Critical Analysis of Information Security Culture Definitions

Zainab Ruhwanya, Jacques Ophoff

Critical Analysis of Information Security Culture Definitions

Zainab Ruhwanya[1][000-0003-2339-7154] and Jacques Ophoff[1,2][0000-0003-0634-5248]

[1] University of Cape Town, Cape Town, South Africa
[2] Abertay University, Dundee, United Kingdom
Zainab.ruhwanya@uct.ac.za, j.ophoff@abertay.ac.uk

Abstract. This article aims to advance the understanding of information security culture through a critical reflection on the wide-ranging definitions of information security culture in the literature. It uses the hermeneutic approach for conducting literature reviews. The review identifies 16 definitions of information security culture in the literature. Based on the analysis of these definitions, four different views of culture are distinguished. The shared values view highlights the set of cultural value patterns that are shared across the organization. An action-based view highlights the behaviors of individuals in the organization. A mental model view relates to the abstract view of the individual's thinking on how information security culture must work. Finally, a problem-solving view emphasizes a combination of understanding from shared value-based and action-based views. The paper analyzes and presents the limitations of these four views of information security culture definitions.

Keywords: Information Security Culture, Culture, Shared-Value View, Action-Based View, Mental Model View, Problem-Solving View.

1 Introduction

In information security culture, the concern is no longer in the technical aspect of information security but the balance between processes and technology with the actors such as individuals, groups and organizations [34]. It is well established that cultivation of information security culture in a social context influences the behaviors of individuals which result in significant effects on the protection of information [15, 45]. This importance of information security culture has resulted in numerous studies centered on "security culture" and its relationship to different information security subjects such as information security, information security privacy, information security management, and security education training and awareness (SETA) [7, 9, 12, 50]. While information security culture is increasingly researched in the information security field, the term "information security culture", lacks a shared understanding of its definition [37].

This lack of shared understanding of the definition of information security culture is not only inherited from "culture" but also from the main field of information systems [2]. Culture is a complex phenomenon that spans from different fields and has numerous definitions in the literature [31, 46]. These definitions of culture emphasize on

different concepts which include values, symbols, knowledge, behavior, attitudes, belief, perception and underlying assumptions [21, 30, 41, 48]. This complexity of culture has also impacted the theoretical clarity and conceptualization of information security culture in the literature. Depending on the culture theory used, researchers in information security culture focus their understanding of information security culture on actions (behaviors) [38, 49], and shared organizational values [7, 10, 11]. Other researchers categorize information security culture as a part of or as a subculture of organizational culture [42]. These different definitions of information security culture also impact the cultural dimensions, concepts, frameworks and type of analysis used to assess information security culture. This lack of clarity brings the need to study further, what information security culture entails.

What information security culture is and what it entails has essential consequences for recognizing information security culture as a contributing domain of knowledge to information security and information systems. As it has been for information systems conceptualizations [2, 5], a definition of information security culture is of interest because it can help in establishing a common ground for understanding and researching information security culture in the organization and different social contexts including cross-cultural studies. Also having a shared understanding will make it easy for researchers to compare and build upon each other's work [2, 5].

Therefore, the goal of this article is to advance the understanding of information security culture, by critically reflecting on how information security culture is defined in the information security literature. The objective is not to provide yet another definition for information security culture or to develop a taxonomy but to review and compare different views of the term information security culture. We recognize that other studies have reviewed the literature on information security culture in terms of dimensions and frameworks used to assess information security culture also provided a short review of different definitions of information security culture [1, 26, 37]. What distinguishes our studies with other studies is that we provide a systematic collection and review of definitions of information security culture categorized in four views of culture.

Since information security culture has its roots in culture, we extend Straub et al. [46] classification of definitions of culture to categorize definitions of information security culture. Straub et al. [46] classified culture into three categories, as (i) shared value views like Hofstede's cultural theory [20] (ii) outcomes-oriented (problem-solving) views like Schein's [40, 41] and (iii) General All-encompassing definitions and distinctions. Enrolling to their school of thought, we extend this categorization of definitions of culture as a framework to differentiate understandings of information security culture in the literature. The review of the literature on information security culture in this article follows a hermeneutic framework by Boell & Cecez-Kecmanovic [4]. The hermeneutic approach is fit for an understanding of the phenomenon of interest while emphasizing on critical engagement [4].

