Journal of Information Security and Applications 44 (2019) 12–22

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

An analysis on the dimensions of information security culture concept: A review

Akhyari Nasir[a,*], Ruzaini Abdullah Arshah[b], Mohd Rashid Ab Hamid[c], Syahrul Fahmy[a]

[a] Faculty of Computer, Media and Technology Management, TATI University College, Teluk Kalong, Kemaman, Terengganu 24000, Malaysia
[b] Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang, Lebuhraya Tun Razak, Kuantan, Pahang 26300, Malaysia
[c] Faculty of Industrial Management, Universiti Malaysia Pahang, Lebuhraya Tun Razak, Kuantan, Pahang 26300, Malaysia

ARTICLE INFO

Article history:

Keywords:
Information security culture
ISC concept
ISC model
ISC dimensions

ABSTRACT

The cultivation of positive *Information Security Culture* (ISC) is an effective way to promote security behavior and practices among employees in the organization. However, there is yet a consensus on a standard set of dimensions for the ISC concept. ISC has been associated with many facets, with some overlapping dimensions found in the literature. There is little explanation, if any, as to why this happens or to what extent do variances of dimensions affects ISC concept and findings. This paper presents an analysis of the different dimensions in conceptualizing the ISC. Eight major databases including *Web of Science, Scopus* and *Google Scholar* were systematically exhausted using PRISMA and a total of 79 studies from 2000 to 2017 was selected for analysis. While different approaches such as adopted theories affect the dimensions of ISC, our analysis also covered other contributing factors such as the objective of the study, type of organization under study and the information security maturity level. In addition, we found no evidence of a set of widely accepted concepts and dimensions for ISC. This review provides substantial evidence on the numerous dimensions used in ISC and could be utilized by academicians as a reference in ISC-related studies.

1. Introduction

Information Security Culture (ISC) is accepted as an effective way to promote secure behavior and to manage security risks in the organization (Baggett [15]; Dervin, Kruger and Steyn [27]; Martins and Eloff [63]; Ruighaver and Maynard [95]; Schlienger and Teufel [103]; Von Solms [123]; Zakaria [126]). Although there are numerous studies in this area, there is a lack of widely accepted dimensions for ISC as different perspectives and concepts are used. This causes problems for academician in identifying the actual concept of ISC as well as for the practitioners to cultivate and assess a positive ISC in the organization, thus limiting its full potential.

There are different dimensions of ISC found in the *Information Security Policy* (ISP) compliance behavior literature. For example, D'Arcy and Greene [25] used *Top Management Commitment, Security Communications* and *Computer Monitoring* whilst Alkalbani, Deng, and Kam [9] used *Top Management Commitment, Accountability* and *Information Security Awareness* as dimensions in ISC. Although they share a similar dimension (*Top Management Commitment*), they did not agree on other dimensions and incorporated different dimensions in their respective studies. As such, the effect of ISC towards ISP could not be significantly attributed to the specific dimensions.

There are also a number of ISC models and frameworks developed based on specific dimensions and research objectives. Alhogail and Mirza [8] in their Systematic Literature Review of ISC-related studies for the period of 2003–2013 discovered 12 out of 62 studies discussing ISC models and frameworks. Interestingly, these models used different dimensions from one and another.

Despite several recent views on ISC including Karlsson, Astrom and Karlsson [52]; Karwowski, Glaspie and Karwowski [37]; and Mahfuth, Yussof, Baker and Ali [62]; there is little interest in the identification of ISC dimensions. Mahfuth et al. [62] conducted a review to identify ISC based on definitions and frameworks in studies between 2003 and 2016. Although they managed to identify ISC dimensions in their review, there was no further analysis on these dimensions. Karlsson et al. [52] conducted an extensive review ranging from 2000 to 2013 by classifying ISC studies based on four main categories: *Research Topic, Underlying Theory(ies), Research Purpose* and *Research Method*. Although this study provided a significant findings by providing a clear summary on the particular themes investigated, including the theories and concepts that in-

* Corresponding author.
E-mail addresses: akhyari@tatiuc.edu.my (A. Nasir), ruzaini@ump.edu.my (R.A. Arshah), rashid@ump.edu.my (M.R.A. Hamid), fahmy@tatiuc.edu.my (S. Fahmy).

https://doi.org/10.1016/j.jisa.2018.11.003
2214-2126/

fluence the concept of ISC, however it did not focus on how these underlying theories influence the dimensions of ISC.

Although we agree with Karlsson et al. [52], that there are various concepts that have been adopted for ISC, which would explain why there are different concepts of ISC. However, we strongly feel that the variances go much further than the general concepts of ISC, i.e. there are also differences in the dimensions of ISC. As such, this review is crucial in painting a clearer picture of ISC. In addition to putting forth the notion that the variances in ISC are based on dimensions, this work also report the factors contributing to these variances. This review would benefit academicians in conducting future ISC-related studies as well as practitioners for identifying the various dimensions of ISC. A thorough analysis of concepts, models and frameworks was carried out to investigate the different dimensions of ISC, exhausting publications for the period of 2000 to 2017.

Section 2 presents the methodology adopted in this study. Section 3 discusses the variances of ISC dimensions while the implications of these variances are discussed in Section 4. Section 5 lists the limitations of this work. Conclusion and future work are presented in Section 6.

2. Methodology

This work utilizes the *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA) method [72]. It has two main parts, namely meta-analysis and systematic review. A systematic review provides objective summary of what has been written on the research topic. It is valuable in wide research areas, where many publications exist, each focusing on a narrow aspect of the field [17]. Meta-analysis refers to the use of statistical technique in a systematic review to integrate the results of selected studies [72]. The main objective of PRISMA is the reporting of a transparent literature review [58]. This methodology has been used for a comprehensive literature review in numerous fields [24,51,58]. There are three stages in the implementation of PRISMA in this study: literature search; selection of eligible papers; and data extraction and summary.

2.1. Literature search

Eight leading electronic databases were selected for identifying potential articles: *Scopus, Web of Science, Google scholar, IEEE/IEE Electronic Library, EBSCOhost, ACM Digital Library, Elsevier Science Direct*, and *Emerald Library*. Search was conducted using the keywords "*information security culture*" and "*security culture*". The search included journals and conference articles as well as Masters and PhD thesis published during the period of 2000 to 2017. A total of 405 articles was extracted based on the search strategy. After the removal of duplicated papers with redundant information, 239 potential articles remained. The titles and abstracts were then screened and irrelevant studies were removed, cutting the potential articles to 205.

2.2. Study selection and eligible papers

Full-text articles were reviewed and analyzed for eligibility. These articles consist of studies on ISC models and concepts in the organizational settings. The dimensions used in ISC were carefully identified as some articles did not explicitly mention the dimensions used. We refer to dimensions as "*a distinct aspect that contributes in forming the concept of ISC*". In some articles, dimensions were referred to as "factor". Some papers used these dimensions in discussing ISC cultivation and some papers refer them for improving the current ISC in the organization. Interestingly, we also discovered that some papers such as Da Veiga and Eloff [117]; Martins and Eloff [63]; and Tolah, Furnell, and Papadaki [114] used both terms of cultivating (e.g. create, implement) and managing (e.g. assess, improve) in discussing the ISC concept in their papers. Therefore, as long as the factors fit our definition of dimensions, the articles were selected for further analysis.

Articles that did not discuss the dimensions of ISC were excluded. In addition, articles that discussed ISC in other settings such as smart living environment were also excluded from this review. Articles that discussed *Information Security Climate, Information Security Obedience* or *Information Security Management* without focussing on any ISC model or concepts were excluded as well. Two studies by Nenad [74] and Cárdenas-Solano, Martínez-Ardila, and Becerra-Ardila [18] were excluded since the English version of the paper were not available. A study by Mcintosh [71] too was excluded because the full version of the article could not be downloaded. We also included two more papers that met our criteria from the references of the selected papers. The final number of eligible articles was 79 (see Fig. 1).

2.3. Data extraction and summary

Data were gathered and any disagreement between the authors was discussed and solved. Each article was categorized based on the ISC concept and its dimensions. All dimensions were recorded in a single column (see Table 1). Some articles also discussed the sub-dimensions of ISC and were recorded in the same column. The concepts, theories and approaches adopted in conceptualizing ISC were recorded in the last column.

We found that it is a common practice to use more than a single theory in the conceptualization of ISC. For example, the ISC concept by Schlienger and Teufel [102] is based on concept of *Organization Culture* by Schein [97] and *Corporate Culture* by Rühli [94]. We also discovered a number of articles that solely use literature review to identify the dimensions of ISC. Some articles used both literature review and theory to model ISC. All these approaches were recorded for further analysis.

