Journal of Fundamental and Applied Sciences

Research Article

ISSN 1112-9867

Available online at http://www.jfas.info

INFORMATION SECURITY CULTURE GUIDELINES TO IMPROVE EMPLOYEE'S SECURITY BEHAVIOR: A REVIEW OF EMPIRICAL STUDIES

N. Akhyari[1,*], A. A. Ruzaini[2] and A. H. Rashid[3]

[1]Faculty of Computer, Media and Technology Management, TATI University College, 24000 Kemaman, Terengganu, Malaysia

[2]Faculty of Computer Systems and Software Engineering, Universiti Malaysia Pahang, 26300 Kuantan, Pahang, Malaysia

[3]Faculty of Industrial Management, Universiti Malaysia Pahang, 26300 Kuantan, Pahang, Malaysia

Published online: 01 February 2018

ABSTRACT

This paper reviews Information Security Culture (ISC) studies published in six leading databases from year 2000 until 2016 to investigate empirical findings that could support the relationship between ISC and employee's security behavior as well as to identify the findings that could be applied as guidelines to cultivate ISC in the organization. This review discovered that there is lack of comprehensive empirical studies have been done to provide sufficient empirical findings in supporting the relationship between ISC and security behavior. The approaches of the studies in terms of conceptualization and operationalization of ISC concept also limit the applicability of the findings to be used as the guidelines for ISC cultivation. This paper provides clear justifications on these issues and indicated a clear direction on the future of ISC research to be taken.

Keywords: information security culture; information security policy compliance behavior; security behavior.

Author Correspondence, e-mail: akhyari@tatiuc.edu.my

doi: http://dx.doi.org/10.4314/jfas.v10i2s.21

Journal of Fundamental and Applied Sciences is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License. Libraries Resource Directory. We are listed under Research Associations category.

1. INTRODUCTION

In organizational context, it was widely accepted that employees are the weakest link in information security chain [1-2]. Most of the time, this is because of their security behavior when dealing with information assets [2-6]. For this reason, information security scholars have recommended practitioners to establish a positive Information Security Culture (ISC) to influence employee's information security behavior so that their behavior will improve and in turn will minimize information security breaches [7-8]. In [9] has defined security behavior as a set of core information security activities that have to be adhered by end-users to maintain information security as defined by Information Security Policy (ISP). From this perspective, the implementation of ISC would influence and improve employees' behavior towards compliance with ISP in the organization.

Despite this strong recommendation by the scholars, it is still unclear regarding guidelines available to establish ISC that will significantly influence employees' security behavior. Although there are some guidelines and standards available for establishing Information Security Management System (ISMS) such as BS 7799 or ISO/IEC 27001 [10] and OECD [11], however these guidelines are not focusing on ISC and there is no proof on its effectiveness in influencing employee's security behavior. Moreover, although there are quite number of ISC-related studies available in literature, there are still no clear and comprehensive empirical findings that could be used as solid ISC guidelines by the practitioners to be applied in their organization. The issue arises as to why so many studies have been conducted but there is still lack of findings that could be used as guidelines to cultivate an effective ISC strategy in the organization. Obviously, in producing the findings that could be used as references for ISC guidelines in influencing security behavior, the studies must provide empirical findings on the relationship between ISC and security behavior. At the same time, these studies must incorporate a clear approach in conceptualizing the ISC concept by using particular aspects or dimensions so that these dimensions could be used as aspects or elements in guidelines of ISC cultivation. In addressing these two main issues, therefore, this study reviews and analyses all ISC studies in literature to answers the two specific Research Questions (RQ) as follows:

RQ1: To what extent the available empirical findings are supporting the relationships between ISC and employee's security behavior?

RQ2: To what extent the available empirical findings are providing clear guideline or strategy in terms of aspects required to cultivate ISC in improving employee's security behavior?

The next section discusses the method and process used in this study followed by results and

analysis pertaining in answering the two RQs. The implications of the findings are discussed in Discussions section. This paper concludes the findings by summarizing the status and issues of current ISC studies and findings towards contributing to ISC guidelines.

2. METHODOLOGY

In general, this review followed reference process of systematic review approach as proposed by [12]. This process consists of seven phases as depicted in Table 1. In the first phase, we defined our two Research Questions (RQs) as discussed in the introduction section. These two RQs also become our scope of review and influenced our direction of activities undertaken. Based on the two RQs, this study requires the selection of articles that overlapped from two areas of literature, which are ISC and security behavior as depicted in Fig. 1. This is because we have to find and analyze the studies that specifically examined the relationship between ISC and security behavior. Therefore, in the second phase, in order to get more coverage of articles selection, we decided to do the searching process towards six leading databases in computing fields which include the Google scholar, IEEE/IEE Electronic Library, EBSCOhost, Elsevier Science Direct, ACM and Emerald Library.

Table 1. Phases of the reference process for a systematic review [12]

Phase	Output
1. Defining the research question	Research Question
2. Building the Infrastructure	Conceptual meta-model as a framework to represent the subject matter Classification system
3. Searching the literature	Preliminary inclusion of studies based on database research
4. Selecting the studies for inclusion	Set of final eligible studies
5. Assessing the quality of included studies and structuring of their results	Assessed and structured studies
6. Combining the results	Representation of the gained and integrated results
7. Create a structured report	Report on the findings and the evidence gained

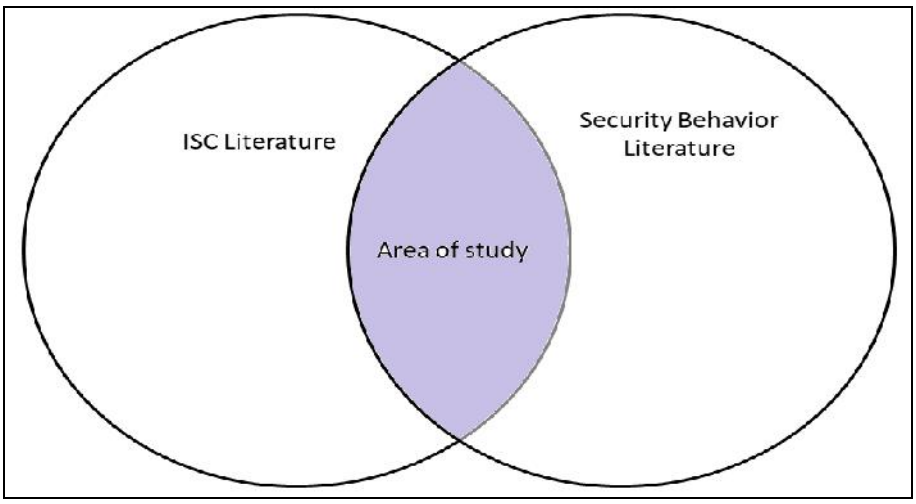

Fig.1. Area of study in which articles are selected from

In the third phase, we decided to start the searching by focusing on all ISC-related articles based on keywords of "Information Security Culture" and "Security Culture". Specifically, in this phase of literature search process, we also followed guidelines by [13] in order to establish the reliability and validity of this review. All key aspects and activities in searching the articles are recorded and described in this study. Besides using the six databases as mentioned above, we also performed forward and backward searches based on identified articles. Then, based on these ISC-related articles that we discovered, we narrow-down our search to select only ISC articles that have examined relationship with security behavior and other additional inclusion criteria. This was done by assessment on the title, abstract, and then by full-text evaluation. In summary, the inclusion criteria are as the following:

1. The article must be written in English
2. The article is peer reviewed and published in year 2000 until 2016
3. The article must reporting empirical findings on relationship between ISC and employee's security behavior in the organizational settings
4. The ISC concept used in the study must be clearly conceptualized and operationalized

The selected articles were analyzed accordingly to answer the two research questions for this review**.** The inclusion criteria of articles selection above also represent the fourth phase of our systematic review. All the selected papers and justifications of selection are discussed in the following sections.

In the fifth phase, the quality of selected articles is determined by the evidences provided by the articles in answering the two RQs. For RQ1, the articles must provide statistical evidence on the relationship between ISC and security behavior. In this study, the statistical results of selected studies in terms of path coefficient, β and Spearman Correlation, r as these values are

representing the relationship between ISC and security behavior. As for RQ2, the articles selected also must clearly define the ISC concept used in the study so that we could identify the type of construct particularly in terms of dimension of the construct. In ISC literature, generally there are two types of ISC construct. The first one is single-level construct. It is in the form of general aspect of ISC construct measured by several reflective indicators [14-15]. The second conceptualization approach treats ISC as multidimensional second-order construct [16-17].

From the perspective of our study, the second approach of conceptualization of multidimensional construct will provide more comprehensive findings especially in providing clearer aspects of ISC guidelines. Since these dimensions are representing distinct aspects of ISC used in the study, these dimensions also representing guidelines in terms of aspects to be used in cultivating ISC. For example in [17], the authors used dimensions of Top Management Commitment, Security Communications and Monitoring in representing ISC concept. They found out that these dimensions were significant in forming ISC concept and could be used as a guideline to cultivate ISC in an organization. On the other hand, the studies that did not using particular dimensions in representing their ISC concept could not provide clear and distinct aspects of ISC to be used as guidelines or strategies to cultivate ISC. Instead of using particular dimensions, the ISC concept in these studies are conceptualized and operationalized as reflective constructs measured by several interchangeably indicators that usually representing the same aspect of ISC. Therefore, the findings from these studies could only provide the findings on the relationship between ISC and security behavior but could not provide particular guidelines on how to cultivate ISC. All the detail discussions regarding these two RQs are presented in the later sections as these will represent the sixth phase of our systematic review process.

3. RESULTS AND ANALYSIS

The results of searching process based on the keywords from selected databases as well as forward and backward searches are presented in Table 2. Some articles are published in more than one database. One article which is [18] has been excluded from the study because we cannot find the English version of this article. The final number of articles available is 116. However, after full text reading and analysis based on inclusion criteria, only six articles met all the criteria to be used in this review. In specific, there are only 5% articles from 116 articles found in the searching process that empirically study the relationship between ISC and security behavior. The next subsections will investigate these issues in more detail based on

the RQs.

Table 2. Search results

Database	Articles
Ebscohost	[19-39], [3]
ACM	[20], [40-42]
Google Scholar	[3], [8], [38], [24-26], [18-19], [32], [28-30], [15], [17], [21], [40-106]
Science Direct	[30], [107], [14], [22], [25-26], [28-29], [92], [3], [38], [108], [32], [56]
Emerald	[97], [17], [68], [109-110]
IEEE Xplore	[7], [82], [64], [47], [44], [84], [111-124]
Forward search	[125]
Backward search	[16], [126-127]

3.1. RQ1

To answer this RQ, a detailed view of all empirical findings on the relationship between ISC and particular security behavior constructs need to be presented. This will provide a whole picture on the effect of ISC towards security behavior from current literature. Table 3 shows statistical findings on the relationships between ISC and particular constructs of security behavior in terms of path coefficient (β) and correlation coefficient (r) for all selected studies. It also shows the ISC concept based on dimension and particular aspects used for each dimension. The table shows that security behavior constructs consist of Attitude (ATT) and Normative Belief (NB), as well as the ultimate dependent variable of interest in the selected studies. Interestingly, despite strong recommendations from information security scholars that the cultivation of positive ISC will influence employees' security behavior in line with ISP, there is actually lack of empirical findings to confirm this relationship. As mentioned in previous section, there only 6 from 116 studies that specifically examine the relationship between ISC and security behavior. This is an indication that instead of widely recommendation of ISC establishment in guiding employee's security behavior, there is actually lack of findings available to be used as guidelines to cultivate an effective ISC.

According to Table 3, there are also some mixed findings have been produced by these six studies. Specifically, in [127] has found that there is non-significant relationship between ISC and Attitude as well as between ISC and Normative Belief in line with ISP violation. This finding also reported by [128] in their systematic literature review suggesting that security culture is a weak predictor towards dependent variables used in security behavior literature. The author in [127] has concluded that although an organization has strong ISC, the ISC

could not influence the employees in weakening their attitude and normative belief towards violating the ISP. This is because ISC concept used in his study is considered as a longer-term organizational issue that more commonly attributed to organizational culture. Consequently, according to the author, it has weaker influence compared to shorter-term organizational issues such as recent observations or experiences concerning information security in the workplace which may have stronger influence on employees' attitude and subjective norm towards intentional violations of ISP.

