Maynard, & Chang, 2007) and to investigate relationships of other constructs such as information security awareness and information security culture (Wiley, McCormac and Calic 2020). It is also necessary to understand the view of industry towards information security culture in order to align efforts and direct future research. Karlsson et al. (2015) performed a state-of-the-art review of information security culture between 2000 and 2013. One of their key conclusions was that no papers at that time investigated the ***impact*** ("fruits") of information security culture on information security in an organisation. A further review of information security culture definitions and frameworks was conducted by Mahfuth, Yussof, Baker, and Ali (2017) ranging from 2003 to 2016, concluding that there was not a standard ***definition*** of information security culture. They determined that the academic definitions of information security culture mostly focused on the work of Schein (2010). Nasir, Arshah, Ab Hamid, and Fahmy (2019) conducted a systematic literature review of information security culture using the PRISMA method and found that there is inconsistency in defining ***factors*** that conceptualise the ideal information security culture. The research papers included in the studies by both Karlsson et al. (2015) and Mahfuth et al. (2017) were derived from Scopus and leading electronic databases publishing academic research. Their studies did not establish industry's view of the ***impact*** of a strong information security culture, nor of the ***definition*** and ***factors to instil the ideal culture***. A definition of information security culture that is informed from an academic as well as industry context is lacking. Similarly, a list of factors to instil the ideal information security culture and the resultant impact as informed by both academia and industry are also lacking.

2. Research aims

The aim of this research was to determine the concept of information security culture from an industry perspective to complement existing theory. To achieve this, the following research question was formulated:

What constitutes an information security culture in organisations?

This research question was answered using a mixed-method whereby a literature review was conducted about the concept and an industry perspective was obtained. The literature review was conducted to summarise existing literature on information security culture definitions and factors to instil (cultivate/establish/improve) the ideal information security using a document analysis approach. The industry perspective of information security culture was obtained using a quantitative and qualitative research method with a survey to analyse the results and to integrate them with the literature perspective.

The remainder of the paper is structured as follows: In section 3 the background of information security culture definitions is discussed, followed by the scoping review in section 4. This is followed by section 5 where a summary is given of the factors, as derived from academic literature that could instil the ideal information security culture. Section 6 deals with the research methodology applied to obtain a perspective from the industry. The quantitative results are presented in sections 7 and 8. The discussion and interpretation are provided in sections 9 and 10, followed by the conclusion in section 11.

3. Background to information security culture

Despite the variety of definitions and interpretations of information security culture, there are a number of common aspects which the definitions address. Authors refer to the values, basic assumptions and behaviour of employees that are visible in artefacts (Da Veiga & Eloff, 2010; Schlienger & Teufel, 2002; Van Niekerk & Von Solms, 2010). Information security culture encompasses the thinking, feelings and everyday activity of employees (Sabbagh, Watterstam, & Kowalski, 2012). Special attention is paid to the values that guide employees in what behaviour should be considered as acceptable or unacceptable when processing information (Dhillon, Syed, & Pedron, 2016; Van Niekerk & Von Solms, 2010). It has been argued that “the information security culture focuses on the socio-cultural aspects of information security management” (Schlienger & Teufel, 2002: 198).

Initially, Schein’s organisational culture definition (1992, 2009) was used and information security culture was defined as "a natural aspect in the daily activities of every employee" (Schlienger & Teufel, 2002: 197). Culture is one of the most challenging aspects to change in an organisation and is evident beyond and organisation’s products, services, founders and leadership (Schein 1992). Schein’s organisational culture model comprises three distinct levels defined by him, namely artifacts, espoused values and basic underlying assumptions. Artifacts (the most superficial level, external manifestations of organisational culture) - language, manner of dressing

and communication, etc.). Proclaimed values - strategies, goals, philosophies. The basic concepts (the deepest level of organisational culture) are beliefs. These components, according to most researchers, are also components of information security culture.

Subsequent research also included the concept of knowledge (Helokunnas & Kuusisto, 2003; Van Niekerk & Von Solms, 2010). Other definitions of information security culture have become more comprehensive, including the concepts of perceptions, values, assumptions and knowledge with the aim of protecting information assets in the organisation in such a manner that it becomes second nature (AlHogail & Mirza, 2014). The dimensions of organisational culture (basis of truth and rationality; nature of time and time horizon; motivation; stability vs. change/innovation/personal growth; orientation to work, task, co-workers; isolation vs. collaboration/cooperation; control, coordination and responsibility; and orientation and focus – internal and/or external) as defined by Deter, Schroeder and Mauriel (2000) were also considered by researchers when investigating the information security culture in organsiations (Chia, Ruighaver & Maynard, 2002). The researchers of that study found the approached to be successful in understanding the quality of information security culture in an organisation.

Authors have also considered the protection of an organisation's information assets as a goal of information security culture (Alfawaz, Nelson, & Mohannak, 2010). At the same time, "people are very often perceived as an obstacle rather than an asset in this regard" (Furnell & Thompson, 2009: 5) as security incidents and breaches are often related to employee error or negligence (Da Veiga, 2018). However, today more and more authors are exploring information security culture from the human perspective as a critical resource to success in protecting information resources. A person can become either an object or a subject of social engineering, negative information and psychological influences or manipulation by intruders. Therefore, in further work, the concept of a culture of information and psychological security was introduced, defined as a way of organizing and developing life activity, in which the subject of information interaction recognizes himself as the subject of information and psychological security, is able to identify threats to information and psychological security, owns technologies for protecting against them and is capable of securely transforming the information environment (Astakhova, 2011).

Information security culture is a dynamic phenomenon. Scientists have paid special attention to the fact that the information security culture changes over time (Chia, et al. 2002; Ngo, Zhou, & Warren, 2005; Ruighaver et al., 2007; Da Veiga & Eloff, 2010). Organisations should focus on a balance between maintaining stability while also focusing on continuous development to ensure consistent protection of information resources in a changing environment.

Information security culture is often present in an organisation as dominant culture and as subcultures where different departments or job levels can each have a unique information security culture (Da Veiga & Martins, 2017). Where a subculture of information security is not conducive to the protection of information, it can be referred to as a counterculture, which is destructive towards the protection of information (Astakhova, 2010). Countercultures must be identified and actions implemented to purposefully direct them, thereby aligning them with the dominant information security culture. Astakhova introduced the concept of cultural capital, using the consolidation of knowledge, behaviour and skills to illustrate the organisation's competence to protect information resources, which gives the organisation a certain social status and standing in

society (Cole, 2019). This supports the view of Schein (2004) that the essence of culture is a reflection of the group's aspiration not only for self-preservation but also for development. The development of employees plays a critical role in instilling an information security culture in which information resources are protected, not only as a result of adequate technology and processes but also of having skilled employees and focusing on the cognitive aspects of their development (Astakhova, 2014).

The aim is to instil a culture in which information assets, including employees, are valued and protected, thereby obtaining social and economic benefits for the organisation (Astakhova, 2015) while minimising and mitigating security threats and incidents.

4. Scoping review of information security culture definitions

A scoping review was conducted, which is an initial review of the available literature with the objective of conducting a wide review of the research topic (Grant & Booth, 2009). This method was applied to compile a consolidated definition of information security culture from literature focusing on articles that have made a significant impact in the field of information security culture. Harzing's Publish or Perish software (POP) (Harzing, 2019) was used for the scoping review. Harzings is a software tool that retrieves highly cited papers within the topic being searched. A limitation of using Harzings is that the list of the most cited articles will not include recent publications on the topic nor publications in books or other languages, but for the purpose of this study it outlines the prominent articles that made a significant impact over time as evident in the citation metrics.

As a first step, the researchers did a search using Harzings to identify the ten most cited articles where the keywords "information security culture" were used in the title and body of the articles. No restriction was used for the timeframe. The identified papers were not coded as some only contained one or two sentences on the specific topic. An article that was listed in the top ten most cited articles, but did not focus on defining or describing the concept of information security culture was excluded, such as the article by Dhillon and Torkzadeh (2006), which focused on identifying information security objectives and not the information security culture, and that by Kruger and Kearney (2006), focusing on information security awareness. Kraemer, Carayon, and Clem (2009) and Shaw, Chen, Harris, and Huang (2009) were also listed but did not provide a definition or clarification of the term of information security culture and their article was therefore not included. The paper of Von Solms (2006) was also excluded as it only mentions information security culture as part of the fourth wave. Where papers were excluded the next cited paper was included to derive a list of ten papers. The final list of ten papers from step one was as follows:

- Vroom and Von Solms (2004)
- Da Veiga and Eloff (2010)
- Leach (2003)
- Da Veiga and Eloff (2007)
- Van Niekerk and Von Solms (2010)
- Von Solms and Von Solms (2004)
- Ruighaver, et al. (2007)
- Thomson, Von Solms & Louw (2006)
- Martins and Eloff (2002)

- Kraemer, Carayon (2006)

As a second step, the researchers performed another search in Harzings to identify articles where the keywords were used in only the title. From this list, the top ten cited papers were again extracted The same approach was applied to exclude papers if it did not cover the concept of information security culture as such, but perhaps only referred to it. Some of the papers that were excluded were the article by Flores, Antonsen, and Ekstedt (2014) focusing on behavioural information security governance factors that can drive information security knowledge sharing. Where papers were excluded, the next cited paper was included to derive a list of ten papers. The final list of ten papers from step two was as following:

- Da Veiga & Eloff (2010)
- Van Niekerk & Von Solms (2010)
- Thomson, Von Solms, & Louw (2006)
- Martins & Eloff (2002)
- Schlienger & Teufel (2003b)
- Schlienger & Teufel (2003a)
- Schlienger & Teufel (2002)
- AlHogail (2015b)
- Alfawaz et al. (2010)
- Da Veiga & Martins (2015a)

The two lists were then combined giving 20 papers of which four were duplicates, namely Da Veiga & Eloff (2010), Van Niekerk & Von Solms (2010), Thomson, Von Solms, & Louw (2006) and Martins & Eloff (2002). The four duplicate papers were removed deriving a final list of 16 papers.

These 16 papers were reviewed by the researchers to identify if a formal definition for information security culture is stated and, if not, if information security culture is discussed in a manner to describe the concept in an informal manner. The factors that are discussed in the research papers that could potentially influence the information security culture (e.g. governance, management, awareness and training, performance appraisals and risk assessment) were excluded in this section as it is discussed in section 5.

Table 1 presents a summary of whether the 16 papers included a formal information security culture definition or a description of the concept:

- Formal definitions: If authors pertinently define information security culture, the definitions are provided in quotes and the “Formal definition” column is marked with an X.
- Description: Where authors included discussions or descriptions about the concept of information security culture without a formal defining, the discussion relating to the term is summarised. The factors that could influence the information security culture are excluded. The “Description” column is marked with an X.

The research in Table 1 is presented in order of the number of citations each paper received, as depicted in the last column.

Table 1. Information security culture definitions and descriptions

	Information security culture definitions and descriptions	Formal definition	Description	Citations
1	A formal definition is not provided, but the concept is described as an ideal information security culture is evident where the employees of an organisation follow the guidelines voluntarily in such a manner that it becomes second nature. In describing the concept the authors refer to artefacts, espoused or shared values and basic tacit assumptions with a focus on changing the culture in line with security policies. (Vroom & Von Solms, 2004).		X	448
2	A formal definition is provided as, "an information security culture is therefore defined as the attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organisation's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour (i.e. incidents) evident in artifacts and creations that become part of the way things are done in the organisation to protect their information assets. This information security culture changes over time" (Da Veiga & Eloff, 2010: 198).	X		327
3	No formal definition is provided, but the concept is introduced as the creation of a strong security culture being the best way to motivate staff to behave consistently in a security-conscious way aligning their behaviour with corporate security mandates as created through strong leadership and by senior management (Leach, 2003).		X	263
4	A formal definition is provided, namely "An information security culture is defined as the assumption about those perceptions and attitudes that are accepted and encouraged in order to incorporate information security characteristics like the way in which things are done in an organisation" (Da Veiga & Eloff, 2007: 362).	X		244
5	No formal definition is provided, but an information security culture is described as consisting of four information security related levels, namely artefacts, espoused values, shared tacit assumptions and knowledge (Van Niekerk & Von Solms, 2010).		X	227
6	No formal definition is provided, but the concept of an information security culture is introduced in the conclusion of the paper. The paper introduces the concept of a group culture that is in line with policies, resulting in acceptable actions and behavioural patterns of the individual group members thus where actions of employees are in line with the vision of management. (Von Solms & Von Solms, 2004).		X	204
7	Authors explicitly say that they do not define or give a definite opinion of what good security culture is. They discuss information security culture in the context of aspects that could influence it such as governance and risk management. They do state the following: "In an ideal security culture, end-users, security administrators and managers will be motivated to reflect on their behaviour at all times, to assess how their behaviour influences security and what they can do to improve security" (Ruighaver et al., 2007: 59).		X	179
8	The authors use the term of Information Security Obedience is used as the term to define information security culture "as	X		162