3. ISC concepts based on dimensions

Table 1 reveals that there are various concepts of ISC based on different set of dimensions. There are at least 48 variances of ISC dimensions found in the literature. Consistent with the findings of Mazhelis and Isomäki [70], our analysis reveals that various theories, concepts and approaches contributed to the variances in ISC dimensions. There were also other factors that contribute to these variances. The following sub-sections discuss this issue by classifying the concepts or theories as well as other factors that contributing to the differences in ISC dimensions in literature.

3.1. ISC based on organizational culture

Earlier ISC studies adopted the concepts of *Organizational Culture* (OC), *Corporate Culture*, and *Organizational Behavior* in conceptualizing ISC. This is not new since Alhogail and Mirza [8], and Pevchikh [85] have acknowledged this fact in their reviews. In addition to the popular concepts of OC by Schein [97–99]; the OC concepts by Detert et al. [28] are also used as reference in the development of ISC models. Since these two concepts are distinct in nature, the ISC dimensions derived from them are apparently different.

As evident in Table 1, majority of the studies used the Schein's OC concepts to conceptualize ISC compared to other concepts. The ISC developed based on this concept have three dimensions representing the three levels of OC, namely *Artifacts and Creations; Col-*

Table 1
Concepts and Dimensions of Information Security Culture.

No.	Author	Dimensions and Sub-Dimensions/Factors (if any)	Adopted Theories, Concepts and/ or Approaches
1.	Schlienger and Teufel [102]	**3 Dimensions**: Corporate Politics, Management, Individuals **11 Sub-dimensions**: Security Policy, Organizational Structure, Resources, Implementation of Security Policy, Definition of Responsibilities, Qualification and Training, Awards and Prosecutions, Audit and benchmarks, Critical Attitude, Act carefully and with due diligence, Communication	■ Organizational Culture [97,99] ■ Corporate Culture [94]
2.	Van Niekerk and Von Solms [75]; Van Niekerk and Von Solms [77]; Van Niekerk and Von Solms [78]; Niekerk [36], Reid and Niekerk [91], Reid et al. [92]; Van Niekerk and Von Solms [76]	**4 Dimensions**: Artefacts, espoused values, shared tacit assumptions, information security knowledge **4 Sub-dimensions**/Factors: ISP, Security Knowledge, Belief, Security Behavior	■ Organizational Culture [97,99]
3.	Da Veiga and Eloff [117]	**7 Dimensions**: Leadership and Governance, Security Management and Operations, Security Policies, Security Program Management, User Security Management, Technology Protection and Operations, Change Management	■ Organizational Culture [97,99] ■ Organizational Behavior [93] ■ Information Security Components (Da Veiga & Eloff [118])
4.	Da Veiga and Martins [120]; Martins and Da Veiga [66], Da Veiga [116]	**9 Dimensions**: Information Asset Management, Information Security Management, Change Management, User Management, Information Security Policies, Information Security Program, Trust, Information Security Leadership, Training and Awareness	■ Organizational Culture [97,99] ■ Organizational Behavior [93] ■ Information Security Components by Da Veiga and Eloff [118], using dimensions similar to Da Veiga, Martins, and Eloff [122]
5.	Martins and Da Veiga [116]	**4 Dimensions**: Management, Policies, Awareness, Compliance **9 Sub-dimensions**: Information Security Commitment, Information Security Importance, Information Security Policy Effectiveness, Information Security Directives, Information Security Responsibility, Information Security Necessity, Information Security Assets, Information Security Monitoring Perception, Information Security Consequences	■ Organizational Culture [97,99] ■ Organizational Behavior [93] ■ Information Security Components by Da Veiga and Eloff [118] ■ Literature Review
6.	Chen et al. [19]	**3 Dimensions**: Artifacts and creations, Collective Values, Norms and Knowledge, Basic assumptions and beliefs **3 Sub-dimensions**: Security Policy, SETA, Computer Monitoring	■ Organizational Culture [97,99] ■ ISC Conceptual Model [77,78]
7.	Parsons et al. [84]	**4 Dimensions**: Sanctions, Rewards, Job Roles, No. of Employee	■ Organizational Culture [97,99] ■ Organizational climate, rewards and punishments
8.	Kraemer and Carayon [56]	**6 Dimensions**: Employee Participation, Training, Hiring Practices, Reward System, Management Commitment, Communication and Feedback	■ Organizational Culture [97,99] ■ Organizational Culture by Guldenmund [39]
9.	Hassan et al. [44]	**12 Dimensions**: Security Knowledge (SK); Security Awareness (SA); Security Behaviour (SB); Security Policy Enforcement; Security Decision Making Should Rely On Facts And Rationality That Security Is Important (SD); Improving Information Security Requires A Long-Term Commitment (SLT); Proper Security Systems And Process Motivate Employee To Adhere To Security Policies And Procedure (SESP); Organizations Must Make Continuous Changes To Improve Information Security (SCH); Employee Should Be Involved In Improving The Overall Organization"s Information Security (SBI); Collaboration And Cooperation Are Necessary For Effective Information Security (SCC); A Shared Security Vision And Shared Security Goals Are Critical For Effective Information Security (SCV); Information Security Needs Should Be Determined By External And Internal Requirements (SEI); Top Management Commitment (TMC)	■ Organizational Culture [97,99] ■ Health Belief Model (HBM) ■ Literature review
10.	Chia et al. (2003a), Ruighaver et al. [96], Chia et al. [20], 2002b], Parsons et al. [83], Koh et al. [54]	**8 Dimensions**: The Basis of Truth and Rationality; The Nature of Time and Time Horizon; Motivation; Stability versus Change/Innovation/Personal Growth; Orientation to Work, Task, Co-Workers; Isolation versus Collaboration/Cooperation; Control, Coordination and Responsibility; Orientation and Focus – Internal and/or External **11 Sub-dimensions**: Belief of The Importance of Security, Trust, Security Goals, Security Strategies, Social Participation, Change Management, Responsible for Security, Employee's Involvement in Security and Collaboration, Top Management Commitment, Security Governance, External Factors and Internal Need	■ Organizational Culture [28]

(*continued on next page*)

Table 1 (*continued*)