The next section will present the methodology used to identify the definitions of information security culture. Section 3 will present a review of culture theories used as a basis in information security culture definitions. Then Section 4 introduces the

views and Section 5 critically reviews the four views of the definition of the information security culture. Finally, Section 6 will conclude the paper.

2 Methodology

The review process and framework followed in this paper is a hermeneutic framework [4]. It was fundamental for this study to follow a hermeneutics approach, as it is appropriate for the understanding of the phenomenon of interest while emphasizing on critical engagement [4]. The enquiry was accomplished by reviewing and analyzing information security and culture literature related to the field of information system. We included a mini review of culture theories since many researchers in information security culture used different culture theories to guide their definition of information security culture. The literature on the theory of culture was drawn from management, anthropology, and ethnography. This review of culture also assisted in increasing understanding and categorizing definitions of information security culture into related themes. The theories used indicated to affect not only the definitions but also the cultural dimensions, constructs, frameworks and analysis method used in different studies.

Searches were done through Google Scholar, Scopus and databases such as JSTOR, ProQuest and Elsevier. The preliminary search started with a Google scholar search engine because of its broader scope of results. To identify relevant literature, we searched the phrase "information security culture" it resulted in 2510 results. To narrow down the search, we used advanced search with a phrase allintitle: "information security culture" and obtained 212 articles from google scholar, and a search in SCOPUS resulted into 154 articles. Because we are following hermeneutics framework, at first, we retrieved a small set of the highly relevant publications. We started our review with 90 articles.

Sorting and selection criteria were done based on the following, publications with a definition of information security culture, with phrases like information security culture "is" or "defined as". We included definitions which have an indirectly implied understanding of information security culture; this was because information security culture is a complex phenomenon that spans from multiple fields. To narrow the scope the definition kept for analysis was from information security and information systems field. To ensure the quality of research, the majority of selected literature were from reputable peer-reviewed journals and conference proceedings articles [53]. More in-depth searches were further done by citation tracking, using backwards and forwards lookup [53]; this process aided to learn more about information security culture and culture theories in the literature. Our initial plan was to include only definitions from 2010; we concluded that definitions older than 2010 must be included in the review because they play an essential role on building the foundation of many current understandings. In the end, we reviewed sixteen distinct definitions of information security culture. For synthesis, analysis and a better understanding of the literature, we did a qualitative research analysis using AtlasTi. The tool helped analyze literature by thematically grouping concepts and adding relationships between concepts.

3 Culture

This section presents theories of culture that contain different and shared concepts such as values, symbols, knowledge, behavior, attitudes, belief, perception and underlying assumptions [21, 30, 41, 48]. These theories of culture formed the basis for many of the definitions of information security culture in the reviewed literature. These culture theories have also been used to develop information security culture frameworks and formed information security culture dimensions.

3.1 Culture

Culture is a crucial but complex phenomenon that spans across different disciplines such as anthropology, ethnography, sociology, psychology, management studies and information systems. One influential definition of culture is that of Tylor [48]. The researcher relates culture to civilization and defined culture in an ethnographic view as *'..that complex whole which includes knowledge, belief, art, morals, law, custom, and any other capabilities and habits acquired by man as a member of society.'* [48]. *A* different perspective of culture is from social anthropologists Kroeber and Kluckhohn [30] who conducted a critical review of 164 culture definitions. They defined culture as *"… a product; is historical; includes ideas, patterns, and values; is selective; is learned; is based upon symbols, and is an abstraction from behaviour and the products of behaviour*" [30].

Kroeber and Kluckhohn [30], viewed culture as a patterned way of behaving, including implicit behaviours. They further claim that culture influences and shape the behaviours of individuals according to what is expected from them. Thus, culture naturally establishes a system of behaviour rewards and punishment expectations, where members of a group know what type of behaviour can be rewarded or punished [30]. Culture is categorized based on distinct dimensions of shared values at the national level [20], organizational level [6, 21, 41], subunit level [35], and individual level [46]. Majority studies in information security have conceptualized culture based on national and organizational level dimensions.