Table 3. Findings of relationships between ISC and security behavior constructs

Study	ISC Concept	Path Coefficient, β or Spearman Correlation, r between ISC and Particular Security Behavioral Constructs		
		Ultimate Dependent Variable	**ATT**	**NB**
[127]	Single-level Construct	NA	β = 0.019 NS	β = -0.015 NS
[16]	Multidimensional 1. TMC 2. COM	β = 0.552***	NA	NA
[17]	Multidimensional 1. TMC 2. COM 3. MON	β = 0.636**	NA	NA
[129]	Represented by 1. TMC 2. ACC 3. ISA	β= 0.18*** (TMC) β= 0.24*** (ACC) β= 0.18*** (ISA)	NA	NA
[15]	Single-level Construct	NA	r = 0.703	NA
[21]	Single-level Construct	NA	β = 0.24**	β = 0.46**

*p < 0.01 **p < 0.05 ***p < 0.001

NA – Not Applicable

Legend (ISC Dimension):

TMC – Top Management Commitment

COM – Security Communications

MON – Computer Monitoring

ACC – Accountability

ISA – Information Security Awareness

On the other hand, in [15] has found that organizational ISC has significant influence on employees' attitude towards policy and procedures. Unlike findings by [127], in [15] claimed that an organization that has better ISC is more likely will have better employees' attitude towards ISP. Obviously, these mixed findings could be justified by two different aspects between these two studies. First, study by [15] used attitude towards following ISP as the ultimate dependent variable whereas [127] used attitude towards ISP violation as his ultimate dependent variable of interest. In security behavior literature, these two dependent variables are opposite with each other and there are also differences in terms of theories and approaches used for these two dependent variables.

Second, besides using different ultimate dependent variable, these two studies also used different ISC construct in terms of conceptualization and operationalization. These differences are among common issues in ISC literature. There are always different concept of ISC used in literature [66] and there is also no agreement on how ISC should be conceptualized and operationalized because there is lack of validated approaches in this field [97]. The ISC concept in [15] was conceptualized by conducting literature review focusing on organizational culture by [130], organizational climate, rewards and punishment. In their study, the factors or dimensions influencing ISC are Sanctions, Rewards, Job Roles and Number of Employee. In contrast, study by [127] has used conceptualization and operationalization of ISC that originated from [46]. The ISC model or concept by [46] was originally developed from a mixed-mod (qualitative and quantitative) study of developing and testing a theoretical model to demonstrate the influence of top management support on ISC and level of security policy enforcement. Therefore, by using different approaches and theories, these two concept of ISC produced are also different. Moreover, in terms of operationalization, both studies used different items to measure the ISC construct. All these differences have produced different ISC concept, which in turn have influenced the results and findings in both studies.

Nevertheless, besides studies by [127, 15], there is lack of study that specifically examining the relationship between ISC and Attitude, Normative Belief as well as Self-Efficacy. Table 3 clearly shows that most of relationship between ISC and particular security behavioral factors such as Attitude, Normative Belief and Self-Efficacy are still not completely and

comprehensively examined. This indicated by the NA (Not Applicable) tag in the table. Ironically, most of the studies are investigating the direct impact of ISC towards employees' intention to comply such as by [16-17, 129] as shown in Table 3. While these studies have given useful findings to practitioners and academia, the impact of ISC towards the most significant behavioral factors of Attitude, Normative Belief and Self-Efficacy in security behavior literature were not comprehensively examined. In fact, these particular relationships should be investigated because these behavioral factors are proven to be the most significant factors of employees' security behavioral intention [132]. Furthermore, according to Theory of Planned Behavior (TPB), an individual intention towards a particular behavior is depending on his/her Attitude, Normative Belief and Self-Efficacy. Therefore, the findings on these particular relationships will provide more comprehensive knowledge and understanding on ISC effect towards security behavior and in turn will provide more convincing findings in confirming the actual influence of ISC towards security behavior.

The study by [21] is the only recent study that examined more comprehensive relationship between ISC and security behavior. Although they did not focusing only to the effect of ISC construct towards security behavior, their findings provided more comprehensive findings of relationship between ISC and employees security behavior compared to other studies. Specifically, they found that ISC has significant effect on Attitude and Normative Belief towards resisting social engineering. This knowledge is crucial in providing the comprehensive understanding on the influence of ISC towards security behavior especially from the context of Theory of Planned Behavior (TPB). Since security behavioral intention is depending on these three main TPB constructs of Attitude, Normative Belief and Self-Efficacy, the findings have provided additional knowledge on how significant the ISC influences these behavioral factors which in turn will influence their security behavioral intention. Additionally, in [21] also examined the mediation effect of three behavioral factors on the relationship between ISC and employee's security behavioral intention. These examination and findings are also important as they indicated the roles of three behavioral factors in influencing the relationship between ISC and employee's security behavioral intention.

Nevertheless, from the perspective of this review, instead of providing more comprehensive findings on the relationship between ISC and employee's security behavior, there are several limitations on the findings to conclusively support the relationship between ISC and employee's security behavior. First, the ultimate dependent variable used is quite different from commonly used in security behavior especially in ISP compliance behavior. In ISP

compliance behavior literature, the common used ultimate dependent variable are Intention to Comply, Attitude towards ISP Compliance, Actual ISP Compliance and Intention to ISP Violation [128, 132]. Second, there are still one behavioral factor of TPB still did not being examined in the study which is Self-Efficacy. Since TPB suggests that behavioral intention is determined by Attitude, Normative Belief and Self-Efficacy, these whole set of behavioral factors need to be examined to get more deep knowledge on the relationship between ISC and employee's security behavior.

Apart from study by [21, 127] also examined the effects of three security behavioral factors of Attitude, Normative Belief and Self-Efficacy towards the ultimate dependent variable of behavioural intention, Table 4 shows the relationships between these three behavioural factors towards an ultimate dependent variable in the selected studies. As depicted in the table, among six studies, there are only two studies examined these relationships, with [21] used intention to resist social engineering and [127] used intention to ISP violation as the ultimate dependent variable of interest. Consistent with security behavior literature, in general, both studies found significant relationship of these three behavioral factors towards employee's security behavioral intention. However, there are slightly different interesting findings to be noted. Among the three factors, Normative Belief is the strongest predictor in [127] whereas in [21] Normative Belief is the weakest. On the other hand, Attitude is the strongest predictor in [21] but weakest in [127]. Despite the opposite direction of ultimate dependent variable, another justification on this contradict findings could be explain by the differences of other constructs used in the model. Instead of using ISC, these two studies also used another different constructs in their models which in turn affected the regression results.