	Information security culture definitions and descriptions	Formal definition	Description	Citations
	'de facto user behaviour complying with the vision of senior management as defined in the Corporate Information Security Policy' (Thomson, Von Solms & Louw, 2005: 74)" Thomson, Von Solms & Louw; 2006: 8).			
9	A formal definition is provided, namely "Information security culture can thus be defined as the assumption about which type of information security behaviour is accepted and encouraged in order to incorporate information security characteristics like the way in which things are done in an organisation" (Martins & Eloff, 2002: 205-206).	X		131
10	A formal definition is not provided, but information security culture is described as, "a subculture in regard to general corporate functions. It should support all activities so that information security becomes a natural aspect of the daily activities of every employee. The three layers of information security culture and their interaction are illustrated in Figure 1." (Schlienger & Teufel, 2003b:3), namely artefacts and creations, collective values, norms and knowledge, and basic assumptions and beliefs.		X	111
11	A formal definition is not provided but, information security culture is described as a subculture of the organisation's culture and comprises three levels, namely artefacts and creations, collective values, norms and knowledge, and basic assumptions and beliefs (Schlienger & Teufel, 2003a).		X	104
12	A formal definition is not provided, but the concept is described as following, "Security culture should support all activities in a way, that information security becomes a natural aspect in the daily activities of every employee" (Schlienger & Teufel, 2002: 197). "The information security culture focuses on the socio-cultural aspects of information security management" (Schlienger & Teufel, 2002: 198).		X	103
13	A formal definition is provided as, "The collection of perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction with information assets in [an] organisation with the aim of influencing employees' security behavior to preserve information security (Alhogail & Mirza, 2014b)'' (AlHogail, 2015b: 567).	X		75
14	A formal definition is not provided, but information security culture modes are proposed. In this paper information security culture is described in terms of security behaviour that comprises four modes, namely Not knowing-Not doing, Not knowing-Doing, Knowing-Not doing and Knowing-Doing. "These observations provide a basis for us to propose "the information security culture mode". In this mode, organisations would work towards developing an information security culture where all employees adhere to its information security policy and rules even when no one is around and when their behaviour is not being monitored." (Alfawaz et al., 2010:54).		X	72
15	A formal definition is provided namely, "An information security culture consists of the manner in which employees perceive and interact (behave) with the controls that are implemented to protect information. An information security culture therefore comprises the following: basic assumptions regarding information security and how to protect and interact with information in all formats; the attitudes and beliefs of employees in respect of information security, controls, compliance and how to protect and interact with information; and knowledge of the organisation's	X		68

	Information security culture definitions and descriptions	Formal definition	Description	Citations
	information security policy and compliance requirements, what information security incidents are, how to minimise risk to information when processing it, and what constitutes confidential or sensitive information from an organisational as well as a legislative perspective to mention but a few aspects" (Da Veiga & Martins, 2015a: 165).			
16	"Security culture is defined as aspects of the organisational security philosophy that directly or indirectly affects the overall security of the network" (Kraemer and Carayon 2006: 150).	X		44

Only the information security culture definitions and descriptions depicted in table 1, as derived from the 16 papers, were analysed to identify common themes and concepts. In total 13 themes were identified, which excludes any factors discussed in the papers that could influence the information security culture. The themes were derived by identifying terms that relate to the same concept of synonyms. For example, the theme behaviour comprises of terms such as behaviour, behave, daily activities, way things are done, actions, second nature and behave consistently. In total 14 of the 16 definitions or descriptions of information security culture included terms related to behaviour. Coding was applied only to the definitions in Table 1. The process was followed by three of the authors to eliminate biases and to ensure reliability.

Table 2 portrays the clusters of themes in column one. Column two gives a description of the theme as summarised from table 2. The authors that addressed the themes in the information security culture definition or description are depicted in the last column, "Authors".

Table 2. Information security culture definition themes

	Themes	Concepts derived from table 1	Authors
1	Behaviour	The definitions or descriptions that address behaviour (behave) or daily activities of behaviour or the way things are done including actions are clustered under behaviour. Second nature or behaving consistently is also included in this the behaviour cluster. Behaviour is mentioned by most of the authors which are the manner in which organisations culture develops.	Alfawaz, et al., 2010 Alhogail, 2015b Da Veiga & Eloff, 2007 Da Veiga & Eloff, 2010 Da Veiga & Martins, 2015a Leach, 2003 Martins & Eloff, 2002 Van Niekerk & Von Solms, 2010 Van Solms & Von Solms, 2004 Von Solms, 2006 Vroom & Von Solms, 2004 Ruighaver et al., 2007 Schlienger & Teufel, 2002 Schlienger & Teufel, 2003b Thomson et al., 2006
2	Human	The human element relating to either employees, individuals, groups, stakeholders, end-users, group members are clustered under human linking to the human element as the source of the behaviour which results in the emerging culture.	AlHogail, 2015b Alfawaz et al., 2010 Da Veiga & Eloff, 2010 Da Veiga & Martins, 2015a Leach, 2003 Von Solms & Von Solms, 2004 Von Solms, 2006

	Themes	**Concepts derived from table 1**	**Authors**
			Vroom & Von Solms, 2004 Ruighaver et al., 2007 Schlienger & Teufel, 2002 Schlienger & Teufel, 2003b Thomson et al., 2006
3	Artefacts and creations	The words artefact and creations emanate from Schein's definition of organisational culture and are used in a number of definitions and descriptions.	Da Veiga & Eloff, 2010 Schlienger & Teufel, 2003a Schlienger & Teufel, 2003b Van Niekerk & Von Solms, 2010 Vroom & Von Solms, 2004
4	Values, norms and knowledge	The words value, norms and knowledge emanate from Schein's definition of organisational culture and is used in a number of the definitions and descriptions.	AlHogail, 2015b Da Veiga & Eloff, 2010 Da Veiga & Martins, 2015a Schlienger & Teufel, 2003a Schlienger & Teufel, 2003b Van Niekerk & Von Solms, 2010 Vroom & Von Solms, 2004
5	Basic assumptions and beliefs	The word assumptions and beliefs emanate from Schein's definition of organisational culture and are used in a number of definitions and descriptions.	AlHogail, 2015b Da Veiga & Eloff, 2007 Da Veiga & Eloff, 2010 Da Veiga & Martins, 2015a Martins & Eloff, 2002 Van Niekerk & Von Solms, 2010 Schlienger & Teufel, 2003a Schlienger & Teufel, 2003b Vroom & Von Solms, 2004
6	Organisation	The definitions and descriptions of information security culture relate to organisations with some definitions specifically including the term organisation.	AlHogail, 2015b Da Veiga & Eloff, 2007 Da Veiga & Eloff, 2010 Da Veiga & Martins, 2015a Martins & Eloff, 2002 Schlienger & Teufel, 2003a Schlienger & Teufel, 2003b Vroom & Von Solms, 2004
7	Protect information	Various definitions and descriptions include the protection of information assets within the context of preserving security and protecting information. The protection also extends to improving security of information and information assets that are visible in security characteristics or controls.	AlHogail, 2015b Da Veiga & Eloff, 2007 Da Veiga & Eloff, 2010 Da Veiga & Martins, 2015a Leach, 2003 Ruighaver et al., 2007
8	Management	Management	Leach, 2003 Schlienger & Teufel, 2002 Thomson et al., 2006 Von Solms & Von Solms, 2004 Von Solms, 2006
9	Attitudes/ perception	The words attitude and perception emanates from the individual tier of organisational behaviour and is used in a number of definitions.	AlHogail, 2015b Da Veiga & Eloff, 2007 Da Veiga & Eloff, 2010 Da Veiga & Martins, 2015a
10	Policy	Some definitions and descriptions relate the human behaviour to be in line with	Alfawaz et al., 2010 Da Veiga & Martins, 2015a Thomson et al., 2006

	Themes	Concepts derived from table 1	Authors
		the information security and other related policies.	Von Solms & Von Solms, 2004 Vroom & Von Solms, 2004
11	Change	Some authors of the papers referred to changing the information security culture.	Da Veiga & Eloff, 2010 Thomson, Von Solms & Louw, 2005 Vroom & Von Solms, 2004

The predominant themes from table 2 are behaviour of humans in an organisational context. The behaviour over time becomes part of the way things are done, i.e. second nature, as a result of employee assumptions, values and beliefs, their knowledge and attitude towards and perception of the protection of information assets. The information security culture is directed by the vision of senior management as defined in the information security policy and is visible in the artefacts of the organisation and behaviour exhibited by employees.

While the vision of senior management and the information security policy direct employee behaviour, which over time becomes the way things are done or as such a culture, there are also other factors that can influence the information security culture. The next sections provide an overview of these factors (which was excluded in the previous two tables) from a literature perspective.

5. Factors to create the ideal information security - academic research

For an organisation in the process of forming and developing an information security culture, it is important to take into account all the factors and, if possible, to determine the degree of dependence of the information security culture on each of them. Factors affecting information security culture can be classified according to various criteria: by level of influence (micro and macro level); on the environment of occurrence (external and internal); in the direction of influence (protected information, information system user); in order of importance (important and less important); by degree of distribution (factors of general and local action), etc.

Among these factors, a special role in the formation and development of information security culture belongs to a group of external and internal factors (Da Veiga & Martins, 2017). The concept of the external environment contains everything that is outside the enterprise, but concerns all spheres of its activity. Environmental factors (external factors) are objective and affect the information security culture, either contributing to or hindering its development. The factors of the internal environment (intra-organisational factors) relate to the organisation; therefore, they are characterised to a certain degree by the subjectivity of influence.

Our study ultimately aims to develop technologies for effective management decisions of the organisation's information security culture with the aim of increasing it. Therefore, as a methodological basis for the classification of factors of influence on information security culture, we used the classical theory of organisation management (Mescon, Albert and Khedouri 1988), according to which any operations of an organisation (including management of organisational culture and information security culture) are influenced by external (environmental factors) and internal (internal organisational factors) factors.

Environmental factors include factors of direct and indirect effects. Direct impact factors directly affect the organisation's operations: suppliers, labor, laws and regulatory agencies, consumers and competitors. Indirect impact factors may not have a direct or immediate effect on operations of the organisation but could also have an influence. These factors include the state of the economy, scientific and technological progress, socio-cultural and political changes, the influence of group interests and significant events that could affect the organisation across countries according to Mescon, Albert and Khedoui (1988).

This approach is consistent with the rational theory of organisational culture of Edgar Schein (2010) as it considers purposeful management of the process to cultivate an organisational culture. According to this theory, organisational culture will be formed because of joint overcoming by the organisation's employees of the difficulties of the processes of external adaptation and internal integration. External adaptation is the organisation's response to environmental requirements. The difficulties of external adaptation are the problems of the organisation's survival in the market, finding its market niche, the formation of relations with business partners, consumers and competitors (Schein 2010).

On this basis, we grouped environmental factors (1) that affect the culture of information security as part of the organisational culture into five groups: 1.1. National culture. 1.2. Political and legal factors. 1.3. Economic factors. 1.4. Socio-cultural factors. 1.5. Technical and technological factors. Direct and indirect factors may be included in each group. For example, to economic factors, we attribute the general state of the country's economy (indirect influence factor) and the state of individual industry markets: suppliers, consumers, competitors, labour resources (direct influence factor).

According to the theory of organisational culture of Schein (2010), internal integration occurs in the process of a joint decision by members of the organisation of tasks, achievement of common goals, and resolution of basic internal problems. They are closely related to the deep ideas of the individual about the nature of man, the nature of the human activity, the relationship between people, about truth, time and space according to him.

In studies of information security culture factors, external influence is also attributed to factors external to the person (that is, the employee) that may affect the organisation's information security culture. Internal influence refers to internal factors associated with the individual, such as personality, which can influence how a person perceives intellectual property from his belief system, personality or experience (Padayachee 2012, Hellriegel, Slocum and Woodman 1998, Da Veiga and Martins 2017).

However, such a limitation of internal factors of influence on organisational culture does not allow us to consider information security culture as an object of management in a wider, organisational context. Therefore, in the process of classifying the internal, as well as external factors of information security culture, we used the management theory. According to the management theory, the number of internal organisational factors (i.e. internal variables of the organisation and situational factors within the organisation) other than the external environment include not only people but also goals, objectives, structure, and technology (Mescon, Albert and Kehdouri 1988).

The level and strategy of managing an organisation are influenced by the general condition of the organization; determined by its goals and objectives of protecting information in accordance with the stage of its life cycle. This is due to the information security culture corporate factors identified by us (2.1.): 2.1.1. The internal state of the organisation (stability, dynamism, business activity). 2.1.2. Stage of the life cycle of the organisation. 2.1.3. The level of the overall organisational culture of the enterprise. 2.1.4. Availability of a system for protecting confidential information in an organisation. 2.1.5. Resources.

The structure and technologies of the organisation assume the presence of functional zones and certain management technologies used to achieve the goals of the organisation. For information security culture, such a functional area is the sphere of IT functioning and information protection and - the controls used for this. This is due to the functional factors we have identified - information and management factors (2.2.): 2.2.1. Management 2.2.2.Information security and policies and procedures. 2.2.3. Information security risk management. 2.2.4. Operational management. 2.2.5. Change management. 2.2.6. Personnel information security management. 2.2.7. Information security education training, awareness and communication. 2.2.8. Information security behaviour management. People as an intra-organisational factor involve the analysis of such aspects of the individual behavior of an employee of an organisation as abilities, relationships, needs, values, expectations and perceptions (Mescon et al. 1988). This determines the factors of influence on the information security culture of the organisation associated with the personnel (2.3.): 2.3.1. Personality and values. 2.3.2. Needs. 2.3.3. Emotional condition. 2.3.4. Knowledge of information security. 2.3.5. Information security compliance. According to the concept of interdependence of internal variables in an organisation, all intra-organisational factors are closely interrelated, a change in one of them affects all the others (Mescon, et al. 1988).