National culture level. An organizational social anthropologist, Hofstede [21] defined culture at a national level as *"the collective programming of the mind which distinguishes the members of one group or society from those of another*". According to Hofstede [21], values form the core of culture, and an individual acquires culture from his/her group [21, 48] and culture distinguishes one group from another [21]. Although there are myriad of national culture dimensions in the literature [18, 21, 22, 43], Hofstede's [21] theory of culture is extensively used and well endorsed in information system and information security research. Information security studies have used Hofstede's national level dimensions for assessments of cultural values in information security threats, behavioral issue, privacy concerns, data protection [17, 24, 44], and cross-cultural comparisons [9, 23, 31, 46, 52].

Organizational culture level. There are many organizational culture frameworks used in information security research. This study acknowledges organization culture frameworks from theorist such as Schein's [41], Hofstede [21], Kotter & Heskett [28],

Detert, Schroeder, & Mauriel [14], and the competing values framework of Quinn & Spreitzer [36]. This section presents a review of Schein's organizational culture framework and its relation to information security in the organization. Schein [41] defines culture as *"…the pattern of basic assumptions that a given group has invented, discovered, or developed in learning to cope with its problems of external adaptation and internal integration, and that have worked well enough to be considered valid, and therefore to be taught to new members as the correct way to perceive, think, and feel in relation to those problems"*. Also, Schein [41] claims that an organization can have many subcultures depending on their role. Consequently, researchers in information security, also categorize ISC as a subculture of the organization culture [42]. Moreover, the majority of information security culture dimensions have their origin from Schein's organizational culture frameworks [1, 38, 49], fewer with Hofstede [21] organizational culture [47] and the Competing values frameworks (CVF) of Quinn and Spreitzer [36] adopted by [7].

4 Classifications of Information Security Culture Definitions

In the realization of many distinct definitions of security culture and their inheritance from culture definitions, we extended the classifications of the definition of culture based on [46]. Straub et al. [46] classified culture into three categories, as (i) Shared value views like Hofstede's cultural theory [21] (ii) Outcomes-oriented (problem-solving) views like Schein's [41] and (iii) General All-encompassing definitions and distinctions. While this earlier classification of culture by [46] informed the formation of our understanding of categories, our analysis is distinct as we were interested in definitions of information security culture rather than culture. Hence this study categorized information security cultural definitions as follows:

i. Shared values view: highlights the set of security values patterns shared across the organization
ii. Action-based view: emphasizes the security behaviours of individuals in the organization
iii. Mental model view: relates to the individual's thinking on how information security culture works
iv. Problem-solving view: relates to a combination of understanding from values-based and action-based views

The classification of each definition, as shown in Table 1, is undertaken according to its most prevalent emphasis concerning these views.

Table 1. Some definitions of information security culture and their corresponding views

View	Definition of information security culture
Shared values view	"reflects the values and beliefs of information security shared by all members at all levels of the organization." [13]
	"a collection of high-level shared security values, beliefs and assumptions in information security." [8]
	"a shared pattern of values, mental models and activities among users or employees" [27]

