International Journal of Security and Its Applications
Vol.9, No.7 (2015), pp.163-178
http://dx.doi.org/10.14257/ijsia.2015.9.7.15

Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study

Areej Al Hogail

Department of Information Systems
College of Computing and Information Sciences
King Saud University
alhogail@ccis.imamu.edu.sa

Abstract

An information security-aware culture will minimize internal threats to information assets through the construction of appropriate information security beliefs and values that guide employee behavior when interacting with information assets and information technology systems. This paper aims to illustrate the application of the Information Security Culture Framework (ISCF) to asses and cultivate an information security aware culture within an organization through an empirical study. The ISCF is a comprehensive framework that consists of five dimensions (Strategy, Technology, Organization, People, and Environment) and integrates change management and the human factor in information security. The empirical study includes three case studies, selected to demonstrate the effectiveness of ISCF in describing and explaining the organizational information security culture. A sequential mixed method, to collect quantitative survey data and qualitative interview data, is used to demonstrate the validity and reliability of the framework. The ISCF therefore could be used by all types of organizations in order to assess whether an acceptable level of information security culture has been implemented and, if not, corrective actions are suggested.

Keywords: *information security culture; information security management; change management; human behavior; human factor in information security*

1. Introduction

This section has three main parts. The first presents a brief introduction to the information security culture. The second provides a literature review of the available information security culture frameworks and assessment in addition to a detailed review of the information security culture framework (ISCF). The third section introduces the work described by this paper.

1.1 Information Security Culture

Organizations should focus on employees' behavior to achieve information security, as their security effectively depends upon what employees do or fail to do [1]. Focusing on the technical aspects of security, without appropriate consideration of the human interaction with the system is evidently inadequate [2]. Human behavior represents the weakest link in the security chain [3–6].

Information security culture can be defined as follows: "The collection of perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction with information assets in [an] organization with the aim of influencing employees' behavior to preserve information security" [7].

Information security culture provides a guide to human behavior when interacting with information technology (IT) systems to avoid actions that may cause risks to the security

ISSN: 1738-9976 IJSIA

of information assets or the IT systems. The culture that promotes good security-related human behavior through knowledge, artifacts, values, and assumptions is far more effective than regulations that simply mandate employees' behavior. Without a proper information security culture, the enforcement of security policies through the traditional cycle is less likely to be effective [8] than when employees know, understand, and accept the necessary precautions.

Alfawaz *et al.* [9] studied a user's security behavior and suggested that significant security gains could be achieved by strengthening the security culture of organization members. Many studies suggest that implementing information security culture inside organizations can lead an employee to act as a "human firewall" [10]. They suggest that organizations need to take formative steps in order to create an environment where security is "everyone's responsibility" and where doing the right thing is the norm [1], [11–15]. Dojkovski *et al.* [16] suggested that a strong information security culture in organizations might deal with many of the behavioral issues that cause information security breaches in such organizations.

1.2 Literature Review

Organizations need a comprehensive framework and guidelines to build a security-aware culture. A literature analysis in [17] indicated the lack of a comprehensive framework to guide the cultivation and assessment of an effective information security culture. Moreover, most available approaches that address the threats posed by employee behavior do not focus on the interaction between the behavior of the employee and the organizational culture [1] and do not focus on directing the employees' behavior.

Available frameworks have focused on the information security culture in an organization and its relationship to one specific dimension. To clarify, [18-19, 5, 15] have studied the effect of organizational culture on the information security culture and focused on the policies and strategies. [1, 21] have proposed an awareness program to cultivate an information security culture. [9, 16, 22] studied the effects of national setting on human behavior and the information security culture.

Most available framework were lacking in a comprehensive view that integrated the human, the organization and the technology to provide organizations with an all-inclusive framework to aid the organization's information security practitioner in the implementation and adoption of an information security culture [7]. Therefore, there is a strong need for a comprehensive framework to cultivate and assess a security-aware culture.

Moreover, Okere *et al.* [23] stated that there is no method or toolset to assess an information security culture as there is no published or widely accepted and consolidated approach that assigned how to assess the culture and more research in this area is needed. However, one way to measure the status of an organization's information security culture is to use a questionnaire such as the ones proposed by [4, 6] or [24] to achieve an understanding of factors influence the employees security behavior.