Closely intertwined are the intra-organisational factors that we have identified that affect information security culture. This harmonic relationship is expressed in the field of information security by the concept of "trust". Trust is the ontological status of information security, based on the theory of trust (Askakhova 2016). Therefore, we identified factors of mutual trust between the employer, employees and customers (2.4.) as a separate group of intra-organisational factors. We attributed to them: 2.4.1. Mutual trust between the employer and employees, as well as between employees of the organisation. 2.4.2. Customer trust in the organisation.

Having developed a systematic classification of factors of information security culture as an object of management, we undertook an analysis of approaches to the content of individual factors that various researchers proposed in their publications. As such, the 16 papers of table 1 were included as a starting point supplemented by other relevant studies in information security culture. Table 3 in column 1 indicates whether the factor is considered as an internal or external influence on the IS culture. Researchers who suggested factors that may influence the culture of information security are listed in column 2. Factors are described in column 3.

Table 3. Factors that could influence an information security culture from literature

Factors influencing information security culture	Researchers	Description
1. External environmental factors		
1.1 National culture	Alfawaz et al., 2010; Flores et al., 2014; Sherif, Furnell, & Clarke, 2015.	National culture influences the way information is processed as well as the protection thereof. National culture also affects the information security culture. Privacy aspects are for example dealt with differently across national cultures, so also the free flow of information, openness and transparency, which could be open or limited.
1.2 Political and legal factors	AlHogail, 2015b; Bulgurcu, Cavusoglu, & Benbasat, 2010; Da Veiga & Martins, 2015b; Ifinedo, 2014; Knapp, Morris, Marshall, Byrd, 2009; Lim Chang, Ahmad, Maynard, 2012; Schlienger & Teufel 2002.	The development and implementation of government policies in the field of information security in the country, government initiatives, the level of development and implementation of legislation in the field of information security and information security culture have an impact on information protection and security in an organisation - all this creates favourable conditions for a positive information security culture.
1.3 Economic factors	Kuznetsova, 2005; Martins, & Eloff, 2002; Astakhova, 2010.	Periods of economic crises in the country may be accompanied by legal nihilism, "shadow" factors (corruption, criminal communities, clan groups) and, as a result, increased threats to business information security and the emergence of countercultures in information security culture. Post-crisis periods could have a positive effect on the development of an information security culture.
1.4 Socio-cultural factors	Astakhova, 2017 Flier, 2015; Schlienger and Teufel 2002.	Different ideas of employers and workers on social welfare dominate in different socio-cultural periods of the development of society. The subjects of information security culture should be aware of this - both employers and employees of the organisation – as the success of the development of an information security culture in the organisation also depends on it.
1.5 Technical and technological factors	Alhogail 2015b, Greig, Renaud & Flowerday, 2015; Alfawaz et al., 2010; Dojkovski, Lichtenstein, & Warren, 2007; Lim et al. 2012.	The level of digitalisation in different countries has an impact on innovative development and the degree of intellectualisation of labour. The types of information security threats and their danger and, as a result, attention (or inattention) to the problems of the information security culture are affected by this. The high level of information security technology and information technology vendors could influence the development of an information security culture.
2. Internal factors		
2.1 Organisational factors		
2.1.1 The internal state of the organisation (stability, dynamism, business activity)	Greig et al. 2015; Noorman, Nazrin, & Khairulnizan, 2017; AlHogail, 2015; Alfawaz et al., 2010; Dojkovski et al., 2007; Helokunnas &	The crisis state of the organisation or periods of instability of the enterprise, associated with a shortage of material, financial and technological resources, can lead to the emergence of countercultures; getting employees to step up and challenge the dominant information security culture. Internal post-crisis periods could also have a positive effect

Factors influencing information security culture	**Researchers**	**Description**
	Kuusisto, 2003; Schlienger & Teufel, 2002	on the development of an information security culture in an organisation.
2.1.2 Stage of the life cycle of the organisation	Schein, 2010.	In mature and ageing organisations, where conservative views and bureaucratic tendencies are very strong, there is a risk of information security countercultures threatening the dominant information security culture. Therefore the life cycle of the organisation should also be considered.
2.1.3 The level of the overall organisational culture of the enterprise	Alnatheer & Nelson, 2009; Reid, Van Niekerk, & Renaud, 2014; Tang, Li, & Zhang, 2015.	The organisational culture also has an effect on information security culture.
2.1.4 Availability of a system for protecting confidential information in an organisation	Williams, 2009; Parsons, Calic & Barca, 2016; Parsons et al., 2017.	The experience of employees in the field of protection of confidential information forms the knowledge, values, needs and patterns of their behaviour. This could have a positive effect on increasing the level of information security culture.
2.1.5 Resources	Alhogail 2015b; Lim, Ahmad, Chang & Maynard 2010; Da Veiga & Eloff 2010.	Resources are required for the implementation and/or change of an information security in an organisation. Budget and funding are important to implement security practices of which return on investment should also be demonstrated.
2.2 Management factors		
2.2.1 Management and governance	AlHogail, 2015; Alshaikh, Ahmad, Maynard, & Chang 2014; Da Veiga, & Eloff 2010; Da Veiga, & Eloff, 2007; Faily, Furnell, & Fléchais, 2010; Flores & Ekstedt, 2016; Koh, Ruighaver, Maynard & Ahmad, 2005; Leach, 2012; Lim, et al. 2010; Lim et al. 2012 Sherif et al., 2015; Wilderom, Van den Berg, & Wiersma, 2012; Zakaria, Gani, Nor & Anuar, 2007.	Management, leadership, governance together with roles and responsibilities, buy-in and accountability from management towards information security in the organisation are corner stones to inculcate a strong information security culture. Management has to define the organisation's information security strategy, lead by example and establish sponsorship. Disrespect for the history, traditions and style of leadership in the organisation can lead to the undermining of the dominant information security culture and the emergence of information security countercultures. Management should also formally assign information security responsibility.
2.2.2 Information security policies and procedures	Da Veiga, & Eloff 2010; Da Veiga, 2016b; Box & Pottas, 2013; Knapp et al., 2009; Lim, et al. 2010; Sherif et al., 2015; Thomson et al., 2006; Von Solms & Von Solms 2004; Vroom & Von Solms, 2004.	The knowledge and perception that employees have about the information security policy requirements could influence the information security culture. The information security policy, procedures and standards direct the information security culture. It also aids in establishing shared values and beliefs. Aligning the information security policy with best practice is also an important aspect to ensure.
2.2.3 Information security risk management	Da Veiga, & Eloff, 2010; Shameli-Sendi, Aghababaei-Barzegar, & Cheriet, 2016; Munteanu & Fotache, 2015; OECD,	The concept of an information security risk culture is emphasised in order to minimise information security risk. The information security culture could be influenced in the way that the organisation identifies, prevents, detects and responds to information security incidents.

Factors influencing information security culture	**Researchers**	**Description**
	2002; Sabbagh et al., 2012.	The information security risk prevention system, the practice of checking employees when they are hired and monitoring their actions, all reduce personnel risks and increase the likelihood of successful development of an information security culture.
2.2.4 Operational management	Shameli-Sendi et al., 2016; Ben-Asher & Gonzalez, 2015; Hassan & Ismail, 2012; Knapp et al., 2009; Vroom & Von Solms 2004	Operational management incorporates the management of aspects such as using a risk assessment approach to govern information security, including monitoring and review, as well as internal and external audits and using international standards such as ISO27001 or Cobit, which could aid in directing a positive information security culture.
2.2.5 Change management	AlHogail, 2015; Chia, et al., 2002; Hassan & Ismail, 2012; Ngo, et al., 2005; Ruighaver et al., 2007; Vroom & Von Solms, 2004.	Information technology, information security, the management and operations thereof and processes should include change management, which could aid employees to integrate and accept change in order for it to become part of the information security culture over time.
2.2.6 Personnel information security management	Furnell & Rajendran, 2012; Leach, 2012; Padayachee, 2012.	The result of personnel management should be the creation of favourable working conditions for employees of an organisation that could affect the information security culture: ease of use of systems, low staff turnover, independence from temporary employees, staff competence and effectiveness of monitoring procedures, job satisfaction, safety methods, disciplinary procedures, monitoring safety, supervision, efficiency and rewards.
2.2.7 Information security education, training awareness and communication	Da Veiga & Martins, 2015a; Hovav & D'Arcy, 2012; Leach, 2012; Lim, et al. 2010; Lim et al. 2012; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014; Safa et al., 2015; Schlienger & Teufel 2003b; Sherif et al., 2015; Thomson, Von Solms & Louw 2006. Wiley, et al., 2020.	Information security education, training and awareness (SETA) have a positive influence on the information security culture over time as established in previous studies. SETA is implemented to help employees to understand the risk and threats to information, what and how to implement information security controls and how to comply with the information security policies, procedures and related standards. Various researchers have also emphasised the important role of communication which is necessary to update employees about changes or new requirements for information security.
2.2.8 Information security behaviour management	Gabriel & Furnell, 2011; Alfawaz et al., 2010; Da Veiga & Eloff, 2010; Hassan & Ismail, 2012; Herath & Rao, 2009; Sherif et al., 2015.	Employees exhibit certain behaviour when they interact with information security controls, which researchers refer to as security behaviour. The objective is to instil security behaviour that is contributing to the protection of information assets and aligned to the organisation's information security policies as opposed to behaviour that results in risks and threats to the protection of information.
2.3 Human (related to employees) factors		
2.3.1 Personality and values	Astakhova, 2013; Dojkovski et al., 2007; Martins, & Eloff, 2002; Tolah Furnell, & Papadaki, 2017.	Values such as responsibility, integrity, trust, ethicality, values, motivation, orientation and personal growth could have an impact on the information security culture.

Factors influencing information security culture	Researchers	Description
2.3.2 Needs	Astakhova, 2010; Van Niekerk & Von Solms, 2005, 2006; Da Veiga & Martins, 2017.	Personal dissatisfaction of employees can cause intentional information security incidents – resulting in a counter information security culture.
2.3.3 Emotional condition	Gabriel & Furnell, 2011; Faily et al., 2010; Furnell & Rajendran, 2012; Hu, Dinev, Hart, & Cooke, 2012; Padayachee, 2012; Parsons et al., 2014; Sherif et al., 2015.	The emotional state of the employee (working time, intensity and productivity of labour, working conditions, the socio-psychological atmosphere in the enterprise, wage level, established criteria of work: urgency and accuracy of the assignment, obligations towards other people, etc.) affects motivation for activity and job satisfaction which could impact on the information security culture. Other soft issues such as media coverage, personal benefits, competence, ethics and commitment together with personality types could also play a role.
2.3.4 Knowledge of information security	Park, Kim, & Park, 2017; Hassan & Ismail, 2012; Thomson et al., 2006; Van Niekerk & Von Solms, 2006; Van Niekerk & Von Solms, 2010; Saleh, Refai, & Mashhour, 2011.	Employees' knowledge of information security, obtained throughout their lives and during the implementation of awareness, training and education programmes, has a positive effect on the development of an information security culture in an organisation. Each employee has their own knowledge and understanding of the information security policy and controls which influences how they process organisational information.
2.3.5 Information security compliance	Da Veiga, & Eloff, 2010; D'Arcy & Greene, 2014; Furnell & Thompson, 2009; Parsons et al., 2014; Tsohou, Karyda, & Kokolakis, 2015.	Knowledge of the information security policy and related procedures could have a positive impact on employees' attitude towards compliance with information security policies. One would expect that an organisation with a strong or positive information security culture also exhibits compliance as a visible trait.
2.4 Factors of mutual trust of the employer, employees and customers		
2.4.1 Mutual trust between employer and employees, as well as between employees of the organisation	Astakhova, 2015, 2018; Chia, Ruighaver & Maynard, 2002; Da Veiga & Martins, 2015a; Da Veiga & Eloff, 2007; Ruighaver, et al. 2007; Reid et al., 2014; Van Niekerk & Von Solms, 2010;	Trust between all parties in an organisation is important for the development of the information security culture. Collaboration and cooperation based on mutual trust are necessary for effective information security and for the development of an information security culture. Harmonisation of knowledge, values, needs and behaviour of the employer (to ensure the organisation's information security) and employees (for self-realisation and self-development) can contribute to the successful development of the information security culture.
2.4.2 Customer trust in the organisation	Da Veiga & Martins, 2015b; Da Veiga & Eloff, 2007.	The trust of clients in the organisation in relation to the preservation of private information and their trust in the messages of the organisation increase the responsibility of the employer and employees for the information security organisation and contribute to the improvement of information security culture.

Each of the justified factors is important and has its own field and power of influence. Their range will differ in different periods of time, which requires constant attention from management.