No.	Author	Dimensions and Sub-Dimensions/Factors (if any)	Adopted Theories, Concepts and/ or Approaches
11.	Lim et al. [59], Lim et al. [60]	**8 Dimensions**: The Basis of Truth and Rationality; The Nature of Time and Time Horizon; Motivation; Stability versus Change/Innovation/Personal Growth; Orientation to Work, Task, Co-Workers; Isolation versus Collaboration/Cooperation; Control, Coordination and Responsibility; Orientation and Focus – Internal and/or External **5 Sub-dimensions**: Management involvement, locus of responsibility, information security policy, education/training, budget practice	■ Organizational Culture [28]
12.	Ramachandran et al. [90], Ramachandran et al. [88]	**3 Dimensions**: Beliefs about identity, Beliefs about rule compliance, and Beliefs about security	■ Organizational Culture [28] ■ ISC Framework by Tejay and Dhillon [112], Chia et al. [20]
13.	Tang et al. [111]	**4 Dimensions**: Compliance, Communication, Accountability, Governance	■ Hofstede's organizational culture framework [48] ■ Information Technology Security Management [124]
14.	Alhogail [6], Alhogail and Mirza [7], Alhogail [5], Alhogail and Mirza [50], Alhogail and Mirza [7]	**9 Dimensions**: Strategy, Technology, Organizational, People, Environment, Preparedness, Responsibility, Management, Society and Regulations	■ ISC Conceptual Model [77,78]
		10 Sub-dimensions: Training, Focus groups, Change agents, Motivation, Milestones and measures, Involvement, Management support, Resources, Communications, Culture analysis	■ STOPE [16], Human Diamond Dimension and Change Management
15.	Da Veiga et al. [122], Da Veiga [115]	**8 Dimensions**: Information Asset Management, Information Security Management, Change Management, User Management, Information Security Policies, Information Security Program, Trust, Information Security Leadership *__6 Dimensions after factor and reliability analysis__: Management of Information Security, Performance Management, Performance Accountability, Communication, Governance, Capability Development	■ Organizational Behavior [93]
16.	Martins and Eloff [63,64]	**9 Dimensions**: Policy and Procedures, Risk analysis, Benchmarking, Budget, Management, Trust, Awareness, Ethical Conduct, Change	■ Organizational Behavior [93] ■ Organizational Culture
17.	Martins and Da Veiga [67]	**8 Dimensions**: Information Asset Management, Information Security Management, Change Management, User Management, Information Security Policies, Information Security Program, Trust, Information Security Leadership	■ Organizational Behavior [93]
18.	Da Veiga and Martins [119,121], Martins and Da Veiga [68]	**10 Dimensions**: Information Asset Management, Information Security Management, Change Management, User Management, Information Security Policies, Information Security Program, Trust, Information Security Leadership, Training and Awareness, Privacy Perception *__6 Dimensions after factor and reliability analysis__: Information Security Commitment, Management Buy-in, Information Security Necessity and Importance, Information Security Policy Effectiveness, Information Security Accountability, Information Usage Perception	■ Organizational Behavior [93] *Same dimension with Nico Martins and Da Veiga [67] but with two added dimensions of Training and Awareness, Privacy Perception
19.	Helokunnas and Kuusisto [47]	**3 Dimensions**: Technical, Management and Institutional Wave	■ Information Security Awareness by Siponen [107]
20.	Kuusisto et al. [57]	**5 Dimensions**: Resources, Security policy, Commonly accepted norms, The unity of values of all parties involved to security culture forming process, The communication distance.	■ Habermas' theory of communicative action [40,41]
21.	Knapp et al. [53]	**1 Dimension**: Top management	■ Analyze open-ended questions ■ Literature review
22.	Alfawaz et al. [2]	**3 Dimensions**: Knowledge, Skills, and Individual Preferences Work	■ Literature review ■ Utilizing "knowing-doing gap" concept by Pfeffer and Sutton [86], Classification Theory by Smith and Medin [108] and Parsons [82]
23.	Alfawaz [3]	**3 Dimensions**: Organizational culture, National culture, Technological **12 Sub-dimensions**: Top management commitment, IS structure, Skills and training, Awareness, Motivation, Information and knowledge sharing, Information security technology, Change management, Power distance, Individualism vs. collectivism, Uncertainty avoidance, Context	■ National Culture by Hofstede [49] ■ Context Culture Value by Hall [42] ■ ISC Framework by Chia et al. [20]
24.	Baggett [15], Press [87]	**9 Dimensions**: Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management, Reassessment	■ Guidelines for Security of Information Systems and Networks. ■ [80] of the Organization for Economic Cooperation and Development (OECD)
25.	Al-Mayahi and Mansoor [1]	**3 Dimensions**: ISP, ISP Awareness, Compliance	■ The process of full adoption of ISC in an organization by Chia, Maynard, and Ruighaver [20]
26.	Lopes and Oliveira [61]	**11 Dimensions**: Security Policy; Organization of Information Security; Asset Management; Human Resources Security; Physical and Environmental Security; Communications and Operations Management; Access Control; Information Systems Acquisition, Development and Maintenance; Information Security Incident Management; Business Continuity Management; and Compliance	■ ISO IEC 27002:2005 [109]

(*continued on next page*)

Table 1 (*continued*)

No.	Author	Dimensions and Sub-Dimensions/Factors (if any)	Adopted Theories, Concepts and/ or Approaches
27.	Dhillon et al. [29]	**10 Dimensions**: Interaction, Association, Subsistence, Bisexuality, Territoriality, Temporality, Learning, Recreation and Humor, Defense, Exploitation	■ Hall's theory of cultural messages [43]
28.	Sherif and Furnell [105], Sherif, Furnell, and Clarke [106]	**5 Dimensions**: Security behavior, Top Management, Security Awareness and Education, Security Policy, Security Acceptance	■ Literature review on information security compliance and ISC
29.	Ramachandran and Rao [89]	**4 Dimensions**: Security-related Belief, Management Actions Emphasizing IS Security, Management Actions Emphasizing Productivity, Top Management Teams' Belief	■ Literature review
30.	Williams [125]	**4 Dimensions**: Response not Reaction, Responsibility, Community of Practice, Awareness **23 Sub-dimensions**: What is being protected; Value versus cost; Risk assessment; Balanced/suitable response to threats; Internal policy and procedure; Legal; Policy: Standards and best practice; Internal and external obligations and perceptions of data privacy, rights of patients, rights of staff; Governance; Ethics, beliefs and trust; Socialization of the group; Capability; Adaptability to change; Management of security in organization; Information system used; Workflow integration; Risk perception; Security issues; Impact; Objectives of security; Breach identification and consequences; Personal motivation	■ Literature review
31.	Alnatheer and Nelson [14]	**4 Dimensions**: Corporate Citizenship, Legal Regulatory Environment, Corporate Governance, Cultural Factors	■ Literature review
32.	M. Shahibi et al. [104]	**4 Dimensions**: Principles, Organizational Behavior Tier, Culture Level, Security Control	■ Literature review
33.	Hassan and Ismail [45]	**6 Dimensions**: Behavioral, Change Management, Information Security Awareness, Organizational System, Security Requirements, Knowledge	■ Literature review
34.	Alnatheer [12], Alnatheer et al. [13]	**3 Dimensions**: Top Management Involvement, Training, Policy Enforcement	■ Literature review
35.	Alnatheer [10]	**7 Dimensions**: Top Management Support, Security Policy and Policy Enforcement, Security Awareness, Security Training and Education, Security Risk Assessment, Security Compliance, Ethical Conduct	■ Literature review
36.	Temesgen et al. [113]	**5 Dimensions**: Knowledge to information security, Management of Information Security, Communication, Governance, Performance Accountability	■ Literature review
37.	Dojkovski et al. [32], Dojkovski et al. [30], Dojkovski et al. [34]	**5 Dimensions**: Individual and Organizational Learning, E-learning, Managerial, Behavioral, Ethical, National and Organizational Culture **Sub-dimensions**: Policy and Procedures, Benchmarking, Risk Analysis, Budget, Management, Response, Training, Education, Awareness, Change Management, Responsibility, Integrity, Trust, Ethicality, Values, Motivation, Orientation, Personal Growth	■ Literature review
38.	Dojkovski et al. [31], Dojkovski, Lichtenstein and Warren [33]	**9 Dimensions**: Leadership/Corporate Governance, Organizational Culture, Managerial, Individual and Organizational Learning, Organizational Security Awareness, National and Ethical Culture, Government Initiatives, IT Vendors, Behavioral Issues **18 Sub-dimensions**: Risk Analysis, Budget, Policy and Procedures, Response, Self-Assessment, Employment contract/Handbook, E-learning, Training, Education, Informal Awareness, Marketing, Responsibility, Integrity, Trust, Ethicality, Values, Motivation, Orientation, Personal Growth	■ Literature review
39.	D'Arcy and Greene [26]	**2 Dimensions**: Top Management Commitment, Security Communication	■ Literature review
40.	D'Arcy and Greene [25,4]	**3 Dimensions**: Top Management Commitment, Security Communication, Computer Monitoring	■ Literature review
41.	Alkalbani et al. [9]	**3 Dimensions**: Top Management Commitment, Accountability, Information Security Awareness	■ Literature review
42.	Greig et al. [38]	**3 Dimensions**: ISP Awareness, Security Behavior, Information Security Knowledge	■ Literature review
43.	Alnatheer [11]	**8 Dimensions**: Top Management Support, ISP, Information Security Awareness, SETA, Information Security Risk Analysis and Assessment, Information Security Compliance, Ethical Conduct Policies, Organization Culture	■ Literature review
44.	Hassan and Ismail [46]	**4 Dimensions**: Security Behaviour, Security Value, Security Awareness, Enforcement of Security Policy	■ Literature review
45	Tolah et al. [114]	**7 Dimensions**: Top Management Support, ISP, Education and Training, Information Security Risk Assessment, Ethical Conduct, Job Satisfaction, Personality Traits	■ Literature review
46.	Masrek [69], Masrek, Nazrin Harun, and Khairulnizan Zaini [79]	**6 Dimensions**: Management Support, Policy and Procedures, Compliance, Awareness, Budget and Technology	■ Literature review
47.	Fagade and Tryfonas [35]	**6 Dimensions**: Leadership and Governance, Security Management and Organizations, Security Policies, Security Program Management, User Security Management, Technology Protection and Operations	■ Information Security Components (Da Veiga & Eloff [118])
48.	Nasir, Arshah, and Hamid [73]	**7 Dimensions:** ISP, Risk Management, SETA, Top Management, Monitoring, Information Security Knowledge, Information Security Knowledge Sharing	■ Organizational Culture [97,99] ■ ISC Conceptual Model [77,78]