Table 4. Relationship between ATT, NB and SE towards an ultimate dependent variable of interest in selected studies

		Path Coefficient, β with Dependent Variable		
Study	**Ultimate Dependent Variable Used**	**ATT**	**NB**	**SE**
[127]	Intention to Violate ISP	β= 0.201*	β= 0.471**	β= 0.148**
[16]	Security Compliance	NA	NA	NA
[17]	ISP Compliance Intention	NA	NA	NA
[129]	Information Security Compliance	NA	NA	NA
[15]	Attitude towards Compliance	NA	NA	NA
[21]	Intention to Resist Social Engineering	β= 0.57**	β= 0.08**	β= 0.09**

*p < 0.01; **p < 0.05; ***p < 0.001

Analysis of findings on the relationship between ISC and particular constructs of security behaviour also could be explained by using R^2. Table 5 shows the R^2 values of endogenous constructs of all selected studies involving the relationships between ISC and Attitude, Normative Belief and Self-Efficacy as well as the ultimate dependent variables use in selected studies. In the table, the constructs that appear in the bracket represent the exogenous constructs involved in the regression. Since R^2 value is the variance of the endogenous constructs explained by the exogenous constructs, therefore different set of exogenous constructs will produce different regression results. The table clearly show that there is lack of solid findings on the actual effect of ISC towards security behavior in terms of Attitude, Normative Belief and Self-Efficacy and other dependent variables of security behavior. From the six selected studies, only two security behavioural constructs that have the absolute proportion of variance explained by the only ISC construct which are Normative Belief by [127, 21] and ultimate dependent variable of Security Compliance by [16]. This means that there are many more security behavior constructs that still not being examined its effect in relation with ISC. Besides that, the table also shows slightly mixed findings. The proportion of variance of ISC explained in Normative Belief in [127] is weak whereas it is more stronger in [21]. According to [133], the R^2 values of 0.26, 0.13 and 0.02 are considered as substantial, moderate and weak respectively. Moreover, from a wider perspective, these two findings are too little to conclude the actual effect of ISC towards security behavior. Referring to Table 5, it is clear that there are still several security behaviour constructs that not being exclusively explained by the ISC. Moreover, there are also obvious differences in dimensions used to conceptualize ISC in both studies which raised another issues of what is the most comprehensive dimension that could be used to conceptualize ISC.

As from theoretical perspective of TPB that Intention is predicted by Attitude, Normative Belief and Self-Efficacy, the current studies also could not provide strong empirical findings on these relationships. In Table 5, although studies by [127, 21] show the R^2 for ultimate dependent variables explained by the three behavioural factors, both ultimate dependent variables are not exactly the intention to comply with ISP. As depicted previously in Table 4, study by [127] used Intention to Violate and [21] used Intention to Resist Social Engineering. Although these two variables are basically represent intention which is consistent with TPB context, however the exact variable of ISP Compliance Intention will provide more clear findings as [9] defines that information security behaviour is a set of core information security activities that have to be adhered by end-users to maintain information security as defined by ISP. Furthermore, since ISC concept used in both studies are single-level construct, the findings

could not provide particular aspects of ISC cultivation. This issue will be discussed later in RQ2. Therefore, in answering RQ1, we conclude that there are still no solid empirical findings to explain the influence of ISC towards the three behavioral factors of TPB which in turn will explain how these factors will affect intention to comply.

Table 5. Coefficient of determination, R^2 of particular security behavioral constructs in selected studies

Study	Attitude (Exogenous Constructs Involved)	Normative Belief (Exogenous Constructs Involved)	Self-Efficacy (Exogenous Constructs Involved)	Ultimate Dependent Variable (Exogenous Constructs Involved)
[127]	0.228 (ISC, Perceived punishment certainty, Perceived punishment severity, Organizational commitment)	0.022 (ISC)	NA	0.417 (Attitude, Normative Belief, Self-Efficacy)
[16]	NA	NA	NA	0.31 (ISC)
[17]	NA	NA	NA	0.45 (ISC, Job Satisfaction, Perceived Organizational Support)
[129]	NA	NA	NA	0.48 (Top Management Commitment, Accountability, Information Security Awareness)
[15]	NA	NA	NA	NA
[21]	0.19 (ISC,	0.21(ISC)	0.24	0.42 (Attitude.

Information Security Awareness)	(Information Security Awareness)	Normative Belief, Self-Efficacy)

3.2. RQ2

As discussed in previous section, there are only six studies that empirically examined the relationship between ISC and security behavior. This number is decreased significantly when considering the findings that could be used as guidelines and strategies to cultivate ISC in the organization. This is because we believe that in order for ISC findings of a study to have the ability in providing guidelines especially in terms of aspects or elements to be applied in ISC cultivation, obviously the study must use particular dimensions in representing the ISC concept. This is because these dimensions are representing aspects or elements of ISC. For example, study by [17] used three dimensions which are Security Communication (COM), Top Management Commitment (TMC) and Computer Monitoring (MON) to represent the concept of ISC in their study. According to authors in [17], these three dimensions are representing information security efforts that could be done by practitioners in cultivating organizational ISC. Therefore, the findings from this type of study particularly the relationship of ISC based on particular dimensions towards ISC compliance behavior could be used as guidelines or strategies to establish ISC in the organization.

Unfortunately, there is lack of study that conceptualized ISC based on particular dimensions in examining the relationship of ISC towards security behavior. Referring back to Table 3, there are only three studies that fall into this category which are [16-17, 129]. Specifically, in conceptualizing the ISC concept, in [16] used two dimensions which are Top Management Commitment (TMC) and Security Communications (COM). In their next study [17], they used three dimensions by adding one more dimension which is Security Monitoring (MON) into the existing two. Ironically, in [129] has used three ISC dimensions which two of them are totally different with [17]. As depicted in Table 3, instead of using TMC as used in [16-17, 129] used two dimensions of Information Security Awareness (ISA) and Accountability (ACC) which are very different aspects of dimensions compared to [16-17]. While these additional and different dimensions has provided new insights on the concept of ISC, it also leads to a new issue in terms of determining the most comprehensive dimensions in representing ISC concept. Consequently, since these dimensions are representing information security aspects and guidelines on establishing ISC, this scenario has created some problems for practitioners in

selecting the most comprehensive guidelines to be applied in their organization. Moreover, there is still no mutual agreement on the definition, number and formation of dimensions that should be used to represent the ISC concept available in literature [83, 113]. Therefore, as conclusion for RQ2, all these arguments and issues suggest that there is still lack of clear and holistic guidelines of ISC cultivation in improving security behavior available in literature.

4. DISCUSSION AND IMPLICATIONS

Based on the two RQs, it is clearly shown that there is lack of guidelines available to be used by practitioners in establishing an effective ISC strategy in the organization. Despite strong suggestions by the scholars, there are actually very limited findings and empirical evidences on the relationship between ISC and the security behavior of employees in the organization. Although there are quite number of ISC-related studies have been conducted, only few studies have produced empirical findings that could be used as references to establish ISC. Unfortunately, these few studies also could not provide conclusive findings to confirm the relationship. As a result, there is still lack of comprehensive guidelines to be used by practitioners in cultivating effective ISC strategies in order to improve employees' security behavior in the organizations.