6. Research methodology

Mixed methods were applied as the methodological approach to validate the theory from literature conducted using document analyses. This implies that both quantitative and qualitative methods were used concurrently (QUAN + QUAL) e. This combination of the two designs allows researchers to provide comprehensive evidence of the research problem (Johnson & Onwuegbuzie, 2004). The pragmatist world view is applied in this paper as it informs the practical implications of the findings and it supports mixed methods as the methodological approach (Creswell & Creswell, 2017). In this context, the research problem is defined in variables to address the quantitative method as well as themes that support the qualitative domain (Creswell, 2013; Saunders, Lewis, & Thornhill, 2016). The variables are quantitatively measured to determine "the objective reality that exists out there in the world" (Creswell & Creswell, 2017, p. 7), in other words, measurable facts that can produce data (Saunders et al. 2016). Through the use of a semi-structured questionnaire data was collected to support both the quantitative and qualitative methods concurrently (Creswell & Clark, 2017). In this study the view of industry towards concepts in information security culture is measured which can be used to complement existing academic theory about the concept.

6.1 Questionnaire

The objective of the questionnaire was to understand the concept of information security culture from an industry perspective. Nine open-ended questions were specifically included to answer the research questions of this study. These questions addressed concepts such as the ideal information security culture, top traits of security culture and obstacles to improving a security culture. Other researchers also used qualitative studies to understand the concept of information security culture such as Lim, et al. (2012) who used interviews focussing on the implementation of information security practices in order to derive the key organisational culture characteristics. They focused on characteristics as opposed to defining the concept of information security culture and did not publish the questionnaire. As such, the open-ended questions of this study were developed specifically to answer the research questions of this study.

Apart from the nine open-ended questions, ten background questions and ten Likert scale questions were included. The majority of these questions were adapted from the ISCA questionnaire as indicated in Appendix A:

Open-ended questions
The focus was to define the concept of information security culture. Therefore, a question was formulated focussing specifically on the definition of information security culture, namely "What would you define as the ideal information security culture for your organisation?" To further explore the concept of information security culture two more questions were asked, namely:

- What would you regard as the top three traits of a strong information security culture?
- What is that one single thing that you would most like to see your organisation do to create a good security culture amongst employees?

Various studies have pointed out that human behaviour is a threat to information security (Lim, et al. 2012, Da Veiga 2018) with the behaviour of employees over time resulting in the information

security culture (Thompson et al. 2006, Da Veiga and Martins 2017). The concept of behaviour was also the most common theme in the literature descriptions of information security culture in table 1. As such, two open questions were asked to explore the concept of behaviour and if industry also believed human behaviour could be seen as root cause of information security breaches. Two general questions were used so as not to create bias in terms of the concept of behaviour.

- What employee behaviour do you believe could have a negative impact on the protection of information in your organisation?
- What would you regard as the root cause of information security or data breaches in your organisation?

A qualitative study was performed by Lim, et al. (2010) in a financial institution and government institution where they conducted semi-structured interviews to identify emerging concerns and challenges in the information security culture context. Aspects such as senior management support, enforcement of information security policies and security awareness were identified. While challenges were identified by them, the researchers of this study opted not to use those in the open-ended questions of this study to prevent leading questions. To limit bias the researchers used a general question whereby participants can identify any aspects they believe could be seen as a challenge or obstacle to an information security culture. The following question was defined:

- What would you regard as the greatest obstacles to improving the information security culture in your organisation?

To explore the possible outcome of a strong information security culture two questions were asked, one from the perspective of what organisations can achieve and the other to establish how respondents felt their organisation fared.

- What can organisations that have a strong information security culture achieve?
- How do you believe has your organisation fared in terms of the way it deals with information security?

The last question was added asking, “Why is information security important for your organisation?” to establish why information security could be seen as an important concept to respondents.

Background questions

The background questions were asked with yes-no and multiple response scales with the objective to understand the information security context of the organisations that participated. This gave the researchers a view of whether organisations implemented some of the factors that could influence an information security culture in order to obtain a view of the information security culture at artefact level. Questions related to aspects such as whether an information security policy was in place, whether the organisation had an information security officer, if staff received security awareness training, if a reporting line was in place, and so on.

Likert scale questions
The Likert scale questions were included to gain insight in whether the organisations believed information security is necessary and important. This links to the concept of espoused values in the information security culture definition to determine if information security was valued if confidential information was valued and protected and if compliance was valued. These questions did not represent a complete list of factors or values but were used to obtain background information of the participating sample.

The company, iFeedback (2019), was used to conduct the questionnaire administration, survey distribution, and data collection. As part of this process, a pilot test was conducted by iFeedback to ensure that the questions were understandable and applicable to the participating sample. Some of the biographical questions were adapted and some of the questions scales. For example, the country question was added and the scale of the Likert questions was changed from a 3-point scale (Yes, No, Do not know) to a 4-point scale (Never, Rarely, Very often, Always). Terminology was also revised for example, "Acceptable Usage Policy" was added to question 11 to refer the name of the information security policy organisations have for end-users who would be answering the questionnaire. A definition section was added with terms like information security and culture. The final questionnaire was also sent for language editing.

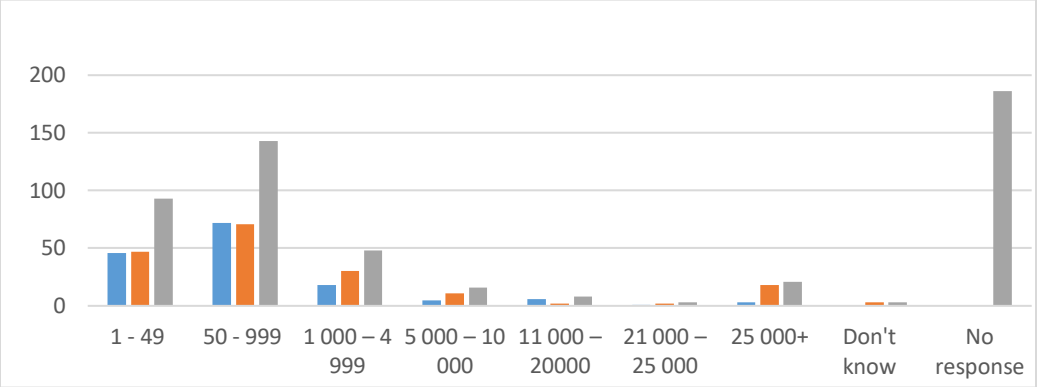
The project received ethical clearance from the university (076/ADV/2016/CSET_SOC) and as such the first page of the questionnaire included an invitation letter explaining the research project to the participants, that it is anonymous, voluntary, that information will be kept confidential and that results will be used for research purposes. A consent section was also included upon which respondents could proceed with the survey if they consented in order to ensure compliance with the research ethics policy of the university.

6.2 Sample

The semi-structured questionnaire was sent out to industry organisations based mainly in South Africa, but some also had international offices. The database of participants is managed by iFeedback (2019) for the purpose of research surveys conducted by industry and academia. Participants were sampled by applying a non-probability convenience sampling technique (Saunders et al., 2016). A total of 512 responses were obtained, 261 of which were fully completed questionnaires. An average of 331 respondents completed all the biographical sections of the questionnaire and 347 respondents completed all the Likert questions.

It was noted that 32% of the responses represented executive level management with 14% top management, 29% managerial, 19% operational staff and the remaining administrative staff. The responses represented organisations in financial services (13%), other (13%), technology and software (11%), education (10%), services (8%), public services (7%), industrial (6%), consumer products (6%), healthcare (5%), communication (5%), energy (5%) and a few other industries representing less than 5%. The majority of the participants were from private organisations (66%), with a third representing public organisations. Of importance to note is that small and medium organisations were represented in the sample as well as large organisations, figure 1.

Figure 1. Organisational sizes



The responses represented organisations that operated in a number of countries, with the majority across Africa and in Europe, see table 4. Although the study was conducted in South Africa, the results give an indication of possible trends in other countries.

Table 4. Country representation

In which countries does your organisation operate?	**Percentage**
1. Africa	48%
2. Europe	19%
3. Middle East and Asia Pacific	11%
4. North America	9%
5. South America	7%
6. Other	5%

6.3 Data analysis

6.3.1 Quantitative analysis

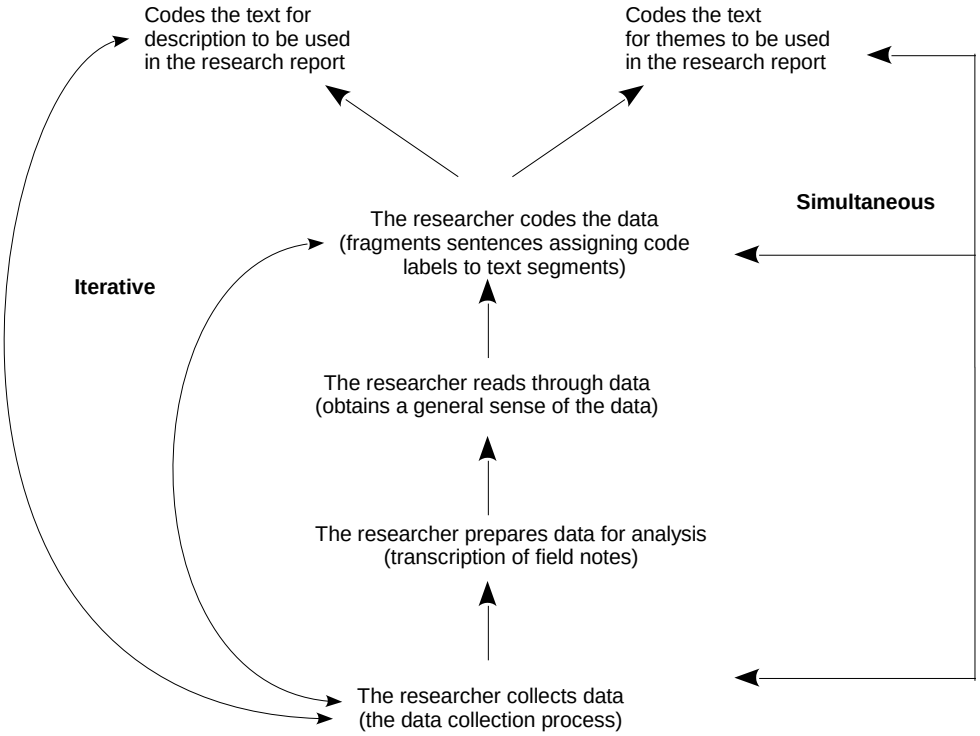
The questionnaire was sent out by iFeedback via email to the population to complete in electronic format. Duplicates were removed and the data of the closed questions were analysed by iFeedback in means and percentages. Further analysis was conducted in Excel and represented through descriptive statistics only. The validity and reliability of the closed-ended questions using factor and item analysis were not performed as the objective was not to develop a validated questionnaire but to rather explore the concept of information security culture using the open-ended questions.

6.3.2 Qualitative analysis

ATLAS.ti (2019) was used to analyse open-ended questions. Qualitative data analysis facilitated an interpretive exploration of the open-ended questions through coding and thematic analysis grounded in the theoretical propositions and case descriptions (Yin, 2017). In this regard Kelle (2013) argued that there are considerations when associating theory and empirical data such as the underlying theory and its elements, the relation of the theory to the data, and the function of the theory. This paper ascribes to Grbich (2012) that suggests a theory is abstract knowledge that is used to explain phenomena. This theory derived in this paper describes concepts and their relation to each other as experienced from participants in industry regarding the phenomena. The qualitative data, collected as answers to open-ended questions, are interpreted through a conceptual understanding gained from the literature study of this phenomenon. This is in line with Bradley, Curry, and Devers (2007), data can facilitate the establishment or validation of relationships between different concepts, leading to the refinement of auxiliary theory.

Sutton and Austin (2015, p. 228) argue, "Coding refers to the identification of topics, issues, similarities, and differences that are revealed through the participants' narratives and interpreted by the researcher". Creswell (2012) describes it as the deconstructing of textual data towards descriptions and broad themes. Miles, Huberman, and Saldana (2013) further the point made by emphasising that coding refers to a reflective analysis and interpretation of the data's meaning. The analysis of the open-ended questions' answers followed the process outlined and motivated by Creswell (2012). Consisting of six steps, step 1, is concerned with the preparation and organisation of the data; step 2, relates to the database coding; step 3, findings and the formation of themes; step 4, representing and reporting these findings; step 5, interpretation ; and step 6, validating and reporting of findings (see figure 2).

Figure 2: The qualitative data analysis process (Creswell (2012))



7. Results: Quantitative analysis

The yes-no questions were analysed and the results are presented in Table 5. The majority of the respondents indicated that their organisation had an information security policy in place (79%), with 77% conducting awareness amongst employees. The awareness activities ranged from monthly emails, staff meetings to newsletters. Interestingly, 69% of the respondents indicated that their organisation had a disciplinary process in place for non-compliance with its information security policies. These three concepts, *the information security policy, awareness and disciplinary action for non-compliance*, were the factors that most of the organisations implemented that could positively influence information security culture, as found in literature.

The factors that were implemented to a lesser extent were induction training where information security was discussed for new employees (57%), the appointment of an information security officer (50%) and having a reporting line/email address where employees could report information security breaches/incidents (49%). Only 37% of the respondents indicated that their organisation gave information security training, with only 12% that had a rewards process (recognition, part of performance appraisals, rewards, etc.) in place for compliance with information security policies.