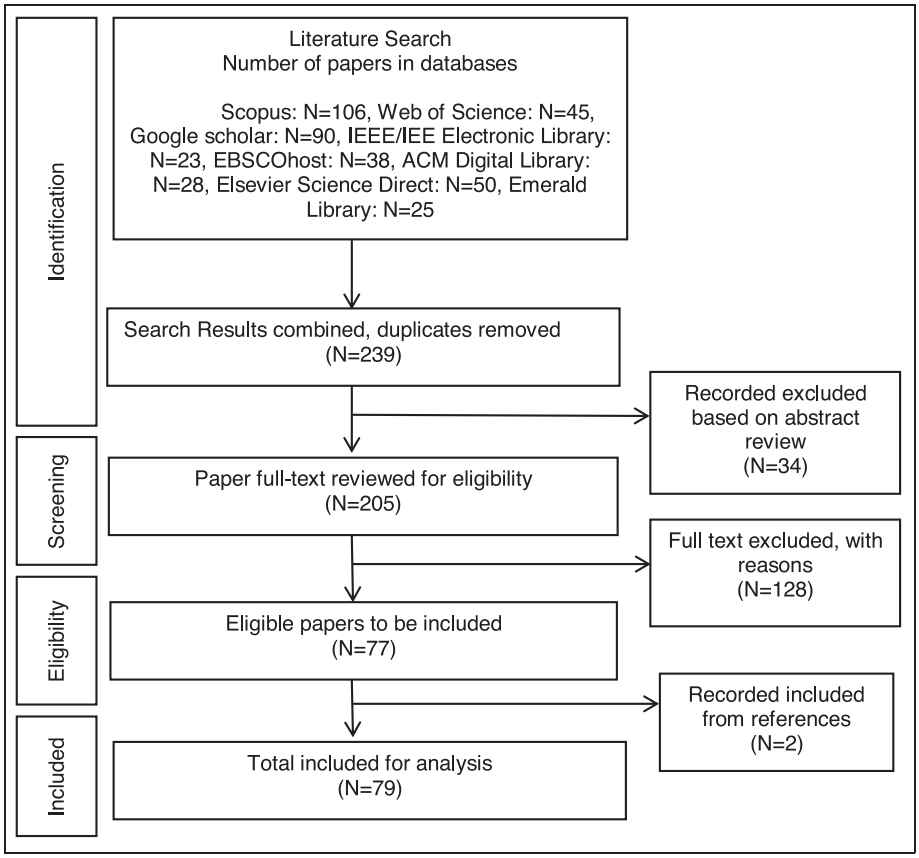

Fig. 1. Flow diagram regarding the systematic search, inclusion and exclusion of studies in our review.

lective Values, Norms and Knowledge; and *Basic Assumptions and Beliefs*.

Interestingly, there is no similar sub-dimensions used in the ISC models. For example, Schlienger and Teufel [102] used three dimensions, which are *Corporate Politics; Management*; and *Individuals;* with 11 sub-dimensions whilst Chen et al. [19] used *Security Policy; Security Education; Training and Awareness (SETA),* and *Computer Monitoring* to represent the three levels of OC. This distinction is also noticed in other ISC models derived from Schein's OC.

One possible explanation for this observation is the use of other concepts in addition to Schein's OC for example the *Organizational Behavior and Information Security Components*, as found in Martins and Da Veiga [65], Da Veiga and Martins [120], and Da Veiga and Eloff [117]; and *Organizational Climate, Rewards* and *Punishments* as found in Parsons et al. [84].

There are also ISC models which were derived solely from Schein's OC without the inclusion of other concepts such as in a series of studies by Van Niekerk and Von Solms [75,77,78]. However, another level was added to the initial three levels of OC, namely *Information Security Knowledge*. In this model, the levels are associated with specific dimensions in each level. For example, they assumed the ISP as a dimension in the *Espoused Value* level of OC. Other dimensions that evolved from these studies are *Belief, Information Security Knowledge, Trust*, and *Top Management Commitment*. This model has been referred in several ISC-related studies. Other recent models derived from Schein's OC include Da Veiga and Martins [120]**;** Martins and Da Veiga [66]**;** and Da Veiga [116].

The second group of ISC models is derived from the OC concepts by Detert et al. [28]. These models have more dimensions compared to the models based on Schein's OC. These ISC models consist of eight dimensions [21,54,96] and developed with the view that these dimensions would fit into all types of organization. Differences are present in terms of strength or level, but not the type of organizations. The authors of these studies believed that OC by Detert et al. [28] is useful and essential in explaining and understanding the ISC concept. They believed and justified the fact that ISC in every organization consisted of these eight dimensions and the differences are only in terms of strength or level of these dimensions but not according to the type of each organization. They promote *Belief, Trust, Security Goals, Security Strategies, Social Participation, Change Management, Responsible for Security, Employee's Involvement in Security and Collaboration; Top Management Commitment; Security Governance; External Factors; and Internal Needs* as sub-dimensions in ISC. Although there is a slight variance in terms of sub-dimensions used, the overall ISC dimensions remain the same.

Although the majority of the studies adopted these two popular concepts of OC, the use of other OC concepts were also found in the literature, for example Hofstede et al. [48] and Guldenmund [39]**.**

3.2. ISC model by Van Niekerk and Von Solms [77,78]

The ISC model by Van Niekerk and Von Solms [77,78] is one of the popular models employing Schein's OC and one of the most referred to. Chen et al. [19] referred to this model in investigating the dimensions of ISC based on information security programs and proposed three dimensions: *Security Policy, SETA*, and *Computer Monitoring*. Nasir et al. [73] used the same approach that produced different dimensions. One possible explanation for this is that Chen et al. [19] focused on information security program whereas Nasir et al. [73] focused on the four levels of ISC model in Van Niekerk and Von Solms [77,78] in developing the ISC dimensions. Other

recent models influenced by Van Niekerk and Von Solms [77] include Alhogail [5]; Alhogail [6]; and Alhogail and Mirza [50]. In these studies, the dimensions of ISC are different from Chen et al. [19] and Nasir et al. [73] as they adopted other concepts in addition to Van Niekerk and Von Solms [77], which are *STOPE (Strategy, Technology, Organization, People, and Environment)* [16], *Human Factor Diamond*, and *Change Management*. We found that Security Policy is the sole common dimension across all studies.

3.3. ISC based on organizational behavior

Apart from the OC concepts by Schein for ISC modeling, some studies adopted the *Organizational Behavior* (OB) concepts by Robbins [110]. This concept is widely used in the development of *Information Security Culture Assessment* (ISCA). ISCA is a set of a questionnaire used to evaluate the level and strength of ISC in the organization. The questionnaire items were originally developed by Martins and Eloff [63] based on Robbin's OB. These ISC models consist of three dimensions, namely *Organizational; Group*; and *Individual*. Each level has its own sub-dimensions, namely *Policy and Procedures; Risk Analysis; Benchmarking; Budget; Management; Trust; Awareness; Ethical Conduct*; and *Change* [63,64].

Da Veiga, Martins, and Eloff [122] further validated this questionnaire, customizing it based on a case study and introduced eight new dimensions: *ISP; Information Security Management; Information Security Program; Information Security Leadership; Information Asset Management; User Management; Change Management*; and *Trust*. Further validation of ISCA includes the development of information security governance framework (Da Veiga and Eloff [118]. This framework comprised of seven dimensions: *Leadership and Governance; Security Policies; Security Management and Organization; Security Program Management; User Security Management; Technology Protection and Operations*; and *Change Management*. These dimensions were used to develop an ISC framework by integrating Schein's OC [98] and Robbins's OB [110] in Da Veiga and Eloff [117]. The term *Information Security Culture Framework* (ISCF) was first coined in this study. ISCF is widely used in ISCA studies. The ISCA instruments of ISC concept based on Da Veiga and Eloff [117] and Da Veiga et al. [122] were used widely in subsequent studies by Da Veiga and Martins ([120,121]; and Martins and Da Veiga [65,67,68]. However, these studies did not use the same number and formation of dimension in their ISC conceptualization. Again, as shown in Table 1, the reason is due to the different additional concept used instead of the OB concept.

While the specific objective of a study has some influences towards the differences in dimensions used, interestingly, in regards to the ISCA-related studies, the authors explicitly mentioned that they customized the dimensions (constructs) used from one study to another in order to meet the specific type of organization under study [67,120,121]. Apparently, these authors suggested that the ISC concept based on dimensions is depends on the type of organization. This concept is not consistent with other authors, such as Chen et al. [19] and Parsons et al. [84] who used the same dimensions of ISC for all types of organizations in their studies.