	"is a specific mode of the organization and development of a subject's information activity, which is represented in the value-oriented models of his information interaction as a sender and receiver of information, under which he determines and controls the unity of existence and development of information objects in their cognitive and communicative manifestations." [3]
Action-based view	"The totality of patterns of behavior in an organization that contributes to the protection of information of all kinds. The prevalence of a security culture acts as a glue that binds together the actions of different stakeholders in an organization" [16]
	"The assumption about which type of information security behavior is accepted and encouraged in order to incorporate information security characteristics as the way in which things are done in an organization" [32]
	"is a subculture in regard to general corporate functions. It should support all activities, so that information security becomes a natural aspect in the daily activities of every employee." [42]
Mental model view	"The way our minds are programmed that will create different patterns of thinking, feeling and actions for providing the security process" [39]
	"a shared pattern of values, mental models and activities among users or employees" [27]
	"a system consisting of interacting framework and content components. Framework contains standardization, certification and measurement of information security. Content includes people attitude, motivation, knowledge and mental models about information security" [19]
Problem-solving view	"the attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organization's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behavior (i.e. incidents) evident in artefacts and creations that become part of the way things are done in the organization to protect its information assets. This information security culture changes over time." [49]
	"The collection of perceptions, attitudes, values, assumptions and knowledge that guides how things are done in organization in order to be consistent with the information security requirements with the aim of protecting the information assets and influencing employees' security behavior in a way that preserving the information security becomes a second nature." [1]
	"a patterned way of security-based thinking shared within an organization; based on values, assumptions, and beliefs, which influences the behaviors and actions of the individuals so that, information security becomes a natural aspect in the daily activities in the organization. This ISC is developed, learned and changes with time with the aim to protect information assets and preserve confidentiality, integrity, and availability of information and information systems resources so as meet to the core organization vision" [38]

4.1 Shared Values View

Definitions in this view emphasized the importance of a set of cultural values as a basis for information security culture in the organization. One exemplar definition is that of [13] who define information security culture from an organization culture definition by [7] as the "*values and beliefs of information security shared by all members at all levels of the organization*". These definitions, as seen in Table 1, are driven with the fact that shared cultural values influence information security culture. Different studies have shared values definitions views as a basis for their evaluation of the information security culture in the organizations. These shared values are based on organizational values [7, 11] and also national values [47]. Chang & Lin [7] emphasized that understanding organizational cultural values is a prerequisite in understanding the information security culture of the organization. Understanding of the shared values is necessary for providing security initiatives that prosper in the organization.

The definitions in this view, do not generally deny the importance of other views of information security culture definitions like action-based view or mental models view,

but they emphasized on a set of shared values in the organization. For instance, Connolly et al. [10] investigated the impact of organizational values such as people-orientation, solidarity, sociability, task orientation and flat [31] on individual security behaviors. Tang, Li, & Zhan [47] defined information security culture by using values-based dimensions such as accountability, communication, compliance and governance. They used Hofstede's dimension of organizational culture namely process-oriented versus results-oriented, employee-oriented versus job oriented, parochial versus professional, open system versus closed system, loose versus tight control and normative versus pragmatic to qualitatively develop propositions that form the causal linkages between organization culture values and information security culture dimensions.

4.2 Action-Based View

Definitions in action-based view as seen in Table 1 emphasize the behavior and activities in the organization and how these actions contribute to the information security of the organization. The central to understanding information security culture according to the action-based view, are the activities that are performed which support information security culture. These are highlighted by definitions referring to aspects such as behaviors, activities, way things are done [16, 32, 42, 49]. One exemplar definition that many current understandings [1, 49, 51] have advanced is that of [32] where they define information security culture as "*the assumption about which type of information security behavior is accepted and encouraged in order to incorporate information security characteristics as the way in which things are done in an organization.*"

The majority of literature in this category adopted [41] definition of organizational culture, and some researchers categorized information security culture as a subculture of the organizational culture [42]. Schlienger and Teufel [42] argue that similar to the organizational culture, ISC must be created, maintained and changed continuously. Other researchers, emphasizes the need to explore the underlying patterns of behavior at the individual, group and organization level [49]. The view supports the cultivation of information security culture as the influence on the behaviors of individuals, which can result in a significant effect in the protection of information [34, 49]. Moreover, Schein's [41] definition of culture emphasizes on learning techniques in order to solve problems in the organizations, and the action-based view makes a significant contribution to information security culture with research on security awareness, training and education (SETA) programs and its influence to information security culture [8, 15, 33].

4.3. Mental Model View

The mental model view as seen in Table 1 is the view of information security culture where the emphasis is on " human's (individuals') thinking about how information security culture should work. One exemplar definition is such as "*the way our minds are programmed that will create different patterns of thinking, feeling and actions for providing the security process*" [39]. Some definitions in the mental model view can also be categorized as a shared view, like [27] defines information security culture as "*a shared pattern of values, mental models and activities among users or employ*ees".