Table 5. Yes-no statement results

Statement	% yes	% no	% don't know
My organisation has an information security policy in place.	79	16	5
My organisation creates awareness among employees about information security.	77	20	3
My organisation has a disciplinary process in place for non-compliance with its information security policies.	69	22	9
New employees in my organisation attend induction training where information security is discussed.	57	36	7
My organisation has an information security officer.	50	41	9
My organisation has a reporting line/email address where employees can report information security breaches/incidents.	49	44	6
My organisation gives employees information security training.	37	56	7
My organisation has a rewards process (recognition, part of performance appraisals, rewards, etc.) in place for compliance with its information security policies.	12	79	9

The Likert scale questions focused on the perception of employees towards certain information security concepts, as depicted in table 6. From a value perspective, the majority of the respondents (86%) believed that their organisation felt strongly about the protection of organisational information (e.g. intellectual property, customer information, employee information, financial information) and had implemented the technical controls to protect it (85%). Most of the respondents (85%) worked with confidential or sensitive information and believed that it was adequately protected (83%). While technical controls were implemented, it seems as though at least a third of employees might not know how to protect confidential information in electronic (28%) or hard copy format (30%), which emphasises the need for information security training. In addition, only 69% believed that everyone in their organisation was complying with information security policies. Having a third of the employees not knowing how to protect confidential information nor complying with the information security policies could introduce incidents and breaches in an organisation. This could relate to the lack of training, as employees believed that technical controls were implemented.

Table 6. Likert scale quantitative question results

Statement	% agree
My organisation feels strongly about the protection of organisational information (e.g. intellectual property, customer information, employee information, financial information).	86
I work with confidential or sensitive information.	85

Statement	% agree
My organisation implements technical controls to protect information on the organisation's IT systems.	85
I believe the information in my organisation is protected adequately.	83
I believe that everyone in my organisation wants to protect organisational information.	79
My organisation has measures in place (e.g. processes, approvals, secure rooms) to protect information on hard copy.	76
I think that everyone in my organisation believes that information security is important.	72
I believe that everyone in my organisation is complying with information-security-related policies.	69
I think that everyone in my organisation knows how to protect confidential information in electronic format (e.g. on the IT systems).	62
I think that everyone in my organisation knows how to protect confidential information in hard-copy format.	60

8. Results: Qualitative analysis

In the open coding process, a set of codes were identified from literature comprising of an initial 16 items. The subsequent coding was concerned with a systematic review of the data framed by the initial 16 items. The process followed the code-to-theory model of Saldaña (2015), that enables the research to extract theoretical assertions from the textual data through initial assignment of codes, the grouping of codes to categories that enable the identification of themes and eventual theory. "Theming refers to the drawing together of codes from one or more transcripts to present the findings of qualitative research in a coherent and meaningful way" (Sutton & Austin, 2015, p. 229). Table 7 lists the 16 themes with a summary of each theme.

Table 7. Initial themes

Initial 16 themes	Grounded	Density	Summary of the theme's quotation content
1. Sensitive/confidential	69	1	Sensitive or confidential information such as client, medical, personal , financial, customer, patient, contracts, IP, logs, bank statements, competitive information, bids
2. Importance for organisation	64	2	Important for confidential information, IP, patents, protection of information and systems, for good governance, compliance, trustworthiness, integrity, competitive advantage, etc.
3. Benefits of safety	60	0	Various benefits such as trust, respect, protection and safe information, fulfilling a mission, avoiding leakage, protecting employees, loyalty, competitive advantage etcetera.

Initial 16 themes	Grounded	Density	Summary of the theme's quotation content
4. Strategies for info security	45	0	Technical controls (e.g. firewalls, scans), procedural controls (e.g. compliance procedures, back up), training and communication
5. Organisational results of a breakdown	19	0	Hacking, lose client trust, fraud, reputational risk, financial loss, lost business, blackmail and risk to competition.
6. Regulations	10	0	Regulatory requirement, acts.
7. IP	8	1	Protecting intellectual property of organisation
8. Understand them	4	1	Understanding
9. Perpetrator	3	0	Competitors, third parties or wrong individuals
10. Penalty for non-adherence	3	0	Dismissal of employees or customers suing organisation
11. Virtual securing	2	1	Password protection and safe dissemination and storing of information
12. Responsibility for actions	2	1	Thinking about actions and risks
13. Awareness	2	1	Awareness of risks
14. Understanding	1	0	Understanding the risk and consequences
15. Physical securing	1	1	Securing of files
16. Limited access	1	1	Limiting access to authorized users
17. Ideal information security culture	1	7	Ideal culture
18. Adoption of security culture	1	1	Total buy-in

The next section gives an overview of the interpretation of the initial themes of the open-ended questions in response to the open-ended questions. Word clouds were also generated in ATLAS.ti and the number of instances each word was mentioned was counted to provide a further overview of concepts mentioned by the respondents.

Respondents were asked why they thought information security was important (Q31). Based on the coding most of the respondents emphasised that information security was linked with their competitive edge in the market, citing the 'company's information', IP and confidential information as the most prominent concerns after 'tender information'. This relates to theme one (sensitive/confidential), theme two (importance for organisation) and theme seven (IP). Additionally, the trust relationship that companies have with their employees and the employee's personal information that is entrusted to the organisation has moral as well as legal concerns. The personal information that was cited range from mundane information such as contact details, residential addresses, to more critically items such as bank details and medical aid claims and information.

Figure 3 illustrates the word cloud of the responses to this question. The protection and security of information dominated the responses, with 141 references to this concept. These two words were removed from the word cloud to identify other prominent concepts. Client (customer) information (65), personal information (38), intellectual property (36) and financial information (18) were deemed as the information to be protected. There were also 30 instances where respondents mentioned that information must be protected for confidentiality purposes and 28 mentioned that sensitive information must be protected.

Figure 3. Why is information security important for your organisation? (Q31)

Figure 4 gives an overview of the views of what an organisation can achieve if it has a strong information security culture.

Figure 4. What can organisations that have a strong information security culture achieve? (Q32)

Respondents felt that if an organisation has a strong information security culture, this will contribute to trust (31) from customers, employees and stakeholders; trust from clients (25) (give service, build confidence, retention and loyalty); the protection (35) of information, systems,

employees, clients and intellectual property; integrity (14) (of the company, information and systems) and ensure confidentiality (11) (see figure 3).

8.1 The ideal information security culture for an organisation

An ideal information security culture seems to be seen as an organisational proactive open engagement with its employers around issues and actions that would affect it. Respondents suggest that an ideal security information culture is framed by organisational strategies such as 'we are all expected to sign a confidentiality agreement', 'keep all staff informed of these kinds of attacks', and 'secure storage of information in any media format'. Although there is an understanding that the people in the organisations' actions and habits would need to be addressed, very few respondents responded with employee-centric descriptions, rather seeing them as somewhat passive in enacting and enabling the ideal information security culture.

Figure 5 displays a summary of the words respondents used to define the ideal information security culture for an organisation.

Figure 5. What would you define as the ideal information security culture for your organisation? (Q33)

The words "information" (89) and "security" (63) were removed from the word cloud for the analysis. The ideal information security culture was defined as one where employees are aware of information security, as seen by the words "employee" (21), "staff" (14), "people" (7) and "everyone" (11) as well as "awareness" (20) and "aware" (17) in the word cloud. There is an emphasis on understanding (15) and knowing (9) how to protect (13) and secure (16) information and that everyone should comply (10) with policies (12). "System/s" (13) was mentioned a number of times as well as "training" (5).

Some respondents referred to the following, which could be linked to values:

- " culture of mutual trust between management/staff";
- "should be second nature";

- "the culture is to be open and transparent about what is important for the organisation to protect";
- "understanding and living the security values";
- "a culture where the security of information is visible throughout all processes, procedures, control measures and applied throughout practice".

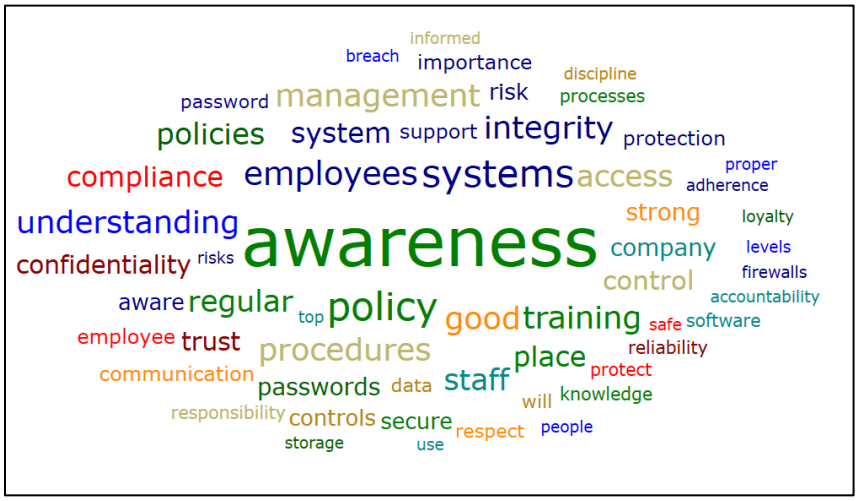
Many respondents listed controls that should be in place such as passwords, back-ups, access control, blocking certain websites, auditing and secure destruction of hard copies. The controls can be linked to the artefacts that would be visible in an organisation.

In summary, the ideal information security culture is linked to the awareness of employees to protect and secure information. Other important concepts are to understand what and how to protect, compliance with and reference to the information security policy.

8.2 Top traits of a strong information security culture

The amorphous view of strong information culture is very evident in the narrow scope of responses to the question with mostly organisational centered regulations being mentioned. Employer attitudes and actions are seen as rather passive and reactive being described mostly in terms if things that they refrain from doing as opposed to 'employer' things that should be done. The benefits are outlined as being mainly for the organisation and less benefit is ascribed to employees. A clear employee benefit was not evident beyond that of 'being tricked' or 'becoming victims of'. A clear theme is evident in regards to communication of employer expectations in the form of signed documents, and continual updates of changing trends. Mutual trust and adherence to regulations are a less prominent theme. The top traits mentioned by the respondents (Q34) are depicted in the word cloud in figure 6.

Figure 6. What would you regard as the top 3 traits of a strong information security culture? (Q34)



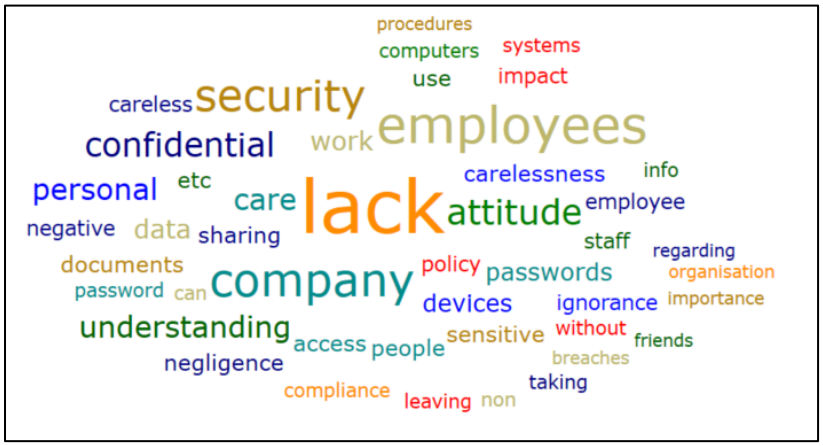
Each trait was mentioned the following number of times:

- Awareness (39);
- Policy/policies (34);
- Systems (19);
- Employees (16);
- Management (15);
- Training (15);
- Understanding (15);
- Integrity (15); and
- Procedures (15).

8.3 Behaviour that could have a negative impact on the protection of the organisation

As the notion of an ideal, strong or so-called mature information security culture is not explicitly conceptualised, negative impacts are predominantly referred to by actions of employees and lack of regulatory policies and proactive action by employers. Trust is again mentioned, but not explicitly contextualised as it is referred to as emotional state rather than a well-described interaction. Respondents indicated a number of behaviours that could have a negative impact on the protection of the organisation's information, as depicted in figure 7.

Figure 7. What behaviour do you believe could have a negative impact on the protection in your organisation? (Q35)



Careless (7), carelessness (8) and no care (12) behaviour was mentioned 27 times by the participants. Behaviour that could have a negative impact was linked to a lack (37) of certain aspects in an organisation, such as a lack of understanding of the policy, lack of attentiveness and detail, lack of training, lack of policy compliance, lack of communication, lack of respect, lack of appropriate systems, lack of management support and a lack of consequences and accountability.

8.4 Root cause of information security and data breaches

Employee negligence, human error, and lack of regulations and proactive engagement on the part of the employer are highlighted the additional items being able to fit into either of those three. At the heart of it the themes of employee action and employer inaction are identified. Figure 8 outlines the concepts respondents identified as the root causes of information security and data breaches.

Figure 8. What would you regard as the root cause of information security or data breaches in your organisation? (Q36)

Carelessness (17), ignorance (12) and negligence (7) were mentioned 36 times, which is in line with the behaviours (i.e. carelessness) mentioned in responses to question 35 that could have a negative impact on the protection of information. The root causes relate mainly to human aspects, such as:

- Carelessness (17);
- A lack of knowledge (14);
- A lack of understanding (13) of breaches, policies, and compliance;
- Ignorance (12);
- Negligence (7);
- Lack of awareness (11);
- Unauthorised access and controls (10);
- Inadequate password management (sharing, strong, change, etc.) (9); and
- Lack of training (7).