In order to overcome the lack of comprehensive frameworks, the author has proposed a comprehensive Information Security Culture Framework (ISCF) for organizations in [25]. The ISCF consists of five dimensions: Strategy, Technology, Organization, People, and Environment (STOPE). Each dimension is composed of a number of related tasks that cover four domains of human behavior factors; preparedness, responsibility, management, and society and regulations. These interact with each other to create an effective information security culture that is able to minimize security threats posed by organizations' insider behavior. It incorporates change management principles adapted from [26] that guide the cultivation of the information security culture. It ensures its smooth implementation with minimum resistance and change chaos. It aims to understand the interrelationship between different factors and issues associated with the information security culture within organizations. It also provides the structure to guide management

and information security specialists with assessment and cultivation. The framework has been validated through an expert review and the validation process has been explained in [25].

The strategy dimension is concerned with the appropriate implementation of different information security strategies such as plans of actions, policies, objectives, best practices, standards, guidelines, and priorities that are designed to guide organization members to reach the goal of protecting information assets. The technology dimension is concerned with security technologies such as hardware, software, services, appliances, and applications that are used within the organization to protect information assets. The organization dimension is concerned with the collection of information security-related beliefs, values, assumptions, symbols, norms, and knowledge that uniquely represent the organization.

The people dimension is concerned with the behavior of any person within the organization who is in direct contact with information assets. The information security culture aims to ensure that information security is everyone's responsibility. The environment dimension is concerned with the identifiable external elements surrounding the organization that affect its structure and operations and eventually the security of the information assets and the information security culture. It includes national culture, ethical conduct, government initiatives, and legal and regulatory systems.

The human factor diamond presents the four domains of human factors that influence information security behavior. The information security culture shall consider each human factor carefully to improve user security behavior. The "preparedness" domain is mainly concerned with training and awareness, knowledge acquisition, and change of old practices. The "responsibility" domain is mainly related to employees' practices and performance such as monitoring and control, reward and deterrence, as well as acceptance of responsibility. The "management" domain is concerned with security policies, practices, directions, and interaction issues. Finally, the "society and regulations" domain is mainly related to social and cultural aspects and regulation issues.

The changeover to adapt to an information security culture needs to be managed effectively and appropriately to achieve the required goals. Ineffective change can lead to chaos that exposes critical information assets to security risks as it requires disruption to what employees are used to do [23, 27-28]. The ISCF have incorporated change management principles from [26] in order to guide the changes that are associated with the development of an information security-aware culture inside the organization and to enhance acceptance of, and compliance with, information security policies and procedures. The principles are: management support, motivation, sufficiency of resources, culture analysis, communication, change agents, involvement and ownership, success measures and milestones, workshops & focus groups, and training. The framework is portrayed in Figure 1.

1.3 The presented work

Organizations need structure and guidance for information security specialists to assess and cultivate the appropriate information security culture that protects the information assets from internal threats caused by employees' behavior. Moreover, organizations need to measure and report on the state of the information security culture frequently. The Information Security Culture Framework (ISCF) provides a comprehensive framework that aids in implementing and maintaining a security-aware culture in different types of organizations. In this paper, the ISCF proposed by the author in [25] guides an empirical study to design an assessment instrument to assess the level of information security culture in three case studies. The data was collected sequentially through an employee survey and then results were validated through interviews with seven information security specialists. The objective was to validate the ISCF assessment instrument, hence providing an applicable and valid instrument that can be used by organizations to cultivate and assess information security culture.