These definitions deal with issues of the minds of the individual culture bearers [46]. Similar to the social view of information systems definitions, this view of information

security culture is socially determined. Actions on information security culture rely on the individuals' interpretation and meaning creation that makes information security culture [27, 39].

4.3 Problem-Solving View

A problem-solving view definition of information security culture presents a combination of understanding of the shared values and action-based view definitions as seen in Table 1. One exemplar definition is that of [38] where they define information security culture as *"a patterned way of security-based thinking shared within an organization; based on values, assumptions, and beliefs, which influences the behaviors and actions of the individuals so that, information security becomes a natural aspect in the daily activities in the organization. This ISC is developed, learned, and changes with time to protect information assets and preserve confidentiality, integrity, and availability of information and information systems resources to meet to the core organization vision."*

A problem-solving view of information security culture is the most promising view. This view looks at what information security culture as a solution can accomplish in the organization [46] by also considering specific organizational values and required actions (behaviors) of the individual. According to Schein (2004), organizations strive for internal integration and external adaptation to ensure business continuity. Similarly, the purpose of information security is to ensure business continuity by preventing the impact of security incidents [16, 45]. Hence with information security culture organization must survive from the external and internal security threats. Internal threats are such as humans (employees) with malicious and non-malicious intents. Humans are bound to consciously or unconsciously cause security violations [29]. Non-malicious intent also categorized as human errors include poor security practices such as opening an unsafe attachment or accessing unsafe URLs, sharing a password, using weak passwords, loss of devices, unclear security policy and procedures, using a known faulty system, and improper systems configuration. As a consequence, information security culture is necessary to make sure an organization can cope with organizational problems of external adaptation and internal integrational for business continuity [41].

5 Discussion

The views are used with different underlying theories or frameworks of culture. However, there is still a need for a critical reflection on each of these views. The objective is not to provide another definition of information security culture but to review and compare the view and their practicality in pushing forward information security culture understanding. How is each view contributing to the understanding, assessment and cultivation of information security culture? To engage in the reflection, we use Alter's [2] framework to assess definitions based on criteria for judging the merits of conceptual models adopted from [25] as seen in Table 2.

- Simplicity: Definitions under the information security culture view are simple other things being equal.

- Clarity: Definitions under the information security culture view contain concepts that are clear and explicit.
- Scope: Definitions under the information security culture view cover the scope of the area of interest and do not overlook essential phenomena and issues.
- Systematic power: Definitions under the information security culture view helps in organizing concepts, relationships, and information related to whatever is being defined.
- Explanatory power: Definitions under the information security culture view helps in describing and explaining the phenomenon and predicting outcomes.
- Reliability: Definitions under the information security culture view lead to relatively similar observations and under-standings when applied to the same situation by different observers.
- Fruitfulness: Definitions under the information security culture view lead to essential questions for research and practice, and help in answering those questions

Table 2. Criteria for judging information security culture definition based on [2, 25]

	Shared values view	**Mental model view**	**Action-based view**	**Problem-solving view**
Simplicity	Yes	No, definitions are abstract	Yes	No, definitions are complex
Clarity	No	No	Yes	Yes
Scope	Yes	No	No	Yes
Systematic power	Yes	No	Yes	Yes
Explanatory power	Yes	Yes	Yes	Yes
Reliability	No	No	Yes	Yes
Fruitfulness	Yes	Yes	Yes	Yes

The shared values view. This view of information security culture encourages research that contributes to the understanding of the role of organizational or national values on influencing information security culture in the organization. This view is simple, has systematic power, explanatory power and covers a broader scope. However, the view lack of clarity because the information security culture assessment focuses on the core cultural values concepts than information security. Moreover, this view lacks reliability due to the lack of consensus on the shared cultural values for the assessment of information security culture. This view has an added value of fruitfulness as it contributes to the development of research that is based on national cultures [24] such as cross-cultural studies [52] and those based on organizational culture [10, 47].