Other aspects that could play a role related to fraud (5) and systems not providing security (5).

8.5 Greatest obstacles in organisation to improve the information security culture

The persistent effort and the iterative nature of the notion of information security culture are evidenced as an obstacle. Complacency, although not stated, is inferred. The achievement of and

the continuous improvement in and of itself is the obstacle. The greatest obstacles mentioned by the participants relate to training and human aspects such as (refer to figure 9):

- Training (20) (lack thereof or insufficient);
- Awareness (14) (lack thereof);
- Management (12) (poor, lack, absence);
- Understanding (11) (lack of understanding of security issues, risks and consequences);
- Culture (9) (e.g. lack of trust, change);
- Systems (9) (complicated systems, poor systems, lack of systems to protect);
- Cost (9) (budget and cost constraints); and
- Resources (8) (lack thereof).

Figure 9. What would you regard as the greatest obstacles to improving the information security culture in your organisation? (Q37)

8.6 Creating a good security culture

The prevailing theme in the responses to this question hinges around the employee understanding the true consequences of their actions and a commitment towards acting in accordance with an ideal as evidenced by references to 'total buy-in', 'understanding the risk', ' risks by their actions' and 'would think twice about just saving information anywhere'. The implication is that the employer has structures and expectations but the risk still lies with the employee actions that are not always predictable or governable. Security, training, awareness and education (SETA) were listed mostly as the resolution to create a good security culture, figure 10.

Figure 10. The single thing that you would like to see in your organisation to create a good security culture amongst employees (Q39)

The respondents referred to the following as the single thing that their organisation should do to create a good information security culture:

- Training (38);
- Awareness (30);
- Communication (improve, regular, constant/repeated) (11);
- Education (9); and
- Of staff (17)/employees (16)/people (7).

Some ideas of creating a good information security culture relate to rewarding employees, capacity building, general meetings, purposeful development and motivation and implementing consequences for non-compliance. These aspects link to the root causes of information security incidents (i.e. lack of awareness, training, and education from question 36) and the greatest obstacles (i.e. lack of awareness, training, education, management from question 37) where respondents indicated that a lack of these aspects could result in security incidents or breaches.

The notion of what a mature/strong organisational information security culture entails is not clearly understood by the respondents. Their perceptions centre on the **actions of the employer** in establishing and maintaining structures, policies, and guidelines to ensure:

- that information employees are exposed to only information and data that they are entitled to,
- employees have a clear understanding of what constitutes desirable actions,
- an iterative ongoing update and adjustment to ICT and related policies to keep abreast of threats,
- establishing and maintaining communication with employees, and
- the need to avoid institutional complacency.

As opposed to the employee that is perceived as having to **refrain from certain actions** such as

- not saving data all over,
- refraining from talking about or sharing information, passwords, etc,

- refrain from accessing restricted information,
- refrain from sharing certain information, and
- not being gullible to be duped.

From this, it becomes a challenge to outline a roadmap towards achieving a mature information security culture and in so doing describe what it entails. The activation of employees towards active participation is additionally noted.

9. Defining information security culture – academia and industry perspective

The literature definition of information security culture can be extended with the views of industry by adding the concepts that were identified by survey respondents.

The literature definition of information security culture as defined in section 4 was as follows: "The behaviour over time becomes part of the way things are done, i.e. second nature, as a result of employee assumptions, values, and beliefs, their knowledge of, attitude towards and perception of the protection of information assets. The information security culture is directed by the vision of senior management as defined in the information security policy and is visible in the artefacts of the organisation and behaviour exhibited by employees", is therefore extended with the following:

- Adding the type of information that must be protected as derived from question 31.

  Information security culture is contextualised to the behaviour of humans in an organisational context to *protect the information processed by the organisation for example that of clients, personnel, intellectual property and financial information*.

- The literature definition can be further expanded by adding the concepts "understanding" of "how" to protect, derived from questions 33, 34 and 37, and the lack thereof, in question 36.
- The concept of "compliance" is added from question 33.
- "Awareness" is added, emanating from questions 34 and 39 and the lack thereof as listed in questions 36 and 37.
- Similarly, "training" is added from questions 34 and 39 and the lack thereof from questions 36 and 37.
- "Education" and "communication" are also added from question 39.
- Reference to "policy" emanates from questions 33, 34, 35, 36 and 39; this aligns with the literature definition which also includes the information security policy.
- "Procedures" is referred to in questions 33, 34 and 39.

…through compliance with the information security policy and procedures and an understanding of how to act as embedded through regular communication, awareness, training and education initiatives.

- The impact of a strong or good information security culture that could lead to "trust" and "integrity" is also integrated based on the results of question 32.
- The lack or absence of or poor management was identified as the third highest obstacle to a good information security culture in response to question 37. Similarly, management was identified as a trait in a strong information security culture in answers to question 34. "Management" is therefore emphasised more in the definition.
- Adequate systems were referred to (Q34) as a top trait as well as the lack thereof which could be an obstacle. As such, the concept of an adequate "ICT environment" is added to the definition.

The information security culture is directed by the vision of senior management together with *management support in line with* the information security policy supported by an adequate *ICT environment*, visible in the artefacts of the organisation and behaviour exhibited by employees, thereby *creating an environment of trust with stakeholders and establishing integrity.*

- Carelessness was raised in responses to questions 35 and 36 as a root cause of information security incidents or breaches, together with ignorance and negligence (Q36). This correlates with literature where the negligent or irresponsible behaviour of employees is regarded as reasons for information security incidents. The opposite of carelessness is cautiousness, thoroughness, vigilance, conscientiousness or attentiveness. This concept is thus also added to the definition.
- The concept of internal and external factors from table 3 are also embedded.

The comprehensive definition of information security culture is, therefore:

> *Information security culture is contextualised to the behaviour of humans in an organisational context to protect information processed by the organisation through compliance with the information security policy and procedures and an understanding of how to implement requirements in a cautious and attentive manner as embedded through regular communication, awareness, training and education initiatives.*
>
> *The behaviour over time becomes part of the way things are done, i.e. second nature, as a result of employee assumptions, values and beliefs, their knowledge and attitude towards and perception of the protection of information assets. The information security culture is directed by the vision of senior management together with management support in line with the information security policy and influenced through internal and external factors, supported by an adequate ICT environment, visible in the artefacts of the organisation and behaviour exhibited by employees, thereby creating an environment of trust with stakeholders and establishing integrity.*

10. Factors to instil an information security culture – academia and industry

Figure 11 provides a synthesised visual interpretation of what constitutes information security culture by integrating the concepts derived from literature and the views of industry experts. This figure addressed the aim of the paper.

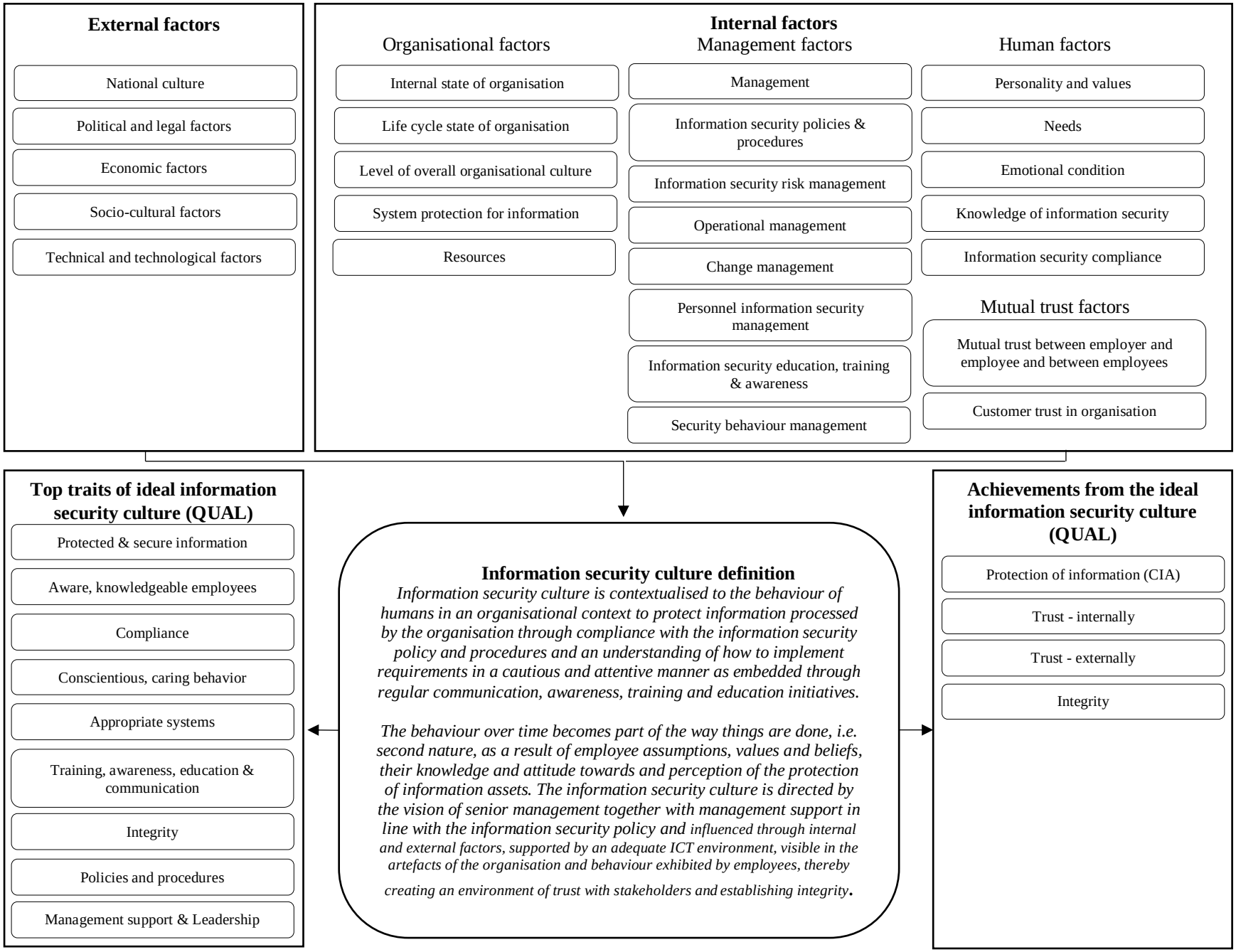
The factors listed in Table 3, derived from literature, that could contribute to instil an information security culture are depicted at the top of the figure. The factors are grouped into external factors with five sub factors and internal factors comprising of organisational, management, human and mutual trust of the employer, employees, and customers, with a total of 20 sub factors as derived from the theory.

Consequences for non-compliance and rewards for compliance were another concept that was identified in the survey which can be considered under the management factors. It is not, however, added as a separate block but can be integrated with the personnel information security management or security behaviour management factor.

The top traits of an ideal information security culture, as derived from the industry survey, are depicted on the left-hand side of the figure. On the right-hand side, the aspects that can lead to having a strong or good information security culture, also derived from the industry survey, are depicted. The information security culture defined and constructed in section 9 is at the centre of the figure.

Figure 11 provides a holistic view of the concept of information security culture. It aims to provide academia and industry with a comprehensive baseline of factors (Table 3) that should be in place and that should be governed effectively to positively influence the information security culture. The resultant impact of the factors is also depicted, giving a view of the potential output that can be visible on an artefact (e.g. policy) or value level (e.g. trust). Figure 11 is, therefore, a visual representation of how the authors have combined the most cited descriptions of the information security culture definition (table 1 and 2), factors from papers (Table 3) based on the organisational management theory and from the semi-structured questionnaire completed by industry.

Figure 11. An organisational Information security culture model (OISCM)


External factors
National culture
Political and legal factors
Economic factors
Socio-cultural factors
Technical and technological factors
Internal factors
Organisational factors
Internal state of organisation
Life cycle state of organisation
Level of overall organisational culture
System protection for information
Resources
Management factors
Management
Information security policies & procedures
Information security risk management
Operational management
Change management
Personnel information security management
Information security education, training & awareness
Security behaviour management
Human factors
Personality and values
Needs
Emotional condition
Knowledge of information security
Information security compliance
Mutual trust factors
Mutual trust between employer and employee and between employees
Customer trust in organisation
Top traits of ideal information security culture (QUAL)
Protected & secure information
Aware, knowledgeable employees
Compliance
Conscientious, caring behavior
Appropriate systems
Training, awareness, education & communication
Integrity
Policies and procedures
Management support & Leadership
Information security culture definition
Information security culture is contextualised to the behaviour of humans in an organisational context to protect information processed by the organisation through compliance with the information security policy and procedures and an understanding of how to implement requirements in a cautious and attentive manner as embedded through regular communication, awareness, training and education initiatives.
The behaviour over time becomes part of the way things are done, i.e. second nature, as a result of employee assumptions, values and beliefs, their knowledge and attitude towards and perception of the protection of information assets. The information security culture is directed by the vision of senior management together with management support in line with the information security policy and influenced through internal and external factors, supported by an adequate ICT environment, visible in the artefacts of the organisation and behaviour exhibited by employees, thereby creating an environment of trust with stakeholders and establishing integrity.
Achievements from the ideal information security culture (QUAL)
Protection of information (CIA)
Trust - internally
Trust - externally
Integrity

The OISCM depicted in Figure 11 improves the current understanding of what constitutes information security culture in organisations and a new improved definition is derived. This definition has more value as it not only represents the research papers, but is also refined based on the feedback from industry.