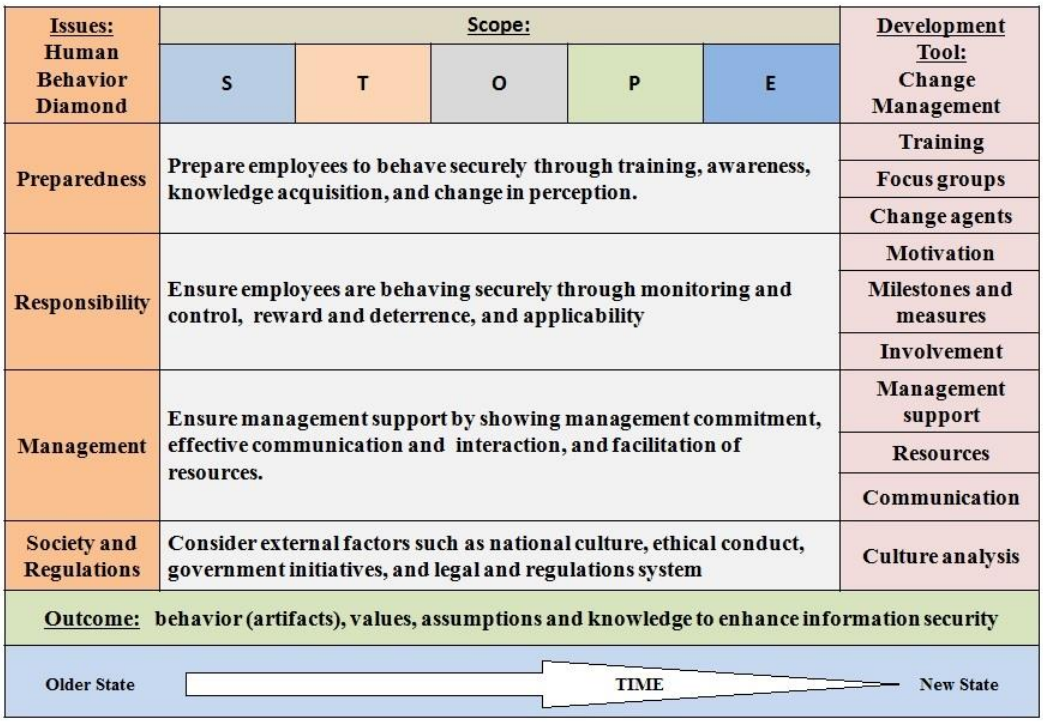

Figure 1. Information Security Culture Framework (ISCF) [25]

2. Methodology

Case study approach is used in this research to assess the information security culture within the participant organizations based on the ISCF in real life situation. According to the methodologies used in information security culture research, 18% of the research papers have used case study methodology [7]. The three case studies were conducted to investigate the experience of the organizations' information security culture. All three organizations are located in Saudi Arabia. The three cases' profiles are summarized as the following:

Case A: A government organization that is responsible for issuing the required rules and regulations and monitoring some financial investments.

Case B: A Small-medium enterprise (SME). Employees may have access to financial and life style records of their clients that should be always kept safe and not disclosed. Moreover, the organization holds many projects- related information that may be desirable for many competitors.

Case C: A multinational trading company that manages subsidiary business all over the Middle East including hotels, restaurants, electronics, food industry and petrochemicals.

2.1 Data Gathering

The data was collected sequentially using a combination of questionnaire and interviews to collect in-depth data about each case study. The questionnaire was used to collect data from the organizations' employees regarding their values, beliefs, perceptions, knowledge and practice towards information security, based on the ISCF. Afterward, seven interviews with information security specialists at the same organizations were conducted, in order to complete the investigation and to validate the survey's results.

The unit of analysis in this research is towards information security culture practices and knowledge. Details of the design and distribution of the questionnaire and interviews will be discussed in the following sections.

2.1.1 Questionnaire: In this study, a questionnaire assessment instrument is developed, based upon the ISCF framework and influenced by previously published information security culture assessment instruments. The questionnaire consists of two parts; firstly, the demographical information that is used to segment the data and to comparisons between the respondents. It collects information regarding age group, academic background, job level, length of employment and information technology experience.