The action-based view. The definitions in this view are simple, and they focus more on individual behavior and activities than holistic organizational security. Programs such as a SETA are seen as the primary drive in the cultivation of information security culture [8, 15, 33]. Research in action-based view focuses on how behaviors influence information security culture. Moreover, this view contains clear concepts, explanatory power, reliability and fruitfulness. The limitation of this view is the lack of scope in terms of the holistic organizational need for security.

The mental model view. The drawback of this view is that conceptualization is abstract and unconscious [52]. Furthermore, the view is challenging in formulating practical

information security culture strategies due to the idiosyncratic interpretation of security. Nevertheless, the mental model view has the potential to lead towards new insight by looking at the psychological and social aspect and cultivation of information security culture in the organization.

The problem-solving view. This view has the potential to overcome the limitations of shared values, action-based and mental model. The problem-solving view provides a more practical definition of culture. It opens a scope for researchers to create studies with the combination of identified values specific to the organization, action appropriate for the organization and the perceived outcome on the information security culture.

The definitions in problem-solving contain clear concepts, cover a broader scope, have systematic power, explanatory power, reliability and fruitfulness. Reviewed literature have shown that understandings of information security culture in a problem-solving view have a potential to produce research to investigate information security culture holistically in terms of understanding, assessment, cultivation and improvement of information security culture in the organization [38, 49]. The only limitation on this category is that it lacks simplicity, although definitions are understandable, they are not simple.

6 Conclusion

The review of information security culture definitions shows that information security culture is a complex phenomenon, inheriting its complexity from culture. By using the hermeneutic approach and extracting themes from the definitions in the reviewed literature, we extended the classification of Straub et al. [47]. We thematically categorized information security culture definitions into four views; shared values view, action-based view, mental model view and problem-solving view. The review has shown that each understanding of information security culture contributes to useful research in information security. These views can be applied to investigate specific research problems, such as core values (organization or national level), SETA based research, behavioral, and holistic organizational information security culture. These views also allow researchers to explore information security culture from specific viewpoints, and in combinations of different views. The problem-solving view, for instance, creates an opportunity to use a combination of shared values, and action-based understanding to create a well-rounded information security culture research.

The discussion included analysis of the information security culture definitions using criteria for evaluating information systems definitions, on simplicity, clarity, scope, systematic power, explanatory power, reliability, the fruitfulness of the definitions [2, 25]. These criteria show that each view has its limitations. A shared values view lacks clarity and consensus on the set of patterned values used for the assessment of culture. The problem-solving view lacks clarity. An action-based has a limited scope, while the mental model view is abstract and challenging in assessing information security culture. Future research should consider exploring these definitions in detail using alternative assessment methods such as the ontological and epistemological assumptions to uncover new and exciting research directions.