In some ISCA studies, there is a lack of consistency in applying the dimensions of ISC concept for the organizations under study. In Da Veiga and Martins [120], the authors states that the differences of ISC dimensions are due to the maturity level of information security of each organization under study such as ISP implementation and other information security programs. On the other hand, the same authors in Martins and Da Veiga [66] have statistically proved that similar dimensions can be applied to international organizations operating in different countries, with different level of data protection maturity level. This suggests that similar ISC dimensions are applicable to the same type of organization but with varying levels of information security maturity. However, common ISC dimensions for organizations with different information security maturity levels were not listed. This scenario suggests that despite the numerous ISCA-related studies, which have produced validated assessment tools to measure and improve ISC of the organization under study, there is yet a consensus on the appropriate dimensions for ISC.

3.4. ISC model based on information security culture framework (ISCF)

ISCA has promoted the development of *Information Security Culture Framework* (ISCF). The first ISCF was discussed in Da Veiga and Eloff [117], based on the dimensions of *Information Security Governance* (Da Veiga and Eloff [118], *Organizational Culture* [98] and *Organizational Behavior* [110]. Recent studies by Alhogail [6], Alhogail [5], and Alhogail and Mirza [50] have developed and validated a comprehensive ISCF comprising of five dimensions: *Strategy, Technology, Organization, People*, and *Environment* (STOPE); and integrated with the *Change Management* and *Human Factor* in information security. This framework also utilized all levels of ISC (*Artifacts, Value, Belief* and *Information Security Knowledge*) based on the ISC model by Van Niekerk and Von Solms [77]. The adoption of different concepts and approaches in these studies has produced different dimensions of ISCF. This proves that although these studies have progressed from ISCA to ISCF, the dimensions of ISC still vary.

3.5. Other models

There are also other ISC models that were not developed based on certain theories or concepts, such as in Knapp et al. [53]; Alnatheer, Chan, and Nelson [13]; Shahibi et al. [104]; Alnatheer and Nelson [14]; Alnatheer [10]; Hassan and Ismail [45]; Dojkovski et al. [33]; and Dojkovski et al. [31]. These ISC models were developed based on literature analysis. Since most of the studies did not review the same articles, therefore the dimensions produced were also different. For examples, Sherif et al. [106] identified five dimensions from 25 selected articles whilst Tolah et al. [114] have identified 7 dimensions from 13 selected articles. Some studies combined both approaches of literature review and adopting a particular concept in ISC for example Knapp et al. [53]; Hassan et al. [44]; Martins and Da Veiga [65]; and Alfawaz et al. [2]. These studies also produced varied ISC dimensions as different concepts were used.

3.6. Extent of variances in ISC dimensions

The aforementioned discussion revealed that there are various formations of dimensions for modeling ISC. While the concepts adopted contribute to these variances, other factors such as objectives of the study; approach taken; type of organization under study; and the maturity level of the organization information security also play a role in ISC dimensions. Although some dimensions are consistently used such as *Policy and Top Management Commitment*, there are still a great number of variances in terms of the formations used.

Analyzing this matter in greater detail, we compare articles from one of the main research areas in ISC: the development and the application of ISCA. Table 2 illustrates the studies related to ISCA, extracted from Table 1. The left-most column is the dimensions used in these studies. Ticked cells indicate a particular dimension used in a particular study. It is apparent that some dimensions that consistently used based on the number of occurrences such as *Security Policy, Change Management, Leaderships and Governance*, and *Trust*. However, there are also 26 different dimen-

Table 2
ISC Dimensions in ISCA-related Studies.

No.	Dimensions	Studies							
		1	2	3	4	5,8	6	7	No. of Occurrences
1	Leadership and Governance		√	√	√	√	√		**5**
2	Security Management and Operations		√						**1**
3	Security Policies	√	√	√	√	√	√	√	**7**
4	Security Program Management		√	√					**2**
5	Information Security Program				√	√	√		**3**
6	User Security Management		√	√	√	√	√		**5**
7	Technology Protection and Operations		√						**1**
8	Change Management	√	√	√	√	√	√		**6**
9	Information Asset Management			√	√	√	√	√	**5**
10	Information Security Management			√	√	√	√		**4**
11	Trust	√		√	√	√	√		**5**
12	Awareness	√							**1**
13	Training and Awareness				√	√			**2**
14	Privacy Perception				√				**1**
15	Risk Analysis	√							**1**
16	Benchmarking	√							**1**
17	Budget	√							**1**
18	Management	√							**1**
19	Ethical Conduct	√							**1**
20	Information Security Commitment							√	**1**
21	Information Security Importance							√	**1**
22	Information Security Directives							√	**1**
23	Information Security Responsibility							√	**1**
24	Information Security Monitoring Perception							√	**1**
25	Information Security Consequences							√	**1**
26	Information Security Necessity							√	**1**
NUMBER OF DIMENSIONS IN A STUDY		**9**	**7**	**8**	**10**	**9**	**8**	**9**	

Study 1 = Martins and Eloff [63,64], 2 = Da Veiga and Eloff [117], 3 = Da Veiga et al. [122], 4 = Da Veiga and Martins [121]; Martins and Da Veiga [68], 5 = Da Veiga and Martins [120], 6 = Martins and Da Veiga [68], 7 = Martins and Da Veiga [116], 8 = Martins and Veiga [116].

sions with different formations used, which is a far too greater number to be used in the conceptualization of a construct.

There is also the issue of consistency (of dimensions) used throughout these studies. Some dimensions have different meanings although similar terms were used for example the dimension of *Trust*. In Martins and Eloff [64] and Da Veiga et al. [122], Trust is defined as the "level of trust between employees and managers", whereas, in Da Veiga and Martins [121] and Martins and Da Veiga [68], it is defined as the "perceptions of users regarding the safekeeping of private information and their trust in the communications of the organization". In addition, consistency of the term used for dimensions are lacking for example *Security Management and Operations* in Da Veiga and Eloff [117], *Security Management and Organization* in Da Veiga and Eloff [118], although both are referring to the same dimension. Tang et al. [111] highlighted the issue of consistency by arguing the definition of ISC used.

There were also instances where the dimensions were changed after the process of factor and reliability analysis were performed as a method to validate the dimensions for the ISC construct in a particular study. For example the initial eight dimensions in Da Veiga et al. [122] became six new dimensions; and ten initial dimensions in Martins and Da Veiga [68] became six. This contributes to variances in ISC dimensions as well as highlighting the lack of common dimensions for ISC.

Martins and Da Veiga [116] formulated and validated new dimensions for ISC using a complex statistical technique, the *Structural Equation Modeling* (SEM), resulting in *Management, Policies, Awareness*, and *Compliance*. Although these new dimensions are similar to the dimensions used in ISCA, they actually are using a whole new set of sub-dimensions that totally different from the previous sub-dimensions in ICSA studies as shown in Table 2. This would suggest that despite the capability of the assessment tools in ISCA to evaluate and improve ISC, there is still a lack of common dimensions for ISC concept in the literature.

4. Discussion and implication

This work highlights the variances of dimensions used to conceptualize ISC found in literature. It has also categorized major dimensions for ISC based on the underlying concepts. While different concepts contribute to variances in ISC dimensions, other contributing factors were also identified in this work including objective of the study; approach of the study; type of organization under study; and the organization's information security maturity level. As the ISC concepts and dimensions are still evolving, the findings of this work would pave the way for future studies in this area.

Our analysis revealed that the concepts of *Organizational Culture* (OC) dominated the conceptualization of ISC, concurring with previous findings by Alnatheer and Nelson [14]; Reid et al., [92]; and Schlienger and Teufel [101] that promotes ISC is a sub-culture of OC. Of the two main concepts of OC, which are Schein [99] and Detert et al. [28], the former was found to be widely adopted [19,66,73,100,102,120]**.** This is consistent with Pevchikh [85] that found most of the ISC concepts or model are influenced by Schein's OC in one way or another; and Kolkowska [55] who argued OC has been successfully used to conceptualize ISC in many ISC-related studies. In addition, the level approach in the Schein's model has made the conceptualization and assessment of ISC more transparent and comprehensive [77,78,81,100].

This review also reveals at least 26 major ISC dimensions from ISCA-related studies. These dimensions are different in terms of number, formation, and definition in conceptualizing ISC. We also found different terms were used to refer to the same dimension and the indication that dimensions were changed after factor and reliability analysis were carried out. This suggests that there is no widely accepted dimensions for ISC and it is still an evolving area as argued by Kolkowska [55], that the differences in dimensions is an indication that the understanding of security culture is still

evolving. As such, there is yet a comprehensive ISC dimensions that is applicable to all types of organization.