The second part aims to assess the information security culture based on the ISCF dimensions. Framework dimensions have been mapped into several representative tasks and statements in order be measured. Then, statements were grouped as clusters to represent each element of the dimensions and, in relation to one another, to represent one issue [6]. The questionnaire questions were divided to cover the following issues:

- Strategy: measure the availability, accessibility and clarity of different strategies; and study the effects of different strategy elements on the employees' behaviour and general information security culture.
- Technology: assess the application of different technical measures, the availability of guidance and support, and their effectiveness in the behavior and culture.
- Organization: assess the values, beliefs, behaviour and knowledge towards information security and their relationship to the information security culture.
- People: assess different human factors of preparedness, responsibility and management role that affect the behavior and their relationship to the information security culture.
- Environment: assess the effect of different external factors of national culture, laws and regulations, ethical conduct and government initiatives on the employees' behaviour and the culture.
- Change management: assess the level of application of each change management principles inside the organization and their effect towards having an effective information security culture.

Statements have been selected to ensure that a statement or more represent each human factor for every dimension. For instance, technology preparedness is represented in the statement: "I have received training on using information security hardware and software". Technology responsibility is represented in the statement: "I know that the appropriate use of technical controls is vital to achieve information security" and so on. Likert scale is used to measure the respondent's degree of agreement or disagreement with each statement. It varies from a 2 points Likert scale of Agree and Disagree answers to a 5 points Likert scale, depending upon the question and the possible responses to avoid bias. The used scale is represented in Figure 2 with an example.

Statement	Agree	Disagree			
I have read information security policy or strategy					
Statement	Agree	I don't Know	Disagree		
The organization has a written information security policy or strategy					
Statement	Strongly Agree	Agree	I don't Know	Disagree	Strongly Disagree
Information security strategy element clearly state what is expected from me.					

Figure. 2 The Questionnaire Scale

In order to achieve a satisfactory sample, the online questionnaire had been sent to all employees in the participated case studies' organizations via e-mail. It was accompanied by a covering letter that describes the questionnaire and emphasizes the confidentiality of the obtained results and ensures the anonymity of participants. Table 1 indicates the number of responses obtained for each case study. After that, data obtained from the survey was prepared for analysis.

Table 1. Questionnaire Response Rate

Criteria	Case A	Case B	Case C
Number of Employees who are in direct contact with information (population)	400	50	100
Number of response	52	20	22
Response rate	13 %	40 %	22 %

2.1.2 Interviews: A number of reasons made the choice of the interview method appropriate in information security culture research. For instance, 15% of research papers in information security culture research have used interviews to collect data [7]. Zakria [29] has recommended the use of semi-structured interviews to collect information concerning employees' basic assumptions, real and implicit security behavior in information security culture research.

An interview guide has been designed to ensure maintaining the direction of the interview, the consistency of the data collected, and to minimize bias as much as possible. Open ended questions were designed to explore aspects of how information security is managed at the organization, general employees' behavior and to confirm the results from the questionnaire. It also aimed to validate the ISCF's suitability of application in each case study.

Seven interviews were carried out through field visits or phone meetings during business hours. The interviews were conducted as described in Table 2:

Table 2. Interviews Details

Case	Number of interviewees	Type
A	3	F2F
B	2	F2F
C	2	phone

For ethical reasons, the identity of the interviewees and the data they provided were kept confidential, and the collected data was used for research only. The potential benefits of the interview had been explained to participants in addition to their rights. The interviews were transcribed and data was then prepared for analysis. The results are presented in the next section.

3. Results and Analysis

3.1 Questionnaire Results

The data collected through the case study questionnaire survey was quantitatively analyzed using the Statistical Package for the Social Sciences (SPSS) software. The data preparation process ensured that the data set had no missing values and was not distorted significantly by the different opinions of specific groups. The data was ordinal and small in size; therefore, a non-parametric test was used when appropriate. The following statistical analysis describes the results.

3.1.1 Reliability: Cronbach's alpha is the most common used technique to measure reliability through providing an indication of internal consistency. The Cronbach alpha value of each dimension and sub dimension of the framework has been analyzed in order to establish the reliability of each dimension based on the theoretical framework. Cronbach alpha values must meet the minimum accepted criteria that is to be above 0.6 to confirm the consistency and reliability of the framework [6]. Table 3 provides the results of the data analysis to construct reliability.