11. Contribution, future work and conclusion

This research aimed to provide an integrated view of the concept of information security culture that can be used to inform academic frameworks, models and assessment tools for information security culture while being informed from an industry perspective and making it easier to implement in organisations. It serves as a reference for future work on information security culture by consolidating previous perspectives and expanding the concept with industry input to a single comprehensive definition of the concept. As our analysis shows, scientific interpretations of the definitions and factors of information security culture are much wider than their understanding in the industry. This is not surprising, since there is always a gap between theory and practice which they must bridge together. Science is aimed not only at description and explanation, but also at predicting the processes and phenomena under study. Given the dynamic nature of an information security culture, employers need to know in which direction it can develop in the future. Therefore, the model of factors influencing the culture of information security presented in the review has prognostic value for them. As for the survey results, they indicate an insufficient level of respondents' knowledge about the culture of information security, a simplified interpretation of the factors influencing it. For scientists, this is an important topic of research on methods and forms of increasing the level of this knowledge.

The effectiveness of measures to form and develop an information security culture in an organisation depends to a large extent on ideas about the boundaries of the concept and the factors that influence this process. However, the employer and employee evaluate the concept of information security culture and the importance of the same factors of its development in different ways, which could lead to a dissonance in their efforts to ensure the organisation’s information security. The theoretical significance of our study lies in the interpretation of the concept of information security culture and the system of external and internal factors influencing its level, taking into account the general theory of organisation management and the theory of organisational culture, as well as modern features of information security culture as part of organisational culture. This system includes, for example, factors caused by the sociocultural transformation of the information society into a knowledge society: the imperative of reaching agreement and mutual trust of employees and the employer through the development of intellectual and cultural capital of the organisation’s employees. Expanding the context and content boundaries of the organisation’s information security culture, as well as the range of factors influencing it, enriches the theoretical section of the science of the information security culture of the organisation.

The results of an empirical study of ideas about information security culture in practice and their comparative analysis with ideas about information security culture in science also have scientific novelty. The revealed discrepancy between the assessments of the significance of various factors of information security culture indicates a lack of awareness among employees of organisations about information security and information security culture, as well as the weak attention of scientists to a number of factors significant for employees. This opens up new horizons for scientific research in the field of information security culture.

The practical significance of the study lies in the fact that the results of a comparative analysis of ideas about information security culture in science and industry can be used to determine guidelines for the policy of formation and development of information security culture in organisations, means and methods of its implementation.

Further theoretical studies are associated with a deeper analysis of factors of the external and internal environment - taking into account the direction, strength and nature of their impact on the level of information security culture, the possibilities of elimination, and so on. The knowledge gained will increase the effectiveness of measures to form and develop information security culture. Therefore, in the future it is advisable to create a multifactor model for assessing the dependence of the information security culture on various factors and, on its basis, a methodology for assessing information security culture. This was indicated in Table 5 and 6 as current organisations have not yet implemented all information security factors (e.g. reward system and induction training).

It seems important to us to repeat the empirical study after measures to raise awareness of workers about information security culture, as well as the interpretation of the results of the identified dynamics of employees' assessments of the significance of different factors of information security culture.

Acknowledgements
This research was supported by funding from the National Research Foundation (NRF) in South Africa for Y-rated researchers, Grant No: 103965.

References

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information security culture: A behaviour compliance conceptual framework. In Proceedings of: The 8th Australasian Information Security Conference (AISC), Brisbane, Australia, 47-55.

AlHogail, A. (2015a). Cultivating and assessing organisational information security culture, an Empirical Study. International Journal of Security and Its Applications. (9)7, 163-178.

AlHogail, A. (2015b). Design and validation of information security culture framework. Computers in Human Behavior. 49, 567-575. doi:10.1016/j.chb.2015.03.054

AlHogail, A., & Mirza, A. (2014). Information security culture: A definition and a literature review. In Proceedings of: The Computer Applications and Information Systems (WCCAIS), 2014, 1-7.

Alnatheer, M., & Nelson, K. (2009). A proposed framework for understanding information security culture and practices in the Saudi context. In Proceedings of: The 7th Australian Information Security Management Conference, Perth, 6–17.

Alshaikh, M., Ahmad, A., Maynard, S.B. & Chang, S. (2014). Towards a taxonomy of information security management practices in organisations. In Proceedings of: The 25th Australasian Conference on Information Systems, Auckland, New Zeeland, 1-10.

Astakhova, L.V. (2010). Information security culture and information destructiveness counterculture: essence and structure. In Proceedings of: The International Conference Economic, legal and socio-cultural aspects of regional development - Socio-cultural aspects of regional development, Chelyabinsk, Russia, 201-205. (Translated from Russian).

Astakhova, L.V. (2011). Information-psychological security in the region: culturological aspect. Bulletin of the Ural Federal District. Information Security, 2011(2), 40-47. (Translated from Russian).

Astakhova L.V. (2013). Human information security vulnerability of organisation: methodology of assessment. Ukrainian Scientific Journal of Information Security, 2(19), 133-138. (Translated from Russian).

Astakhova, L.V. (2014). The concept of the information-security culture. Scientific and Technical Information Processing. 41(1), 22-28. https://doi.org/10.3103/S0147688214010067

Astakhova, L.V. (2015). Information security: risks related to the cultural capital of personnel (review). Scientific and Technical Information Processing. 42(2), 41-52. https://doi.org/10.3103/S0147688215020021

Astakhova L.V. (2016). The ontological status of trust in information security. Scientific and Technical Information Processing. (43)1, 58-65.

Astakhova L.V. (2017). Development of cultural competence of the student in the post-industrial society: imperatives of the capital approach. Integration of Education. (21)1, 35-45. DOI: 10.15507/1991-9468.086.021.201701.035-045 (Translated from Russian).

Astakhova, L.V. (2018). From culture to cultural capital information security of the organisation. Bulletin of Culture and Arts. 3(55), 85-101. (Translated from Russian).

ATLAS.ti. (2019). Software. Retrieved from https://atlasti.com/

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. Computers in Human Behavior. 48, 51-61. doi:10.1016/j.chb.2015.01.039.

Box, D., & Pottas, D. (2013). Improving Information Security Behaviour in the Healthcare Context. Procedia Technology. 9, 1093-1103. doi:10.1016/j.protcy.2013.12.122.

Bradley, E. H., Curry, L. A., & Devers, K. J. (2007). Qualitative data analysis for health services research: developing taxonomy, themes, and theory. Health services research, 42(4), 1758-1772.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly. 34(3), 523-548.

Chia, P. Maynard, S., and Ruighaver, A.B. (2002). "Understanding Organisational Security Culture". Sixth Pacific Asia Conference on Information Systems, Tokyo, Japan, pages 731-740, 2-3 September 2002.

Cole, N.L. (2019). What is cultural capital? Do I have it? Retrieved from https://www.thoughtco.com/what-is-cultural-capital-do-i-have-it-3026374.

Creswell, J. W. (2012). Educational research: planning, conducting, and evaluating quantitative and qualitative research, 4th ed, 501 Boylston Street, Boston, MA 02116: Pearson Education, Inc.

Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches, 4th edition, California: Sage.

Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches, 5th edition, California: Sage.

D'Arcy, J. & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. Information Management & Computer Security, 22(5):474-489.

Da Veiga, A. (2016a). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. In Proceedings of: The SAI Computing Conference (SAI), United Kingdom, London, 1006-1015.

Da Veiga, A. (2016b). Comparing the information security culture of employees who had read the information security policy and those who had not. Information and Computer Security, 24(2), 139-151. doi:10.1108/ics-12-2015-0048.

Da Veiga, A. (2018). An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. Information and Computer Security. 26(5), 584-612. doi:10.1108/ics-08-2017-0056.

Da Veiga, A., & Eloff, J.H.P. (2007). An information security governance framework. Information Systems Management. 24(4), 361-372. doi:10.1080/10580530701586136.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. Computers & Security. 29(2), 196-207. doi:10.1016/j.cose.2009.09.002.

Da Veiga, A., & Martins, N. (2015a). Improving the information security culture through monitoring and implementation actions illustrated through a case study. Computers & Security. 49, 162-176. doi:10.1016/j.cose.2014.12.006.

Da Veiga, A., & Martins, N. (2015b). Information security culture and information protection culture: A validated assessment instrument. Computer Law & Security Review. 31(2), 243-256. doi:10.1016/j.clsr.2015.01.005.

Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. Computers & Security. 70, 72-94. doi:10.1016/j.cose.2017.05.002.

Deter, J.R., Schroeder, R.G. & Mauriel J.J. (2000). A framework for linking culture and improvement intiatives in organisation. The Academy of Management Review. 25(4), 850 – 863.

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

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: an organisational transformation case study. Computers & Security. 56, 63-69. doi:10.1016/j.cose.2015.10.001.

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2007). Fostering information security culture in small and medium size enterprises: An interpretive study in Australia. Paper presented at the European Conference on Information Systems (ECIS), University of St. Gallen, St. Gallen, Switzerland, 1560-1571.

ENISA. (2017). Cybersecurity culture in organisations. Retrieved from https://doi.org/10.2824/10543

Faily, S., Furnell, S.M., & Fléchais, I. (2010). Designing and aligning e-Science security culture with design. Information Management & Computer Security, 18(5), 339-349. doi:10.1108/09685221011095254.

Flier A.Ya. (2015). Good and evil in the cultural and historical sense. Information humanitarian portal. Knowledge. Understanding Skill. No 3, 17–36. http://www.zpu-journal.ru/e-zpu/2015/3/Flier_Good-Evil/,https://cyberleninka.ru/article/n/dobro-i-zlo-v-kulturno-istoricheskom-ponimanii (Translated from Russian).

Flores, W.R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers & Security. 59, 26-44. doi:10.1016/j.cose.2016.01.004.

Flores, W.R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organisations: Investigating the effect of behavioral information security governance and national culture. Computers & Security. 43, 90-110. doi:10.1016/j.cose.2014.03.004.

Furnell, S., & Rajendran, A. (2012). Understanding the influences on information security behaviour. Computer Fraud & Security, 2012(3), 12-15. doi:10.1016/s1361-3723(12)70053-2.

Furnell, S. M., & Thompson, K.L. (2009). From culture to disobedience: recognising the varying user acceptance of IT security. Computer Fraud & Security, 2009(2), 5-10.

Gabriel, T., & Furnell, S. (2011). Selecting security champions. Computer Fraud and Security, 2011(8), 8–12.

Geeling, S., Brown, I., & Weimann, P. (2016). Information systems and culture - a systematic hermeneutic literature review. In Proceedings of: International Conference on Information Resources Management (CONF-IRM), Paper 37.

Grant, M. J., & Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. Health Info Library Journal, 26(2), 91-108. doi:10.1111/j.1471-1842.2009.00848.x.

Grbich, C. (2012). Qualitative data analysis: An introduction: Sage.

Greig, A., Renaud, K., & Flowerday, S. (2015). An ethnographic study to assess the enactment of information security culture in a retail store. In Proceedings of: World Congress on Internet Security (WorldCIS-2015), IEEE, 61–66.

Harzing, A.W. (2007) Publish or Perish. Retrieved from https://harzing.com/resources/publish-or-perish

Hassan, N. H., & Ismail, Z. (2012). A conceptual model for investigating factors influencing information security culture in healthcare environment. Procedia - Social and Behavioral Sciences. 65, 1007-1012. doi:10.1016/j.sbspro.2012.11.234.

Helokunnas, T., & Kuusisto, R. (2003). Information security culture in a value net. In Proceedings of: The IEMC '03 - Managing Technologically Driven Organisations: The Human Side of Innovation and Change, Albany, USA, 190-194.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organisations: role of penalties, pressures and perceived effectiveness. Decision Support Systems. 47(2), 154-165. doi:10.1016/j.dss.2009.02.005.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea. Information & Management, 49(2), 99-110. doi:10.1016/j.im.2011.12.005.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: the critical role of top management and organisational culture. Decision Sciences Journal, 43(4), 615-659.

iFeedback. (2019). iFeedback. Retrieved from: http://ifeedback.co.za/.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information & Management, 51(1), 69-79. doi:10.1016/j.im.2013.10.001.

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture–state-of-the-art review between 2000 and 2013. Information & Computer Security. 23(3), 246-285.

Kelle, U. (2013). Theorization from Data. In U. Flick (Ed.), The SAGE handbook of qualitative data analysis: Sage.

Koh, K., Ruighaver, A. B., Maynard, S. B., & Ahmad, A. (2005). Security Governance: Its Impact on Security Culture. In Proceedings of: The 3rd Conference on Australian Information Security Management (AISM-2005), Edith Cowan University, Western Australia, 47-58.

Knapp, K. J., Morris, R.F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: an organisational-level process model. Computers & Security. 28(7), 493-508. doi:10.1016/j.cose.2009.07.001.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organisational factors in computer and information security: pathways to vulnerabilities. Computers & Security. 28(7), 509-520. doi:10.1016/j.cose.2009.04.006.