References

1. Alhogail, A.: Information Security Culture : A Definition and A Literature Review. IEEE. (2014).
2. Alter, S.: Defining information systems as work systems: Implications for the IS field. Eur. J. Inf. Syst. 17, 5, 448–469 (2008). https://doi.org/10.1057/ejis.2008.37.
3. Astakhova, L. V: The concept of the information-security culture. Sci. Tech. Inf. Process. 41, 1, 22–28 (2014). https://doi.org/10.3103/S0147688214010067.
4. Boell, S.K., Cecez-Kecmanovic, D.: A hermeneutic approach for conducting literature reviews and literature searches. Commun. Assoc. Inf. Syst. 34, 1, 257–286 (2014).
5. Boell, S.K., Cecez-Kecmanovic, D.: What is an Information System ? MARCH, (2015). https://doi.org/10.1109/HICSS.2015.587.
6. Cameron, K.S., Quinn, R.E.: Diagnosing and Changing Organizational Culture. (2011).
7. Chang, S.E., Lin, C.-S.: Exploring organizational culture for information security management. (2007). https://doi.org/10.1108/02635570710734316.
8. Chen, Y. et al.: Impacts of comprehensive information security programs on information security culture. J. Comput. Inf. Syst. 55, 3, 11 (2015). https://doi.org/10.1080/08874417.2015.11645767.
9. Chen, Y., Zahedi, F.M.: Individuals ' internet security perceptions and behaviors : polycontextual contrasts between the United States and China. MIS Q. 40, 1, 205–222 (2016).
10. Connolly, L. et al.: Organisational culture, procedural countermeasures, and employee security behaviour A qualitative study. Inf. Comput. Secur. 25, 2, 118–136 (2017). https://doi.org/10.1108/ICS-03-2017-0013.
11. Connolly, L., Lang, M.: Information Systems Security: The Role of Cultural Aspects in Organizational Settings. Inf. Syst. Secur. (2013).
12. Crossler, R. et al.: Future directions for behavioral information security research. Comput. Secur. 32, 90–101 (2013). https://doi.org/10.1016/j.cose.2012.09.010.
13. D'Arcy, J., Greene, G.: Security culture and the employment relationship as drivers of employees' security compliance. Inf. Manag. Comput. Secur. 22, 5, 474–489 (2014). https://doi.org/10.1108/IMCS-08-2013-0057.
14. Detert, J.R. et al.: A framework for linking culture and improvement initiatives in organizations. Acad. Manag. Rev. (2000). https://doi.org/10.5465/AMR.2000.3707740.
15. Dhillon, G. et al.: Interpreting information security culture: An organizational transformation case study. Comput. Secur. 56, 63–69 (2016). https://doi.org/10.1016/j.cose.2015.10.001.
16. Dhillon, G.: Managing Information System Security. Macmillan International Higher Education (1997).
17. Dinev, T. et al.: User behaviour towards protective information technologies: The role of national cultural differences. Inf. Syst. J. 19, 4, 391–412 (2009). https://doi.org/10.1111/j.1365-2575.2007.00289.x.
18. Hall, E.T., Hall, M.R.: Understanding cultural differences. Intercultural press (1989).
19. Helokunnas, T., Kuusisto, R.: Information Security Culture in a Value Net. IEEE Int. Eng. Manag. Conf. 190–194 (2003).
20. Hofstede, G.: Cultural dimensions in management and planning. Asia Pacific J. Manag. 1, 2, 81–99 (1984). https://doi.org/10.1007/BF01733682.
21. Hofstede, G. et al.: Cultures and organizations: Software for the mind. McGraw-Hill, New York, NY. (2010).
22. House, R.J. et al.: Culture, leadership, and organizations: The GLOBE study of 62 societies. Sage publications (2004).