Table 3. Cronbach's Alpha Attribute Value and the Analysis Results

Factor	No of items	Case A		Case B		Case C	
		α **value**	**Analysis**	α **value**	**Analysis**	α **value**	**Analysis**
S	8	.705	good	.707	good	.816	good
T	6	.720	good	.622	acceptable	.619	acceptable
O	21	.865	good	.832	good	.928	excellent
P	27	.903	excellent	.824	good	.900	excellent
E	10	.775	good	.631	acceptable	.819	good

The values of the Cronbach's alpha ranged from (Case A: 0.705 to 0.903; Case B: 0.622 to 0.832; Case C: 0.619 to 0.928) which is larger than the threshold. This indicates a good internal consistency and reliability. Therefore, the questionnaire appears to be composed of a set of consistent variables for capturing the meaning of the framework.

3.1.2 Validity: In order to establish the validity of the tested framework, SEM analysis using Goodness of Fit Index(GFI) will be used to measure a fit between the proposed framework and the empirical data [30]. The Goodness of Fit Index (GFI) has the criteria that if ($0.9 \leq GFI \leq 0.94$) then it is acceptable fit and if ($0.95 \leq GFI \leq 1.0$) then it is a good fit. Table 4 provides the attribute value of GFI for each case study.

Table 4. Validity Analysis

Goodness Fit Index	**GFI value**	**Acceptance analysis**
Case A	.927	Acceptable fit
Case B	.969	Good fit
Case C	.902	Acceptable fit

It is clear from the results that the GFI is higher than 0.9 indicating that there is a good fit between the empirical data and the framework. This indicates that the framework is meeting its objectives in realistic environment.

3.1.3 Demographical Information: The influence of demographical information and categories was analyzed in order to figure out any external influences upon the level of information security culture among the organizations' members. In order to test the difference, the Independent Sample Kruskal-Wallis non-parametric test at a significance level of .05 was used. It is used for testing whether samples originate from the same distribution and to compare two or more samples that are independent, and may have different sample sizes. For two-option answers, the Mann–Whitney U test is used. The results are summarized in Table 5.

Table 5. Demographical Data Analysis

Null Hypothesis: The distribution is the same across all categories of :	**Test**	**Sig Case A**	**Sig Case B**	**Sig Case C**	**Decision**

Age	Independent Sample Kruskal-Wallis test at significance level of .05	0.396	0.905	0.485	retain the null hypothesis
Education		0.051	0.242	0.767	retain the null hypothesis
Years of experience in organization		0.421	0.487	0.138	retain the null hypothesis
Job level		0.043	0.947	0.138	retain the null hypothesis
Gender	Independent Sample Mann-Whitney U test at significance level of .05	0.796	0.842	-	retain the null hypothesis
Education background in IT		0.0297	0.033	0.857	reject the null hypothesis
Working in IT department		0.054	0.089	0.0408	reject the null hypothesis

From the data in Table 5, it is clear that there is a difference between a background education in IT, working in IT departments and the information security culture because of sig<0.05. It can be concluded that the information security culture, through the knowledge and behavior level among each of the case study members, was affected by only two factors; if their background education was IT-related or if they were working in the IT department.

3.1.4 The STOPE dimensions statistical analysis: Based on Likert scale attitude analysis, the mean will be interpreted as Table 6 using an interval length of (0.75) starting after the cut off line of 64% described below, the distance between the categories should not be considered as equal [31].

Table 6. The Mean Interpretation

Average weight	Decision	State
4.75 - 5	Excellent	Applied almost all requirements and in an excellent state.
4.0- 4.74	Good	Applied most of the requirement s but still requires some improvement.
3.25 -3.99	Weak	Applied some requirement but requires major improvements
0-3.24	Poor	None or few requirements are applied and require key improvements.

To obtain an overall mean for each dimension, the scores from each dimension's items were averaged. Table 7 presents the summary of the results of each case study.