The lack of common dimensions is a big gap in ISC research since academicians and practitioners alike do not have access to a standard ISC reference model. This, in turn, would restrict the findings of ISC-related studies for further generalization and application. For example, Tang et al. [111] found a causal relationship between the dimensions in OC and the dimensions in ISC. However, due to the issue of consistency in dimensions, these findings are restricted as there might be some additional ISC dimensions that could be considered.

The inconsistency of dimensions in ISC concept also affects the applicability of ISC findings. For example, D'Arcy and Greene [25] found that security culture has a significant impact on employees ISP compliance intention, but this findings could not be applied to the whole ISC concept since only three dimensions were used: *Top Management Commitment, Security Communications* and *Computer Monitoring*. This is similar to Alkalbani et al. [9] who found that ISC has a significant impact towards employee's compliance using a different set of ISC dimensions. Since different dimensions were used, the findings could not be generalized to the whole ISC concept. Although the findings could complement each other in identifying applicable ISC dimensions, a more comprehensive study is needed for a wider generalization and application.

4.1. Practical implication

Despite the recommendations made by scholars that a positive ISC would guide and improve information security behavior, there is still a lack of solid guideline that could be used by practitioners to cultivate and assess ISC in their organization. Although there are various ISC models that can be utilized for an effective ISC, practitioners face the uphill task of identifying and selecting suitable ISC aspects for their organization. In deciding the most suitable dimensions of ISC for an organization, practitioners should take into account the cultural aspects of the organization. This is due to the fact that the concepts of organizational culture (OC) are widely used to conceptualize ISC, as reflected in this review. OC directly influences ISC and ISC is a subculture of OC [14,92,101]. For example, the enforcement and development of information security policy require support from OC [20]. In addition, the organizations should have a culture that makes it clear that security is important [23]. A recent study by Connolly et al. [22] found that OC would influence employees' security behavior. As such, the cultivation of positive ISC should coexist with the OC.

5. Limitations

Being a review, this work bears the limitations of rigorousness of the literature search. We have adhered to the PRISMA method, in terms of literature search and documentation. After systematically conducting the literature search twice, we strongly believe that even if any articles were left out, our findings would hold the same. This is due to the great number of ISC dimensions found in the literature.

6. Conclusion and future work

This work has revealed that various concepts are used to conceptualize ISC with organizational culture [97,99] being the most adopted concept. The use of different concepts and approaches led to the variances in ISC dimensions. There are numerous dimensions found in literature causing issues in the generalization and application of ISC-related studies. This study proved that while there is still no mutual agreement in conceptualizing the ISC, there is also no common agreement on the most comprehensive dimensions of ISC concept that could be referred by academician and practitioners. The concepts used in a particular study would hold true only to the study itself and could not be generalized to ISC as a whole. We firmly believe that future directions in ISC-related studies should attempt to address this issue for formulating and validating a standard ISC concept that is applicable to every organization. As each organization has a different level of ISC, a common set of dimensions would enable a more comprehensive and meaningful comparison to be made. This will lead to better ISC planning and strategies.

Acknowledgment

This research is funded by Universiti Malaysia Pahang under the Post Graduate Research Grant Scheme (PGRS170303).

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.jisa.2018.11.003.

References

[1] Al-Mayahi I, Mansoor SP. Information security culture assessment: case study. In: Third international conference on information science and technology (ICIST).; 2013. p. 789–92. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6747661.
[2] Alfawaz S, Nelson K, Mohannak K. Information security culture: a behaviour compliance conceptual framework. In: Conferences in Research and Practice in Information Technology Series, 105; 2010. p. 47–55.
[3] Alfawaz SM. Information security management: a case study of an information security culture. Queensland University of Technology; 2011.
[4] Alharbi N. The role of security and its antecedents in E-Government adoption. Plymouth University; 2017.
[5] Alhogail, A., 2015a. Cultivating and assessing organizational information security culture, an empirical study., 9(7), pp. 163–178.
[6] Alhogail A. Design and validation of information security culture framework. Comput Hum Behav 2015;49(August 2015):567–75.
[7] Alhogail A, Mirza A. A proposal of an organizational information security culture framework. In: Proceedings of International Conference on Information, Communication Technology and System (ICTS) 2014; 2014. p. 243–50. Available at: http://ieeexplore.ieee.org/document/7010591/.
[8] Alhogail A, Mirza A. Information Security Culture: A Definition and a Literature review. In: Computer applications and information systems (WCCCAIS); 2014. p. 1–7.
[9] Alkalbani A, Deng H, Kam B. Organisational security culture and information security compliance for e-government development: the moderating effect of social pressure. Pacific asia conference on information system (PACIS 2015); 2015.
[10] Alnatheer MA. A conceptual model to understand information security culture. Int J Social Sci Humanity 2014;4(2):104–7.
[11] Alnatheer MA. Information Security Culture Critical Success Factors. In: 2015 12th international conference on information technology - new generations; 2015. p. 731–5.
[12] Alnatheer MA. Understanding and measuring information security culture in developing countries : case of saudi arabia. Queensland University of Technology; 2012.
[13] Alnatheer M, Chan T, Nelson K. Understanding and measuring information security culture. In: Pacific Asia conference on information systems (PACIS); 2012. p. 1–15.
[14] Alnatheer M, Nelson K. Proposed framework for understanding information security culture and practices in the Saudi context. In: Australian Information Security Management Conference (December); 2009. p. 6–17.
[15] Baggett WO. Creating a culture of security. Internal Auditor 2003;60(3):37–41.
[16] Bakry SH. Development of security policies for private networks. Int J Network Manage 2003;13(3):203–10. Available at: http://doi.wiley.com/10.1002/nem.472 [Accessed February 14, 2017].
[17] Budgen D, Brereton P. Performing systematic literature reviews in software engineering. In: Proceedings of the 28th International Conference on Software Engineering (ICSE '06); 2006. p. 1051–2.
[18] Cárdenas-Solano L-J, Martínez-Ardila H, Becerra-Ardila L-E. Gestión de seguridad de la información: revisión bibliográfica/ Information security management: A bibliographic review. El profesional de la información 2016;25(6):931–48. Available at: http://www.elprofesionaldelainformacion.com/contenidos/2016/nov/10.html.
[19] Chen YAN, Ramamurthy KRAM, Wen K. Impacts of Comprehensive Information Security Programs on Information Security Culture. J Comput Inf Syst 2015;55(3):11–19.