From the perspectives of this review, this issue is related to two aspects or approaches of ISC studies that have been conducted. The first aspect is due to the lack of studies that examine the comprehensive relationship between ISC and security behavior. There are many more important aspects of relationship between ISC and particular security behavior constructs that still not being examined. Moreover, these studies also did not incorporate and examine the relationship based on theoretical behavioral framework such as TPB. Since TPB is one of the most significant behavioral theory and factors in security behavior literature [128, 132], the findings on how ISC influence these behavioral factors or constructs of TPB will provide useful knowledge to academician especially practitioners as it shows the actual detail and complete ISC effect on particular employees security behavior. These knowledge are beneficial to practitioners in customizing ISC strategies to get the desired security behavior in terms of Attitude, Normative Belief, Self-Efficacy as well as their employees' intention towards security. Furthermore, since the ultimate objective of ISC is to guide employee's security behavior [28-29, 53], the approach of study that incorporated theoretical behavior will produce more deep understanding and richer explanation on the relationship between ISC and employee's security behavior.

As for the second aspect, it is regarding the approach used in conceptualizing the ISC

construct. There are very few studies that conceptualized and operationalized the ISC concept based on dimensions in the examination of its relationship towards security behavior. This fact is consistent with [115], which argued that ISC is always conceptualized as a single-level constructs in the literature. As discussed in RQ 2 section, the conceptualization and operationalization of ISC concept as multidimensional construct is important since the dimensions are actually representing the strategy and guidelines in terms of aspects to be used in establishing ISC in the organization. The best examples of ISC studies that used this approach are by [16-17]. By using this approach, the findings produced could be directly referred and used by the practitioners and academicians as clear guidelines for ISC establishment. As for the studies that did not use particular dimensions to represent ISC concept, their ISC concepts are in general forms without specifically defined each aspect of ISC. The ISC construct used in this type of study is usually is a reflective construct with several interchangeably items to measure only one aspect of general ISC definition such in [46, 15]. Consequently, this type of conceptualization could not provide findings that could be used as a clear guideline or strategy of ISC establishment. Therefore, there is a very demanding situation to conduct studies using the first approach so that more findings could be applied by the practitioners in assisting them to cultivate effective ISC strategies.

5. LIMITATION AND FUTURE WORKS

Although we believed that this review study has revealed some important issues and gaps in ISC literature, however there are some limitations that we want to highlight. Most of the concern of this type of study is relating to the rigorousness of searching process. Although we have followed guidelines and recommendations by [13] in searching and identifying articles from six selected databases, we believed that more databases should be included in order to make sure all articles that meet the criteria for this study have be considered. Nevertheless, the use of Google Scholar database has maximized the selection of important articles because this database contains all articles from various other databases, conferences and publishers.

Another limitation might be is in terms of analysis used in this study. Since the analysis in this review are done based on content analysis, more thorough analysis such as meta-analysis using effect size could be done to get more insight of the particular findings and relationships. Based on the findings in this review, we believe that the future work is very crucial as it contributes to ISC field especially in providing new insights in an attempt to produce a holistic model of ISC cultivation to be used as guidelines for practitioners and reference model for academicians. We intend to formulate a new model of ISC based on comprehensive

dimensions that could represent a holistic concept of ISC and test this model to examine the appropriateness of dimensions proposed.

6. CONCLUSION

Despite number of studies available in ISC literature, there is actually lack of guidelines that could be used to effectively establish ISC in improving security behavior in the organizations. While most of the studies did not focus on examining the relationship between ISC and security behavior, few empirical studies that examined this relationship also could not provide enough empirical evidences on the actual effect of ISC towards security behavior. This was due to the approaches taken in terms of conceptualization and operationalization of ISC, as well as lack of integration with theoretical behavioral framework. Therefore, the conceptualization of ISC as multidimensional concept and the adoption of behavioral theory should be considered and incorporated for this type of study. It will produce more focused, holistic and comprehensive findings on the relationship which in turn could be used as effective strategies of ISC cultivation in improving security behavior of employees in the organizations.

7. ACKNOWLEDGEMENTS

This research is supported by UMP Post Graduate Research Grant Scheme, PGRS170303. The authors fully acknowledged Universiti Malaysia Pahang (UMP) for the approved fund, which makes this important research viable and effective.

8. REFERENCES

[1] Hu Q, Dinev T, Hart P, Cooke D. Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 2012, 43(4):615-660

[2] Richardson R. 2010/2011 CSI computer crime and security survey. 2011, http://gocsi.com/survey/

[3] Thomson K L, von Solms R, Louw L. Cultivating an organizational information security culture. Computer Fraud and Security, 2006, 2006(10):7-11

[4] Baker W, Goudie M, Hutton A, Hylender C, Niemantsverdriet J, Novak C, Ostertag D, Porter C, Rosen M, Sartin B, Tippett P. Verizon 2010 data breach investigations report. New Jersey: Verizon Enterprise Solutions, 2010

[5] Boujettif M, Wang Y. Constructivist approach to information security awareness in the

Middle East. In IEEE International Conference on Broadband, Wireless Computing, Communication and Applications, 2010, pp. 192-199

[6] Poll H. 2015 vormetric insider threat report: Trends and future directions in data security-Healthcare edition. California: Vormetric Inc., 2015

[7] Greig A, Renaud K, Flowerday S. An ethnographic study to assess the enactment of information security culture in a retail store. In IEEE World Congress on Internet Security, 2015, pp. 61-66

[8] Vroom C, Von Solms R. Towards information security behavioural compliance. Computers and Security, 2004, 23(3):191-198

[9] Padayachee K. Taxonomy of compliant information security behavior. Computers and Security, 2012, 31(5):673-680

[10] International Organization for Standardization (ISO). ISO/IEC 27001 information security management. Geneva: ISO, 2017

[11] Organisation for Economic Co-operation and Development (OECD). OECD guidelines for the security of information systems and networks: Towards a culture of security. Paris: OECD, 2002

[12] Goeken M. Towards an evidence-based research approach in information systems. In 32nd International Conference on Information Systems, 2011, pp. 1-16

[13] Vom Brocke J, Simons A, Niehaves B, Riemer K, Plattfaut R, Cleven A. Reconstructing the giant: On the importance of rigour in documenting the literature search process. In 17th European Conference on Information Systems, 2009, pp. 2206-2217

[14] Flores W R, Ekstedt M. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers and Security, 2016, 59:26-44

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

[16] D'Arcy J, Greene G. The multifaceted nature of security culture and its influence on end user behavior. In IFIP TC8 International Workshop on Information Systems Security Research, 2009, pp. 145-157

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

[18] Radivojevic N. Parliamentary control of security information agency in terms of security

culture-state and problems. Zbornik Radova, 2013, 47:475-492

[19] Chen Y A, Ramamurthy K R, Wen K W. Impacts of comprehensive information security programs on information security culture. Journal of Computer Information Systems, 2015, 55(3):11-19