Table 7. The Summary of the Results Statistical Analysis of the STOPE Dimensions

Case A					
	S	T	O	P	E
Mean	3.70	4.17	4.10	4.04	3.94
Standard Error	0.10	0.08	0.12	0.11	0.10
Standard Deviation	0.45	0.38	0.49	0.41	0.38
Confidence Interval	{3.6-3.8}	{4.1-4.3}	{4.0-4.2}	{3.9-4.1}	{3.8-4.0}
Information Security Culture Mean				3.99	
Case B					
	S	T	O	P	E
Mean	3.26	3.83	3.39	3.51	3.54
Standard Error	0.16	0.15	0.20	0.18	0.16
Standard Deviation	0.42	0.38	0.44	0.34	0.25
Confidence Interval	{3.0-3.4}	{3.7-4.0}	{3.2-3.6}	{3.4-3.7}	{3.4-3.7}
Information Security Culture Mean				3.5	
Case C					

	S	T	O	P	E
Mean	3.71	3.79	3.87	3.64	3.97
Standard Error	0.10	0.08	0.13	0.10	0.10
Standard Deviation	0.57	0.37	0.63	0.44	0.39
Confidence Interval	{3.4-3.9}	{3.6-4.0}	{3.8-4.2}	{3.4-3.8}	{3.8-4.1}
Information Security Culture Mean				3.8	

The average mean of weighted means indicates the level of information security culture of each case study. The average mean of the three case studies was between 3.5 and 3.9 which indicates a weak level that requires attention and a need for improvements. In Case A, as the organization has invested heavily in information security, the mean of the T, O and P dimensions was above 4, indicating a good reflection on these variables. Yet more investment is needed, in strategy and in environmental factors. In Cases B and C, all mean values were below 4. In the three cases, the lowest average of weighted mean was in strategy dimension, revealing a critical weakness in strategy planning and implementation at the three organizations which, consequently, reflected upon the information culture level.

The small range of 95% confidence interval demonstrates an indication of the agreement between the organizations' members on the level of the information security culture, suggesting that the mean is adequately representative. The small standard deviation values indicate a small distance from the mean, showing precise results among the organization members and ensuring that the mean is a good representative for each data set. Additionally, a small standard error value points out that the sample means are similar to the population mean and, therefore, the sample is an accurate reflection of the population. Consequently, it can be concluded that the mean value can be used as a representative for the data set. In addition, the small values of the standard error suggest that the sample used was sufficiently representative of the population.

The perceptions of the five STOPE domains have been measured among employees through some statements. The agreement responses on each statement have been accumulated and analyzed based on percentage and presented in Table 9.

Table 8. The Perceptions of the Five STOPE Domains

Dimension	Case A	Case B	Case C
Strategy	92%	95%	95%
Technology	97%	93%	100%
Organization	95%	94%	98%
People	95%	94%	98%
Environment	95%	94%	98%

From the data, all STOPE dimensions have been positively perceived among the three case studies' members. More than 90% of the respondents were favorable for every dimension’s statements. Consequently, the five dimensions were considered important in creating an effective information security culture.

3.1.5 The Relationship between Knowledge and Behavior in Information Security Culture: It is important to evaluate the employees' information security knowledge level and their behavior in order to assess the information security culture in the organization. This will also help to discover any influencing factors and identify any development areas. Spearman's test is used to determine the degree of relationship and influence between the level of security knowledge and the employee's information security behavior and between knowledge and behavior on the level of the information security culture.

Spearman's rho test is a non-parametric measure to assess the degree of relationship between the two variables using a monotonic function [31]. In order to conclude a relationship between two variables using Spearman's test, the significance must be (≤0.05). Using SPSS data has been analyzed and yields the following results as presented in Table 10.

Table 9 The Analysis of the Relationship between Knowledge and Behavior

Variables	Correlation Coefficient	Sig.	Conclusion
Knowledge - employee behavior	0.705	0	Strong positive relationship
Knowledge - How employees perceive management behavior	0.808	0	Strong positive relationship
employee behavior -How employees perceive management behavior	0.551	0	Moderate positive relationship
Knowledge - ISC	.957	0	Strong positive relationship
employee behavior - ISC	.667	0	Moderate positive relationship
How employees perceive management behavior - ISC	0.863	0	Strong positive relationship

From the results, it can be concluded that there is a positive relationship between the levels of knowledge and how employees behave. A strong relationship is also shown between knowledge and the information security culture level. Therefore, for an effective information security culture, the level of knowledge will highly affect the information security behavior and culture and should be considered as a critical factor. Different methods of awareness- raising could be used to equip employees with information security knowledge. This supports the findings of [21].