23. Hovav, A., Arcy, J.D.: Information & Management Applying an extended model of deterrence across cultures : An investigation of information systems misuse in the U . S . and South Korea. Inf. Manag. 49, 2, 99–110 (2012). https://doi.org/10.1016/j.im.2011.12.005.
24. Ifinedo, P.: The Effects of National Culture on the Assessment of Information Security Threats and Controls in Financial Services Industry. Int. J. Electron. Bus. Manag. 12, 2, 75–89 (2014).
25. Järvelin, K., Wilson, T.D.: On conceptual models for information seeking and retrieval research. Inf. Res. 9, 1, 1–20 (2003).
26. Karlsson, F. et al.: Information security culture – state-of-the-art review between 2000 and 2013. (2016). https://doi.org/10.1108/ICS-05-2014-0033.
27. Karyda, M.: Fostering Information Security Culture in organizations : A research agenda. In: Mediterranean Conference on Information Systems (MCIS). pp. 1–10 (2017).
28. Kotter, J.P., Heskett, J.L.: Corporate culture and performance. (1992). https://doi.org/10.1080/15367100903202706.
29. Kraemer, S., Carayon, P.: Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. Appl. Ergon. 38, 2, 143–154 (2007). https://doi.org/10.1016/j.apergo.2006.03.010.
30. Kroeber, A.L., Kluckhohn, C.: Culture: A critical review of concepts and definitions. Pap. Peabody Museum. 47, 1, 223 (1952).
31. Leidner, D.E., Kayworth, T.: A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict. MIS Quartely. 30, 2, 357–399 (2006).
32. Martins, A., Eloff, J.: Information Security Culture. Secur. Inf. Soc. 203–214 (2002).
33. Menard, P.: Proposing SETA Program Design Based on Employee Motivational Fit. Am. Conf. Inf. Syst. 1–5 (2016).
34. Van Niekerk, J., Von Solms, R.: Information security culture: A management perspective. Comput. Secur. 29, 4, 479–486 (2010). https://doi.org/10.1016/j.cose.2009.10.005.
35. Quinn, R.E., Rohrbaugh, J.: A Spatial Model of Effectiveness Criteria : Towards a Competing Values Approach to Organizational Analysis. Manage. Sci. 29, 3, 363–377 (1983).
36. Quinn, R.E., Spreitzer, G.M.: The psychometrics of the competing values culture instrument and an analysis of the impact of organizational culture on quality of life. Emerald (1991).
37. Ramachandran, S. et al.: Variations in information security cultures across professions: A qualitative study. Commun. Assoc. Inf. Syst. 33, 1, 163–204 (2013). https://doi.org/10.17705/1CAIS.03311.
38. Ruhwanya, Z., Ophoff, J.: Information Security Culture Assessment of Small and Medium-Sized Enterprises in Tanzania. In: Information and Communication Technologies for Development. Strengthening Southern-Driven Cooperation as a Catalyst for ICT4D. pp. 776–788 Springer International Publishing (2019). https://doi.org/10.1007/978-3-030-18400-1.
39. Sabbagh, B. Al, Kowalski, S.: Developing social metrics for security modeling the security culture of it workers individuals (case study). 5th Int. Conf. Commun. Comput. Appl. 3, 1, 112–118 (2012).
40. Schein, E.H.: Coming to a New Awareness of Organizational Culture. Sloan Manage. Rev. 2, 3–16 (1984).
41. Schein, E.H.: Organizational Culture and Leadership. Jossey-Bass (2004). https://doi.org/10.1080/09595230802089917.

42. 42. Schlienger, T., Teufel, S.: Information security culture – from analysis to change. South African Comput. J. 31, 46–52 (2003).
43. Schwartz, S.H.: Beyond individualism/collectivism: New cultural dimensions of values. (1994).
44. 44. Smith et al.: Information Privacy Research: An Interdisciplinary Review. MIS Q. 35, 4, 989 (2011). https://doi.org/10.2307/41409970.
45. Von Solms, B., Von Solms, R.: The 10 deadly sins of information security management. Comput. Secur. 23, 5, 371–376 (2004). https://doi.org/10.1016/j.cose.2004.05.002.
46. Straub, D. et al.: Toward a Theory-Based Measurement of Culture. J. Glob. Inf. Manag. 10, 1, 13–23 (2002). https://doi.org/10.4018/jgim.2002010102.
47. Tang, M. et al.: The impacts of organizational culture on information security culture: a case study. Inf. Technol. Manag. 17, 2, 179–186 (2016). https://doi.org/10.1007/s10799-015-0252-2.
48. Tylor, E.B.: Primitive culture: researches into the development of mythology, philosophy, religion, art, and custom. J. Murray (1871).
49. Da Veiga, A., Eloff, J.H.P.: A framework and assessment instrument for information security culture. Comput. Secur. 29, 2, 196–207 (2010). https://doi.org/10.1016/j.cose.2009.09.002.
50. Da Veiga, A., Martins, N.: Defining and identifying dominant information security cultures and subcultures. Comput. Secur. (2017). https://doi.org/10.1016/j.cose.2017.05.002.
51. Da Veiga, A., Martins, N.: Information security culture and information protection culture: A validated assessment instrument. Comput. Law Secur. Rev. 31, 2, 243–256 (2015). https://doi.org/10.1016/j.clsr.2015.01.005.
52. Warkentin, M. et al.: Cross-cultural IS research: Perspectives from Eastern and Western traditions. Eur. J. Inf. Syst. 24, 3, 229–233 (2015). https://doi.org/10.1057/ejis.2015.7.
53. Webster, J., Watson, R.T.: Analyzing the past to prepare for the future: writing a literature review. MIS Q. 26, 2, xiii–xxiii (2002). https://doi.org/10.1.1.104.6570.