[20] Tang M, Zhang T. The impacts of organizational culture on information security culture: A case study. Information Technology and Management, 2016, 17(2):179-186

[21] Flores W R, Ekstedt M. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers and Security, 2016, 59:26-44

[22] Dhillon G, Syed R, Pedron C. Interpreting information security culture: An organizational transformation case study. Computers and Security, 2016, 56:63-69

[23] Martins N, Da Veiga A. The value of using a validated information security culture assessment instrument. In 8th European Conference on IS Management and Evaluation, 2010, pp. 146-154

[24] Gebrasilase T, Lessa LF. Information security culture in public hospitals: The case of Hawassa referral hospital. African Journal of Information Systems, 2011, 3(3):72-86

[25] Da Veiga A, Martins N. Improving the information security culture through monitoring and implementation actions illustrated through a case study. Computers and Security, 2015, 49:162-176

[26] AlHogail A. Design and validation of information security culture framework. Computers in Human Behavior, 2015, 49:567-575

[27] Da Veiga A, Martins N. Information security culture: A comparative analysis of four assessments. In 8th European Conference on IS Management and Evaluation, 2014, pp. 49-57

[28] Van Niekerk J F, Von Solms R. Information security culture: A management perspective. Computers and Security, 2010, 29(4):476-486

[29] Da Veiga A, Eloff J H. A framework and assessment instrument for information security culture. Computers and Security, 2010, 29(2):196-207

[30] Da Veiga A, Martins N. Information security culture and information protection culture: A validated assessment instrument. Computer Law and Security Review, 2015, 31(2):243-256

[31] Glenda R. How to create a security culture in your organization. 2008, http://content.arma.org/IMM/NovDec2008/How_to_Create_a_Security_Culture.aspx

[32] Furnell S, Thomson K L. From culture to disobedience: Recognising the varying user acceptance of IT security. Computer Fraud and Security, 2009, 2009(2):5-10

[33] Stetson D M. Achieving effective medical information security: Understanding the

culture. Bulletin of the Association for Information Science and Technology, 1997, 23(3):17-21

[34] Chmura J. The impact of positive organisational culture values on information security management in the company. Journal of Positive Management, 2016, 7(1):87-98

[35] Arsenijevic O, Trivan D, Milosevic M. Storytelling as a modern tool of construction of information security corporate culture. Ekonomika, 2016, 62(4):105-114

[36] Organisation for Economic Co-operation and Development (OECD). OECD guidelines for the security of information systems and networks: Towards a culture of security. 2002, https://www.oecd.org/sti/ieconomy/15582260.pdf

[37] Baggett W O. Creating a culture of security: The OECD standards for systems security provide internal auditors with a tool for operationalizing tone at the top. Internal Auditor, 2003, 60(3):37-41

[38] Ruighaver A B, Maynard S B, Chang S. Organisational security culture: Extending the end-user perspective. Computers and Security, 2007, 26(1):56-62

[39] Furnell S. End-user security culture: A lesson that will never be learnt? Computer Fraud and Security, 2008, 2008(4):6-9

[40] Alfawaz S, Nelson K, Mohannak K. Information security culture: A behaviour compliance conceptual framework. In 8th Australasian Conference on Information Security-Volume 10, 2010, pp. 47-55

[41] Corriss L. Information security governance: Integrating security into the organizational culture. In ACM Workshop on Governance of Technology, Information and Policies, 2010, pp. 35-41

[42] Renaud K, Goucher W. The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture. In International Conference on Human Aspects of Information Security, Privacy, and Trust, 2014, pp. 361-372

[43] Martins A, Elofe J. Information security culture. In M. A. Ghonaimy, M. T. El-Hadidi, & H. K. Aslan (Eds.), Security in the information society. Massachusetts: Springer, 2002, pp. 203-214

[44] Schlienger T, Teufel S. Analyzing information security culture: Increased trust by an appropriate information security culture. In IEEE 14th International Workshop on Database and Expert Systems Applications, 2003, pp. 405-409

[45] Schlienger T, Teufel S. Information security culture-From analysis to change. South African Computer Journal, 2003, 2003(31):46-52

[46] Knapp KJ, Marshall T E, Kelly Rainer R, Nelson Ford F. Information security:

Management's effect on culture and policy. Information Management and Computer Security, 2006, 14(1):24-36

[47] Helokunnas T, Kuusisto R. Information security culture in a value net. In IEEE Engineering Management Conference, 2003, pp. 190-194

[48] Von Solms B. Information security-The third wave? Computers and Security, 2000, 19(7):615-620

[49] Ernest Chang S, Lin C S. Exploring organizational culture for information security management. Industrial Management and Data Systems, 2007, 107(3):438-458

[50] Schlienger T, Teufel S. The socio-cultural dimension in information security. In M. A. Ghonaimy, M. T. El-Hadidi, & H. K. Aslan (Eds.), Security in the information society: Visions and perspectives. Berlin: Springer Science and Business Media, 2002, pp. 191-201

[51] Da Veiga A, Martins N, Eloff J H. Information security culture-Validation of an assessment instrument. Southern African Business Review, 2007, 11(1):147-166

[52] Veiga A D, Eloff J H. An information security governance framework. Information Systems Management, 2007, 24(4):361-372

[53] Shih C C, Huang S J. Exploring the relationship between organizational culture and software process improvement deployment. Information and Management, 2010, 47(5):271-281

[54] Dojkovski S, Lichtenstein S, Warren M J. Fostering information security culture in small and medium size enterprises: An interpretive study in Australia. In European Conference on Information Systems, 2007, pp. 1560-1571

[55] Lim J S, Ahmad A, Chang S, Maynard S B. Embedding information security culture emerging concerns and challenges. In Pacific Asia Conference on Information Systems, 2010, pp. 463-474

[56] Gaunt N. Practical approaches to creating a security culture. International Journal of Medical Informatics, 2000, 60(2):151-157

[57] Kraemer S, Carayon P. Computer and information security culture: Findings from two studies. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 2005, 49(16):1483-1488

[58] Alnatheer M, Nelson K. Proposed framework for understanding information security culture and practices in the Saudi context. In 7th Australian Information Security Management Conference, 2009, pp. 6-17

[59] Zakaria O, Gani A. A conceptual checklist of information security culture. In 2nd European Conference on Information Warfare and Security, 2003, pp. 365-371

[60] Schlienger T, Teufel S. Tool supported management of information security culture. In R. Sasaki, E. Okamoto, & H. Yoshiura (Eds.), Security and privacy in the age of ubiquitous computing: IFIP TC11 20th International Information Security Conference, May 30 - June 1, 2005, Chiba, Japan. New York: Springer, 2010, pp. 65-77