Kruger, H.A., & Kearney, W.D. (2006). A prototype for assessing information security awareness. Computers & Security. 25(4), 289-296. doi:10.1016/j.cose.2006.02.008.

Kuznetsova, O.E. (2005). Problem of countercultures in the modern organisations. Retrieved from https://rpj.ru.com/index.php/rpj/article/view/14/17.

Leach, J. (2003). Improving user security behaviour. Computers & Security. 22(8): 685-692.

Lim J., Ahmad A.A., Chang S.L.C., & Maynard S.B.M. (2010). Embedding Information Security Culture Emerging Concerns and Challenges. In Proceedings of: The Pacific Asia Information Systems Conference (PACIS 2010). Taipei, Taiwan, National Taiwan University, 463-474.

Lim, J., Chang, S.L., Ahmad, A. & Maynard, S.B. (2012). Towards an Organisational Culture Framework for Information Security Practices. In Gupta M, Walp J & Sharman R (eds), Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions.Hershey, United States: Information Science Publishing, 296-315. DOI: 10.4018/978-1-4666-0197-0.ch017.

Mahfuth, A., Yussof, S., Baker, A.A., & Ali, N. (2017). A systematic literature review: Information security culture. In Proceedings of: The 5th International Conference on Research and Innovation in Information Systems - Social Transformation through Data Science (ICRIIS), 2017 International Conference. https://doi.org/10.1109/ICRIIS.2017.8002442.

Martins, A., & Eloff, J.H.P. (2002). Information security culture. In Proceedings of: IFIP TC11 17th International Conference on Information Security, Cairo, Egypt, 203-214.

Mescon, M.M., Albert, M. & Khedouri, F. (1988). Management. Harper & Row: New York.

Munteanu, A.B., & Fotache, D. (2015). Enablers of information security culture. Procedia Economics and Finance. 20, 414-422. doi:10.1016/s2212-5671(15)00091-x.

Nasir, A., Arshah, R.A., Ab Hamid, M.R., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. Journal of Information Security and Applications. 44(2019), 12-22.

Nel, F. & Drevin, L. (2019). Key elements of an information security culture in organisations. Information and Computer Security. (27)2, 146-164.

Ngo, L., Zhou, W., & Warren, M. (2005). Understanding transition towards information security culture change. In Proceedings of: The 3rd Australian Information Security Management Conference, Perth, Western Australia, 67-73.

Noorman M.M., Nazrin, H.Q., Khairulnizan, Z.M. (2017). Information security culture for Malaysian Public Organisation: a conceptual framework. In Proceedings of: The 2017 4th International Conference on Education and Social Sciences (INTCESS2017), Istanbul, Turkey, 156–166.

OECD. (2002). Guidelines for the security of information systems and networks: towards a culture of security: Organisation for Economic Co-operation Development. Retrieved from:

http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm.

OECD. (2015). Digital security risk management for economic and social prosperity: OECD recommendation and companion document. Retrieved from: http://dx.doi.org/10.1787/9789264245471-en.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. Computers & Security. 31(5), 673-680. doi:10.1016/j.cose.2012.04.004.

Park, E.H., Kim, J., & Park, Y.S. (2017). The role of information security learning and individual factors in disclosing patients' health information. Computers & Security. 2017(65), 64-76.

Parsons, K., Calic, D., & Barca, C. (2016). Self-disclosure on Facebook: comparing two research organisations. Paper presented at the Australian Conference of Information Systems (ACIS), Wollongong, Australia, 1-11.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security. 66, 40-51. doi:10.1016/j.cose.2017.01.004.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security. 42, 165-176. doi:10.1016/j.cose.2013.12.003.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organisational information security culture on information security decision making. Journal of Cognitive Engineering and Decision Making, 9(2), 117-129.

Ponemon. (2018). Cost of data breach study: Impact of business continuity management. Retrieved from: https://www.ibm.com/downloads/cas/AEJYBPWA.

PricewaterhouseCoopers. (2016). Global state of information security survey. Retrieved from: http://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf.

Reid, R., Van Niekerk, J., & Renaud, K. (2014). Information security culture: A general living systems theory perspective. In Proceedings of: The Information Security of South Africa Conference (ISSA2014), Johannesburg, South Africa, 1-8. doi:10.1109/issa.2014.6950493.

Ruighaver, A.B., Maynard, S.B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. Computers & Security. 26(1), 56-62. doi:10.1016/j.cose.2006.10.008

Sabbagh, B.A.M., Watterstam, T., & Kowalski, S. (2012). A prototype for HI(2)Ping information security culture and awareness training. In Proceeding of: The 2012 International Conference on E-Learning and E-Technologies in Education (ICEEE 2012), 32-36.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organisations. Computers & Security. 53, 65-78. doi:10.1016/j.cose.2015.05.012.

Saldaña, J. (2015). The coding manual for qualitative researchers: Sage: London.

Saleh, Z.I., Refai, H., & Mashhour, A. (2011). Proposed framework for security risk assessment. Journal of Information Security, 2011(2), 85-90.

Saunders, M., Lewis, P., & Thornhill, A. (2016). Research methods for business students (Vol. 7). Essex, UK: Pearson.

Schein, E.D. (1992). Organisational Culture and Leadership: A Dynamic View. San Francisco, CA: Jossey-Bass.

Schein, E.D. (2004). Organisational culture and leadership. San Francisco, California: Jossey-Bass.

Schein, E.D. (2009). The corporate culture survival guide. San Francisco, California: Jossey-Bass.

Schein, E.H. (2010). Organisational culture and leadership. San Fransisco: John Wiley & Sons.

Schlienger, T., & Teufel, S. (2002). Information security culture - The socio-cultural dimension in information security management. Paper presented at the Security in the Information Society (Sec2002). IFIP TC11 International Conference on Information Security (Sec2002), Cairo, Egypt, Kluwer Academic Publishers, 191-202.

Schlienger, T., & Teufel, S. (2003a). Analyzing information security culture increased trust by an appropriate information security culture. Paper presented at the International Workshop on Trust and Privacy in Digital Business (TrustBus'03) in conjunction with 14th International Conference on Database and Expert Systems Applications (DEXA 2003), Prague, Czech Republic.

Schlienger, T., & Teufel, S. (2003b). Information security culture - from analysis to change. In Proceedings of: The Information Security South Africa (ISSA2003), Sandton, Johannesburg. 183-195.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). Computers & Security, 56, 14–30.

Shaw, R.S., Chen, C.C., Harris, A.L., & Huang, H.J. (2009). The impact of information richness on information security awareness training effectiveness. Computers & Education, 52(1), 92-100. doi:10.1016/j.compedu.2008.06.011.

Sherif, E., Furnell, S., & Clarke, N. (2015). An Identification of variables influencing the establishment of information security culture. 9190, 436-448. doi:10.1007/978-3-319-20376-8_39.

Sutton, J., & Austin, Z. (2015). Qualitative research: data collection, analysis, and management. The Canadian journal of hospital pharmacy, 68(3), 226.

Tang, M., Li, M.G., & Zhang, T. (2015). The impacts of organisational culture on information security culture: a case study. Information Technology and Management, 17(2), 179-186. doi:10.1007/s10799-015-0252-2.

Thomson, K.L., Von Solms, R., & Louw, L. (2006). Cultivating an organisational information security culture. Computer Fraud & Security, 2006(10), 7-11. doi:10.1016/s1361-3723(06)70430-4

Tolah, A., Furnell, S.M., & Papadaki, M. (2017). A comprehensive framework for cultivating and assessing information security culture. In Proceedings of: The Human Aspects of Information Security & Assurance (HAISA2017) Conference, Australia, Adelaide, 52–64.

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. Computers & Security, 52, 128-141. doi:10.1016/j.cose.2015.04.006.

United Nations General Assembly. (2003). General Assembly. Resolution adopted by the General Assembly, A/RES/57/2. Retrieved from https://doi.org/10.1080/714003707

Van Niekerk, J., & Von Solms, R. (2005). An holistic framework for the fostering of an information security sub-culture in organisations. In Proceedings of: Information Security South Africa (ISSA2005), South Africa, 1–13.

Van Niekerk, J., & Von Solms, R. (2006). Understanding information security culture: a conceptual framework. In Proceedings of: Information Security South Africa (ISSA2006), South Africa, 1-9.

Van Niekerk, J.F., & Von Solms, R. (2010). Information security culture: A management perspective. Computers & Security. 29(4), 476-486. doi:10.1016/j.cose.2009.10.005

Von Solms, B. (2006). Information security – the fourth wave. Computers & Security. 25(3), 165-168. doi:10.1016/j.cose.2006.03.004

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security. 38, 97-102. doi:10.1016/j.cose.2013.04.004

Von Solms, R., & Von Solms, B. (2004). From policies to culture. Computers & Security. 23(4), 275-279. doi:10.1016/j.cose.2004.01.013

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security–what goes where? Information & Computer Security. 26(1), 2-9.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. Computers & Security. 23(3), 191-198. doi:10.1016/j.cose.2004.01.012

Wilderom, C.P.M., Van den Berg, P.T., & Wiersma, U.J. (2012). A longitudinal study of the effects of charismatic leadership and organisational culture on objective and perceived corporate performance. The Leadership Quarterly, 23(5), 835-848. doi:10.1016/j.leaqua.2012.04.002

Wiley, M. A., McCormac, M. A., & Calic, D. (2019). More than the Individual: Examining the Relationship Between Culture and Information Security Awareness. Computers & Security, 101640.

Williams, P.A.H. (2009). Capturing culture in medical information security research. Methodology Innovations Online, 4(3):15–26.

Yin, R. K. (2017). Case study research and applications: Design and methods: Sage publications. UK.

Zakaria, O., Gani, A., Mohd Nor, M., & Badrul Anuar, N. (2007). Reengineering information security culture formulation through management perspective. In Proceedings of: The International conference on Electrical Engineering and Informatics, Institut Teknologi Bandung, Indonesia, 638-641.

Appendix 1: Questionnaire questions

SECTION 2: Background questions (Yes/No/Don't know scale)

11. My organisation has an information security policy in place (also referred to as an Acceptable Usage Policy). Adapted from ISCA, question 2, Da Veiga (2018).
12. My organisation has an Information Security Officer. Adapted from ISCA, question 6, Da Veiga (2018).
13. My organisation creates awareness among employees about information security. Adapted from awareness and training dimension of Da Veiga (2015, 2018).
14. What and how often? (Monthly, Weekly, Daily, Other)
15. My organisation gives employees information security training.
    Adapted from awareness and training dimension of Da Veiga (2015, 2018).
16. What and how often? (Monthly, Weekly, Daily, Other)
17. New employees in my organisation attend induction training where information security is discussed. Adapted from awareness and training dimension of Da Veiga (2015, 2018).
18. My organisation has a reporting line/email address where employees can report information security breaches/incidents. Explain what it entails Adapted from ISCA, question 17, Da Veiga (2018).
19. My organisation has a disciplinary process in place for non-compliance with its information security policies. Adapted from ISCA question 59, Da Veiga (2018).
20. My organisation has a rewards process (recognition, part of performance appraisals, rewards, etc) in place for compliance with its information security policies. Explain what. Adapted from ISCA, question 48, Da Veiga (2015).

SECTION 2: Closed-ended questions (Likert scale: Never, Rarely, Very Often, Always)

21. I believe the information in my organisation is protected adequately. Adapted from ISCA, question 22, Da Veiga (2018).
22. I work with confidential or sensitive information. Adapted from ISCA, question 13 and 15, Da Veiga (2018).
23. My organisation implements technical controls to protect information on the organisation's IT systems. Adapted from question ISCA, question 43, Da Veiga (2018).
24. My organisation has measures in place (e.g. processes, approvals, secure rooms) to protect information on hard copy. Adapted from question ISCA, question 44, Da Veiga (2018).
25. I think that everyone in my organisation believes that information security is important. Adapted from ISCA, question 50, Da Veiga (2018).
26. I think that everyone in my organisation knows how to protect confidential information in electronic format (e.g. on the IT systems). Adapted from ISCA, question 43, Da Veiga (2018).
27. I think that everyone in my organisation knows how to protect confidential information in hard-copy format. Adapted from ISCA question 44, Da Veiga (2018).
28. My organisation feels strongly about the protection of organisational information (e.g. intellectual property, customer information, employee information, financial information). Adapted from ISCA, question 21, Da Veiga (2018).
29. I believe that everyone in my organisation wants to protect organisational information. Adapted from ISCA, questions 50, 55, 58, Da Veiga (2018).

30. I believe that everyone in my organisation is complying with the information-security-related policies. Adapted from ISCA, question 61, Da Veiga (2018).

SECTION 4: Open-ended questions

31. Why is information security important for your organisation?
32. What can organisations that have a strong information security culture achieve?
33. What would you define as the ideal information security culture for your organisation?
34. What would you regard as the top 3 traits of a strong information security culture?
35. What employee behaviour do you believe could have a negative impact on the protection of information in your organisation?
36. What would you regard as the root cause of information security or data breaches in your organisation?
37. What would you regard as the greatest obstacles to improving the information security culture in your organisation?
38. How do you believe has your organisation fared in terms of the way it deals with information security?
39. What is that one single thing that you would most like to see your organisation do to create a good security culture amongst employees?