[20] Chia PA, Maynard SB, Ruighaver A. Exploring organisational security culture: developing a comprehensive research model. In: Sixth Pacific Asia Conference on Information Systems; 2002. p. 1–11.
[21] Chia PA, Maynard SB, Ruighaver AB. Understanding organisational security culture. In: Sixth Pacific Asia Conference on Information Systems; 2002. p. 335–65.
[22] Connolly LY, et al. Organisational culture, procedural countermeasures, and employee security behaviour a qualitative study. Inf Comput Secur 2017;25(2):118–36.
[23] Connolly PJ. Security starts from within. InfoWorld 2000;22(28):39. Available at: http://search.ebscohost.com/login.aspx?direct=true&db=afh&AN=3463962&site=ehost-live.
[24] Consedine NS, et al. Beyond the black box: a systematic review of breast, prostate, colorectal, and cervical screening among native and immigrant African-descent Caribbean Populations. J Immigrant Minority Health 2015;17(3):905–24.
[25] D'Arcy J, Greene G. Security culture and the employment relationship as drivers of employees' security compliance. Inf Manage Comput Secur 2014;22(5):474–89.
[26] D'Arcy J, Greene G. The multifaceted nature of security culture and its influence on end user behavior. In: Proceedings of IFIP TC8 International workshop on information systems security research; 2009. p. 145–57.
[27] Dervin L, Kruger H, Steyn T. 'Value-focused assessment of information communication and technology security awareness in an academic enviornment', Security and Privacy in Dynamic Environments. IFIP International Federation for Information Processing, 201; 2006. p. 448–53.
[28] Detert JR, Schroeder RG, Mauriel JJ. A framework improvement for linking culture and in initiatives organization. Acad Manage Rev 2000;25(4):850–63.
[29] Dhillon G, Syed R, Pedron C. Interpreting information security culture : an organizational transformation case study. Comput Secur 2016;56:63–9. Available at: http://dx.doi.org/10.1016/j.cose.2015.10.001.
[30] Dojkovski S, Lichtenstein S, Warren M. Developing information security culture in small and medium size enterprises: Australian case studies. In: Proceedings of the 6th European conference on information warfare and security; 2007. p. 55–65.
[31] Dojkovski S, Lichtenstein S, Warren M. Fostering information security culture in small and medium size enterprises: an interpretive study in Australia. In: Proceedings of the Fifteenth European Conference on Information Systems; 2007. p. 1560–71.
[32] Dojkovski S, Lichtenstein S, Warren MJ. Challenges in fostering an information security culture in Australian small and medium sized enterprises. In: Proceedings of the 5th European conference on information warfare and security; 2006. p. 31–40.
[33] Dojkovski S, Lichtenstein S, Warren MJ. Enabling information security culture: influences and challenges for Australian SMEs. In: 21st Australasian conference on information systems; 2010. p. 61.
[34] Dojkovski S, Warren M, Lichtenstein S. Information security culture in small and medium sized enterprises: a socio-cultural framework. In: Protecting the Australian homeland : conference proceedings of [the] 6th Australian information warfare & security conference; 2005. p. 263.
[35] Fagade T, Tryfonas T. Security by compliance? A study of insider threat implications for Nigerian banks. In: 4th International conference on human aspects of information security, privacy, and trust, HAS 2016; 2017. p. 128–39. Available at: http://link.springer.com/10.1007/978-3-319-58460-7.
[36] Frederick Van Niekerk J. Establishing an information security culture in Organizations: an outcomes based education approach. Nelson Mandela Metropolitan University; 2005.
[37] Glaspie HW, Karwowski W. Human factors in information security culture: a literature review. In: Advances in intelligent systems and computing; 2018. p. 269–80. Available at.
[38] Greig, A., Renaud, K. and Flowerday, S., 2015. An ethnographic study to assess the enactment of information security culture in a retail store., pp. 61–66.
[39] Guldenmund F. The nature of safety culture: a review of theory and research. Saf Sci 2000;34(1–3):215–57. Available at: http://www.sciencedirect.com/science/article/pii/S092575350000014X.
[40] Habermas J. The theory of communicative action, vol 1: reason and the rationalization of society, Boston: Beacon Press; 1984. Translated by Thomas Mccarthy.
[41] Habermas J. The theory of communicative action, vol 2: lifeworld and system: a critique of functionalist Reason, Boston: Beacon Press; 1989. Translated by Thomas Mccarty.
[42] Hall ET. Beyond culture. Contemp Sociol 1976;7:298.
[43] Hall ET. The silent language. In: The silent language; 1959. p. 73–6.
[44] Hassan, N.H. et al., 2017. Information security culture in health informatics environment : a qualitative approach.
[45] Hassan NH, Ismail Z. A conceptual model for investigating factors influencing information security culture in healthcare environment. Procedia 2012;65(ICIBSoS):1007–12. Available at: http://www.sciencedirect.com/science/article/pii/S1877042812052196.
[46] Hassan NH, Ismail Z. Information security culture in healthcare informatics: a preliminary investigation. J Theor Appl Inf Technol 2016;88(2):202–9.
[47] Helokunnas T, Kuusito R. Information security culture in a value net. In: IEMC '03 Proceedings. managing technologically driven organizations: the human side of innovation and change; 2003. p. 190–4.
[48] Hofstede G, Neuijen B, Ohayv DD. Measuring organizational cultures: a qualitative and quantitative study across twenty cases. Adm Sci Q 1990;35(2):286–316.
[49] Hofstede GH. Culture's consequences, 2nd ed: Comparing values, behaviors, institutions and organizations across nations. Thousand Oaks: Sage Publications, Inc; 2001. p. 924–31. Edn.
[50] Alhogail A, Mirza A. Organizational information security culture assessment. In: International conference on security and management; 2015. p. 286–92.
[51] Hughes-Morley A, et al. Factors affecting recruitment into depression trials: systematic review, meta-synthesis and conceptual framework. J Affect Disord 2015;172:274–90.
[52] Karlsson F, Astrom J, Karlsson M. Information security culture – state-of-the-art review between 2000 and 2013. Inf Comput Security 2015;23(3):246–85.
[53] Knapp KJ, et al. Information security: management's effect on culture and policy. Inf Manage Comput Security 2006;14(1):24–36.
[54] Koh K, Ruighaver A, Maynard S, Ahmad A. Security governance : its impact on security Culture. In: Proceedings of the third australian information security management conference; 2005. p. 1–12.
[55] Kolkowska, E., 2011. Security subcultures in an organization - exploring value conflicts.
[56] Kraemer S, Carayon P. Computer and information security culture: findings from two studies. In: Proceedings of the human factors and ergonomics society annual meeting, 49; 2005. p. 1483–8.
[57] Kuusisto R, Nyberg K, Virtanen T. Unite Security culture may a unified security culture be plausible ?. In: Proc. of the 3rd European conference on information welfare and security; 2004. p. 221–36.
[58] Liberati A, et al. The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. Ann Intern Med 2009;151(4):W65–94.
[59] Lim JJS, et al. Embedding information security culture emerging concerns and challenges. In: Pacis 2010; 2010. p. 463–74.
[60] Lim JS, et al. Exploring the relationship between organizational culture and information security culture. In: 7th Australian information security management conference; 2009. p. 88–97.
[61] Lopes I, Oliveira P. Understanding information security culture: a survey in small and medium sized enterprises. New Perspect Inf Syst 2014;1(275):277–86.
[62] Mahfuth A, Yussof S, Baker A, Ali N. A systematic literature review: information security culture. In: 2017 International conference on research and innovation in information systems (ICRIIS); 2017. p. 1–6. Available at: http://ieeexplore.ieee.org/document/8002442/ [Accessed October 2, 2017].
[63] Martins A, Eloff J. Assessing information security culture. In: Proceedings of the ISSA 2002 information for security for South-Africa 2nd annual conference, 10–12 July 2002; 2002. p. 1–14.
[64] Martins A, Eloff J. Information security culture. Security Inf Soc 2002;86(April):203–14. Available at: https://link.springer.com/content/pdf/10.1007/978-0-387-35586-3_16.pdf [Accessed July 31, 2017].
[65] Martins, N. and Da Veiga, A., 2015a. An information security culture model validated with structural equation modelling., (Haisa), pp. 11–21.
[66] Martins N, Da Veiga A. Factorial invariance of an information security culture assessment instrument for multinational organisations with operations across data protection jurisdictions. J Govern Regul 2015;4(4):47–58.
[67] Martins N, Da Veiga A. Information security culture : a comparative analysis of four assessments. In: European conference on information management & evaluation; 2014. p. 49–58.
[68] Martins N, Da Veiga A. The value of using a validated information security culture assessment instrument. In: Proceedings of the 8th European conference on information management and evaluation, ECIME 2014; 2014. p. 146–54.
[69] Masrek MN. Assessing information security culture : the case of Malaysia Public Organization. In: Proc. of 2017 4th int. conf. on information tech., computer, and electrical engineering (ICITACEE), Oct 18–19, 2017, Semarang, Indonesia Assessing; 2017. p. 5386.
[70] Mazhelis O, Isomäki H. Information security culture: a survey. In: Proceedings of eight international network conference; 2010. p. 153–8.
[71] Mcintosh B. An ethnographic investigation of the assimilation of new organizational members into an information security culture. Nova Southeastern University; 2011.
[72] Moher D, et al. Preferred reporting items for systematic reviews and meta–analyses: the PRISMA statement. Ann Intern Med 2009;151:264–9.
[73] Nasir A, Arshah RA, Hamid MRA. Information security policy compliance behavior based on comprehensive dimensions of information security culture: A conceptual framework. In: 2017 International conference on information system and data mining; 2017. p. 56–60.
[74] Nenad R. Parliamentary control of security information agency in terms of security culture: State and problems. Zbornik radova Pravnog fakulteta, Novi Sad 2013;47(3):475–92. Available at: http://scindeks.ceon.rs/Article.aspx?artid=0550-21791303475R [Accessed July 17, 2017].
[75] Niekerk, J. Van and Solms, R. Von, 2005. A holistic framework for the fostering of an information security sub-culture in organizations. Issa, pp. 1–13.
[76] Niekerk JVan, Von Solms R. A theory based approach to information security culture change. Information (Japan) 2013;16(6B):3907–30.
[77] Niekerk JVan, Solms RVon. Information security culture: a management perspective. Comput Security 2010;29(4):476–86 Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167404809001126.