[61] Von Solms R, Von Solms B. From policies to culture. Computers and Security, 2004, 23(4):275-279

[62] Van Niekerk J, von Solms R. Understanding information security culture: A conceptual framework. In IEEE Information Security for South Africa, 2006, pp. 1-10

[63] Zakaria O. Internalisation of information security culture amongst employees through basic security knowledge. In IFIP International Information Security Conference, 2006, pp. 437-441

[64] Okere I, Van Niekerk J, Carroll M. Assessing information security culture: A critical analysis of current approaches. In IEEE Information Security for South Africa, 2012, pp. 1-8

[65] Dojkovski S, Lichtenstein S, Warren M. Challenges in fostering an information security culture in Australian small and medium sized enterprises. In 5th European conference on Information Warfare and Security, 2006, pp. 31-40

[66] Ngo L, Zhou W, Warren M. Understanding transition towards information security culture change. In 3rd Australian Computer, Network and Information Forensics Conference, 2005, pp. 67-73

[67] Kuusisto T, Ilvonen I. Information security culture in small and medium size enterprises. In Frontiers of E-Business Research Conference, 2003, pp. 431-439

[68] Lacey D. Understanding and transforming organizational security culture. Information Management and Computer Security, 2010, 18(1):4-13

[69] Johnston A C, Hale R. Improved security through information security governance. Communications of the ACM, 2009, 52(1):126-129

[70] Zakaria O. Understanding Challenges of Information Security Culture: A Methodological Issue. In 2nd Australian Information Security Management Conference, 2004, pp. 83-93

[71] Alnatheer M, Chan T, Nelson K. Understanding and measuring information security culture. In Pacific Asia Conference on Information Systems, 2012 pp. 1-16

[72] Parsons K, McCormac A, Butavicius M, Ferguson L. Human factors and information security: Individual, culture and security environment. Technical report DSTO-TR-2484, Edinburgh: Defence Science and Technology Organisation, 2010

[73] Van Niekerk J, von Solms R. A holistic framework for the fostering of an information security sub-culture in organizations. In IEEE Information Security for South Africa, 2005, pp.

1-13

[74] Kuusisto T, Ilvonen I. Information security culture in small and medium size enterprises. In Frontiers of E-Business Research Conference, 2003, pp. 431-439

[75] Kayworth T, Whitten D. Effective information security requires a balance of social and technology factors. MIS Quarterly Executive, 2010, 9(3):163-175

[76] Leach J. Improving user security behaviour. Computers and Security, 2003, 22(8):685-692

[77] Dojkovski S, Lichtenstein S, Warren M. Enabling information security culture: Influences and challenges for Australian SMEs. In 21st Australasian Conference on Information Systems, 2010, pp. 1-10

[78] Kuusisto R, Kuusisto T. Chapter 6: Information security culture as a social system: Some notes of information availability and sharing. In M. Gupta, & R. Sharman (Eds.), Social and human elements of information security: Emerging trends and countermeasures. Pennsylvania: IGI Global, 2009, pp. 77-97

[79] Chia P A, Maynard S B, Ruighaver A B. Understanding organizational security culture. In Pacific Asia Conference on Information Systems, 2002, pp. 1-23

[80] Malcolmson J. What is security culture? Does it differ in content from general organisational culture? In 43rd Annual 2009 International Carnahan Conference on Security Technology, 2009, pp. 361-366

[81] Zakaria O, Gani A, Mohd N M, Badrul A N. Reengineering information security culture formulation through management perspective. In International Conference on Electrical Engineering and Informatics, 2007, pp. 638-641

[82] AlHogail A, Mirza A. Information security culture: A definition and a literature review. In IEEE World Congress on Computer Applications and Information Systems, 2014, pp. 1-7

[83] Lopes I, Oliveira P. Understanding information security culture: A survey in small and medium sized enterprises. In Á. Rocha et al. (Eds.), New Perspectives in information systems and technologies, volume 1, advances in intelligent systems and computing. Cham: Springer International Publishing, 2014, pp. 277-286

[84] Ramachandran S, Rao SV, Goles T. Information security cultures of four professions: A comparative study. In IEEE 41st Annual Hawaii International Conference on System Sciences, 2008, pp. 454-454

[85] Ramachandran S, Rao S. Security cultures in organizations: A theoretical model. In 12th Americas Conference on Information Systems, 2006, pp. 3460-3464

[86] Ramachandran S, Rao C, Goles T, Dhillon G. Variations in information security cultures

across professions: A qualitative study. Working Paper Series WP # 0021IS-19-2012, Texas: University of Texas at San Antonio, 2013, pp. 1-41

[87] Talib S, Clarke N L, Furnell S M. Chapter 4: Establishing a personalized information security culture. In Ismail K (Ed.), Contemporary challenges and solutions for mobile and multimedia technologies. Pennsylvania: IGI Global, 2013, pp. 53-69

[88] Greene G, D'Arcy J. Assessing the impact of security culture and the employee-organization relationship on IS security compliance. In 5th Annual Symposium on Information Assurance, 2010, pp. 42-49

[89] Maynard S, Ruighaver A, Chia P. Exploring organisational security culture: Developing a comprehensive research model. In 6th Pacific Asia Conference on Information Systems, 2002, pp. 1-13

[90] Da Veiga A. Cultivating and assessing information security culture. PhD thesis, Gauteng: University of Pretoria, 2008

[91] Alfawaz S M. Information security management: A case study of an information security culture. PhD thesis, Brisbane: Queensland University of Technology, 2011

[92] Hassan N H, Ismail Z. A conceptual model for investigating factors influencing information security culture in healthcare environment. Procedia-Social and Behavioral Sciences, 2012, 65:1007-1012

[93] Koh K, Ruighaver A B, Maynard S B, Ahmad A. Security governance: Its impact on security culture. In 3rd Australian Information Security Management Conference, 2005, pp. 47-58

[94] Ilvonen I. Information security culture or information safety culture-What do words convey? In European Conference on Cyber Warfare and Security, 2011, pp. 148-154

[95] Thomson K L. Information security conscience: A precondition to an information security culture? Journal of Information System Security, 2010, 6(4):5-19

[96] Kluge E H. Fostering a security culture: A model code of ethics for health information professionals. International Journal of Medical Informatics, 1998, 49(1):105-110

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

[98] Kuusisto R, Nyberg K, Virtanen T. Unite security culture. In 3rd European Conference on Information Warfare and Security, 2004, pp. 221-229

[99] Al-Shehri Y, Clarke N L. Information security awareness and culture. In P. Dowland, & S. Furnell (Eds.), Advances in communications, computing, networks and security: Proceedings of the MSc/MRes programmes from the School of Computing, Communications and

Electronics, 2007-2008, volume 6. North Carolina: Lulu.com, 2009, pp. 12-22

[100] Van Niekerk J F. Fostering information security culture through integrating theory and technology. Doctoral thesis, Port Elizabeth: Nelson Mandela Metropolitan University, 2005

[101] Zakaria O. Employee security perception in cultivating information security culture. In P. Dowland, S. Furnell, B. Thuraisingham, & X. S. Wang (Eds.), Security management, integrity, and internal control in information systems. Massachusetts: Springer, 2005, pp. 83-92

[102] Organisation for Economic Co-operation and Development (OECD). Security of information systems and networks. 2006, http://www.oecd.org/sti/ieconomy/37418730.pdf

[103] Ghernouti-Hélie S. A national strategy for an effective cybersecurity approach and culture. In IEEE International Conference on Availability, Reliability and Security, 2010, pp. 370-373

[104] Finch J, Furnell S, Dowland P. Assessing IT security culture: System administrator and end-user perspectives. In ISOneWorld 2003 Conference and Convention, 2003, pp. 1-10

[105] Sherif E, Furnell S. A conceptual model for cultivating an information security culture. International Journal for Information Security Research, 2015, 5(2):565-573

[106] Dojkovski S, Lichtenstein S, Warren M. Developing information security culture in small and medium size enterprises: Australian case studies. In D. Remenyi (Ed.), ECIW2008-7th European Conference on Information Warfare and Security: ECIW2008. Reading: Academic Conferences Limited, 2008, pp. 55-66

[107] Munteanu A B, Fotache D. Enablers of information security culture. Procedia Economics and Finance. 2015, 20:414-422

[108] Reniers G L, Cremer K, Buytaert J. Continuously and simultaneously optimizing an organization’s safety and security culture and climate: The Improvement Diamond for Excellence Achievement and Leadership in Safety & Security (IDEAL S&S) model. Journal of Cleaner Production, 2011, 19(11):1239-1249

[109] Da Veiga A, Da Veiga A. Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. Information and Computer Security, 2016, 24(2):139-151

[110] Cormack A. Do we need a security culture? Vine, 2001, 31(2):8-10

[111] Govender S, Kritzinger E, Loock M. The influence of national culture on information security culture. In IEEE IST-Africa Week Conference, 2016, pp. 1-9

[112] Teufel S, Teufel B. Crowd energy information security culture-Security guidelines for smart environments. In IEEE International Conference on Smart City/SocialCom/SustainCom,

2015, pp. 123-128

[113] Alnatheer M A. Information security culture critical success factors. In IEEE 12th International Conference on Information Technology-New Generations, 2015, pp. 731-735

[114] AlHogail A, Mirza A. A proposal of an organizational information security culture framework. In IEEE International Conference on Information, Communication Technology and System, 2014, pp. 243-250

[115] Reid R, Van Niekerk J, Renaud K. Information security culture: A general living systems theory perspective. In IEEE Information Security for South Africa, 2014, pp. 1-8

[116] Von Solms R, Van Niekerk J. From information security to cyber security. Computers and Security, 2013, 38:97-102

[117] Al-Mayahi I, Sa'ad PM. Information security culture assessment: Case study. In IEEE International Conference on Information Science and Technology, 2013, pp. 789-792

[118] Hassan N H, Ismail Z, Maarop N. A conceptual model for knowledge sharing towards information security culture in healthcare organization. In IEEE International Conference on Research and Innovation in Information Systems, 2013, pp. 516-520

[119] Al Sabbagh B, Ameen M, Wätterstam T, Kowalski S. A prototype For HI 2 Ping information security culture and awareness training. In IEEE International Conference on e-Learning and e-Technologies in Education, 2012, pp. 32-36

[120] Božić G. The role of a stress model in the development of information security culture. In IEEE 35th International Convention on Information and Communication Technology, Electronics and Microelectronics, 2012, pp. 1555-1559

[121] Woodhouse S. Information security: End user behavior and corporate culture. In 7th IEEE International Conference on Computer and Information Technology, 2007, pp. 767-774

[122] Connolly L, Lang M. Investigation of cultural aspects within information systems security research. In IEEE International Conference for Internet Technology and Secured Transactions, 2012, pp. 105-111

[123] Cardoso M G, Laureano R D, Serrão C. Cybersecurity culture in Portuguese organizations: An exploratory analysis. In IEEE 12th Iberian Conference on Information Systems and Technologies, 2017, pp. 1-5

[124] Al Sabbagh B, Kowalski S. Developing social metrics for security modeling the security culture of it workers individuals (case study). In IEEE Mosharaka International Conference on Communications, Computers and Applications, 2012, pp. 112-118

[125] Santos-Olmo A, Sánchez L E, Caballero I, Camacho S, Fernandez-Medina E. The importance of the security culture in SMEs as regards the correct management of the security

of their assets. Future Internet, 2016, 8(3):1-27

[126] Dojkovski S, Warren M, Lichtenstein S. Information security culture in small and medium sized enterprises: A socio-cultural framework. In 6th Australian Information Warfare and Security Conference, 2005

[127] Dugo T. The insider threat to organizational information security: A structural model and empirical test. PhD thesis, Alabama: Auburn University, 2007

[128] Sommestad T, Hallberg J, Lundholm K, Bengtsson J. Variables influencing information security policy compliance: A systematic review of quantitative studies. Information Management and Computer Security, 2014, 22(1):42-75

[129] AlKalbani A, Deng H, Kam B. Organisational security culture and information security compliance for e-government development: The moderating effect of social pressure. In Pacific Asia Conference on Information Systems, 2015, pp. 1-11

[130] Schein E. H. Organizational culture and leadership. New Jersey: John Wiley and Sons, 2010

[131] D'Arcy J, Greene G. The multifaceted nature of security culture and its influence on end user behavior. In IFIP TC8 International Workshop on Information Systems Security Research, 2009, pp. 145-157

[132] Lebek B, Uffen J, Neumann M, Hohler B, H. Breitner M. Information security awareness and behavior: A theory-based literature review. Management Research Review, 2014, 37(12):1049-1092

[133] Cohen J. Statistical power analysis for the behavioral sciences. New Jersey: Lawrence Earlbaum Associates, 1988

How to cite this article:
Akhyari N, Ruzaini A A, Rashid A H. Information security culture guidelines to improve employee's security behavior: a review of empirical studies. J. Fundam. Appl. Sci., 2018, *10(2S), 258-283.*