[78] Niekerk JVan, Solms RVon. Understanding information security culture: a conceptual framework. In: Proceedings of ISSA 2006; 2006. p. 1–10.
[79] Noorman Masrek M, Nazrin Harun Q, Khairulnizan Zaini M. Information security culture for Malaysian Public Organization: a conceptual framework. In: Proceedings of INTCESS 2017 4th international conference on education and social sciences; 2017. p. 156–66.
[80] OECD Available at: http://www.oecd.org/internet/ieconomy/15582260.pdf .
[81] Okere, I., van Niekerk, J. and Carroll, M., 2012. Assessing information security culture: a critical analysis of current approaches. 2012 Information Security for South Africa.
[82] Parsons J. An information model based on classification theory. Manage Sci 1996;42(10):1437–53 Available at: http://mansci.journal.informs.org/content/42/10/1437%5Cnhttp://mansci.journal.informs.org/content/42/10/1437.short.
[83] Parsons, K. et al., 2010. Human factors and information security: individual, culture and security environment,
[84] Parsons KM, et al. The influence of organizational information security culture on information security decision making. J Cognit Eng Decis Making 2015;9(2):117–29 Available at: http://edm.sagepub.com/content/9/2/117.short.
[85] Pevchikh EOR. Information security culture : definition, frameworks and assessment a systematic literature review. Luleå University of Technology; 2015.
[86] Pfeffer J, Sutton RI. The knowing-doing gap : how smart companies turn knowledge into action. Harvard Business School Press; 2000.
[87] Press I. OECD promotes culture of information security. Digest Electron Commer Policy Regul 2003;26:131–5 Available at: http://content.ebscohost.com.ezproxy.ump.edu.my/ContentServer.asp?T=P&P=AN&K=11917225&S=R&D=bth&EbscoContent=dGJyMNLe80SeqK840dvuOLCmr0%2Bep69Srqe4SraWxWXS&ContentCustomer=dGJyMOzprkiwqq9LuePfgeyx44Dt6flA [Accessed September 21, 2017].
[88] Ramachandran S, et al. Variations in information security cultures across professions: a qualitative study. Commun Assoc Inf Syst 2013;33(11):163–204.
[89] Ramachandran, S. and Rao, S. V, 2006. Security cultures in organizations : a theoretical model., pp. 3460–3464.
[90] Ramachandran S, Rao SV, Goles T. Information security cultures of four professions: a comparative study. In: Proceedings of the annual Hawaii international conference on system sciences; 2008.
[91] Reid R, Van Niekerk J. From information security to cyber security cultures. In: 2014 Information security for South Africa - Proceedings of the ISSA 2014 conference; 2014.
[92] Reid R, Van Niekerk J, Renaud K. Information security culture: a general living systems theory perspective. In: 2014 Information security for South Africa; 2014. p. 1–8. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6950493%5Cnhttp://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6950493.
[93] Robbins, S.P., Odendaal, A. & Roodt, G., 2003. Organisational behaviour : global and Southern African perspectives., pp. 379–400.
[94] Rühli E. Unternehmungskultur - Konzepte und Methoden. In: Rühli E, Keller A, editors. Kulturmanagement in schweizerischen Industrieunternehmungen. Bern und Stuttgart: Paul Haupt Verlag; 1991. p. 11–49.
[95] Ruighaver AB, Maynard SB. 'Organisational security culture: More than just an end user phenomenon', Security and Privacy in Dynamic Environments. IFIP International Federation for Information Processing, 201; 2006. p. 425–30.
[96] Ruighaver AB, Maynard SB, Chang S. Organisational security culture: extending the end-user perspective. Comput Security 2007;26(1):56–62.
[97] Schein EH. Organizational culture and leadership. Wiley; 1992.
[98] Schein EH. Organizational culture and leadership: a dynamic view. Organiz Stud 1985;7:199–201.
[99] Schein EH. The corporate culture survival guide. Jossey-Bass Inc; 1999.
[100] Schlienger T, Teufel S. Analyzing information security culture: Increased trust by an appropriate information security culture. In: Proceedings - international workshop on database and expert systems applications, DEXA; 2003. p. 405–9. 2003–Janua.
[101] Schlienger T, Teufel S. Information security culture: from analysis to change. South Afr Comput J 2003;31:46–52.
[102] Schlienger T, Teufel S. Information security culture - the socio-cultural dimension in information security management. In: Security in the information society: visions and perspectives. IFIP TC11 international conference on information security (Sec2002); 2002. p. 191–201.
[103] Schlienger T, Teufel S. 'Tool supported management of information security culture'. In: Paper presented at 20th IFIP International Information Security Conference, Makuhari - Messe, Chiba, Japan; 2005.
[104] Shahibi, M.S., Fakeh, R.M.R.S.K.W. and Ali, W.A.K.W.D.J., 2012. Determining factors influencing information security culture among ICT librarians., 37(1), pp. 132–140.
[105] Sherif E, Furnell S. A conceptual model for cultivating an information security culture. Int J Inf Security Res 2015;5(2):565–73.
[106] Sherif E, Furnell S, Clarke NL. An identification of variables influencing the establishment of information security culture. In: 3rd international conference on human aspects of information security, privacy and trust, HAS 2015; 2015. p. 436–48. Available at: http://link.springer.com/10.1007/978-3-319-20376-8.
[107] Siponen MT. A conceptual foundation for organizational information security awareness. Inf Manage Comput Secur 2000;8(1):31–41 Available at: http://www.emeraldinsight.com/doi/10.1108/09685220010371394.
[108] Smith EE, Medin DL. Categories and concepts. Cognit Sci Ser 1981;4:203 Available at: http://www.cs.indiana.edu/~port/teach/sem08/Smith.Medin.1983.ch1.2.3.pdf.
[109] Standard, I., 2005. International Standard ISO / IEC,
[110] Robbins Stephen P. Organizational behavior. 9th ed. Prentice Hall International, Inc; 2001.
[111] Tang M, Li M, Zhang T. The impacts of organizational culture on information security culture: a case study Available at: https://link.springer.com.ezproxy.ump.edu.my/content/pdf/10.1007%2Fs10799-015-0252-2.pdf. [Accessed July 17, 2017] .
[112] Tejay G, Dhillon G. Developing Measures of Information Security. The fourth annual workshop on e-business Las Vegas, NV; 2005.
[113] Temesgen G, Lessa, Ferede L. Information security culture in public hospitals : the case of Hawassa referral hospital. Afr J Inf Syst 2011;3(3).
[114] Tolah, A., Furnell, S.M. and Papadaki, M., 2017. A comprehensive framework for cultivating and assessing information security culture., (Haisa), pp. 52–64.
[115] Da Veiga A. Cultivating and assessing information security culture. University of Pretoria; 2008.
[116] Da Veiga A. An Information Security Training and Awareness Approach (ISTAAP) to Instil an information security- positive culture an Information Security Training and Awareness Approach (ISTAAP) to Instil an information security- positive culture. In: Human aspects of information security & assurance (HAISA 2015); 2015. p. 95–107.
[117] Da Veiga A, Eloff JHP. A framework and assessment instrument for information security culture. Comput Secur 2010;29(2):196–207 Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167404809000923.
[118] Da Veiga A, Eloff JHP. An information security governance framework. Inf Syst Manage 2007;24(May):361–72.
[119] Da Veiga A, Martins N. Defining and identifying dominant information security cultures and subcultures. Comput Secur 2017;70:72–94 Available at: http://ac.elscdn.com.ezproxy.ump.edu.my/S0167404817300937/1-s2.0-S0167404817300937-main.pdf?_tid=40d90cc0-7cb3-11e7-8cdb-00000aab0f26&acdnat=1502249678_84da0f3696bfbb37a1ea9a378d1be744 [Accessed June 14, 2017].
[120] Da Veiga A, Martins N. Improving the information security culture through monitoring and implementation actions illustrated through a case study. Comput Secur 2015;49:162–76.
[121] Da Veiga A, Martins N. Information security culture and information protection culture: a validated assessment instrument. Comput Law Secur Rev 2015;31(2):243–56 Available at: http://www.sciencedirect.com/science/article/pii/S0267364915000060 [Accessed August 9, 2017].
[122] De Veiga, A., Martins, N. and Eloff, J.H.P., 2007. Information security culture – validation of an assessment instrument., 11(1).
[123] Von Solms B. Information security the fourth wave. Comput Secur 2006;25:165–8.
[124] Werlinger R, Hawkey K, Beznosov K. An integrated view of human, organizational, and technological challenges of IT security management. Inf Manage Comput Secur 2009;17(1):4–19 Available at: http://www.emeraldinsight.com/doi/10.1108/09685220910944722.
[125] Williams PAH. Capturing culture in medical information security research. Methodol Innovations Online 2009;4(3):15–26.
[126] Zakaria O. 'Internalisation of information security culture amongst employees through basis security knowledge', Security and Privacy in Dynamic Environments. IFIP International Federation for Information Processing, 201; 2006. p. 437–41.