3.1.6 Change Management: To analyze the relationship between change management and an information security culture, a correlation test using Spearman's test is used to determine the degree of relationship. The result of analysis is presented in Table 11.

Table 10. Analysis of Relationship between Change Management and Information Security Culture

Variables	Correlation Coefficient	Sig.	Conclusion
ISC, Change management beliefs	.294	0.04	Low relationship
ISC, Change management current application	.716	0	Moderate positive relationship

From the data, it is obvious that there is a small association between how employees perceive the role of change management and how it is applied or its effect on the information security culture level. Nevertheless, there is a positive relationship between the information security culture level and the application of change management principles. This emphasizes the role of change management in implementing an effective information security culture.

4.1 Interview Results

The interviews collected the required information to validate the questionnaire results and to investigate real organizations' efforts in information security from the people who are in charge of IT and information security inside these organizations. The interviews asked how information is secured and tried to identify any gaps between what is done and

what employees know. For the analysis, the interviewees' responses were compared to the questionnaire results for validation and to identify factors and relationships that affect the information security cultures. A summary of the findings of the semi-structured interviews for each case study is presented in the next section.

4.1.1 Case A: The interviewees confirmed that the organization has information security strategies that are aligned with its IT and business strategies. There are many efforts to inform the employees about the policies using presentations, emails and flyers, nevertheless, the questionnaire results show that many employees are unaware. The interviewees commented on this issue (the high rate of the employees' ignorance on the matter) to the lack of enforcement measures to motivate the employees to read and follow the policy. They have also suggested that policy should be written in a way that is easily digested by all employees, like summarized bullet points or even using graphics.

The IT team confirmed during the interviews that due to issues of authorization and department divisions, they were unable to deliver training for every department and were limited by having their awareness-raising courses approved by the top management. Nonetheless, the interviewees clarified that awareness-raising is continuous and is one of the IT governance department's priorities. This has been translated into good awareness level among employees, as the questionnaire results have shown. Yet, the employees' values and assumptions need more dedicated efforts if they are to be improved; the interview results line up with the questionnaire results in this regard. The interviewees believe that even the top management needs more awareness to improve their assumptions that information security is worth the cost. The interviewees mentioned that they need more authority from the top management to enforce the information security requirements and to raise awareness among employees.

According to the interviewees, rewards have been used only for attending the online awareness courses, which has raised the participation rate from 30% last year to 70% this year. The organization applies government information security-related laws and regulations. However, the questionnaire results pointed out that the majority of the employees are not aware of the related legislation and regulations. The interviewees admitted that there were no efforts to inform employees regarding such regulations.

4.1.2 Case B: The organization has an IT strategy that includes information security. However, the interviews confirmed that there were no awareness efforts in this regard. The low level of information security culture could be linked to the organization's minimal effort in setting security strategies. The organization has focused on the confidentiality and privacy of its clients' information, making good efforts to secure it. In addition, the results of the employees' questionnaire showed that the employees have taken this issue seriously. Consequently, we can conclude that the success of this issue could be linked to the culture created around the organization (i.e., that this issue is a priority) and the measures it has taken to ensure it.

The interviewees assumed that the level of the employees' information security artifacts, knowledge, and values were not sufficient to act securely. There is a lack of guidance in forming appropriate information security knowledge and behavior, risking the security of the organization's information assets. The interviewees confirmed the questionnaire results that the employees believe their management is committed to keeping information highly secure. Nevertheless, both the employees and the IT officers agree that the management has failed in training and awareness-raising. Moreover, the organization rarely delivers regular announcements and news regarding information security. The interviews revealed that no information security behavior monitoring is conducted in the organization; moreover, there is no written policy for reward and deterrence. The interviewees from the IT department were unaware of many related laws

and regulations; consequently, it is reasonable that the employees do not know about them either, as the questionnaire revealed.

4.1.3 Case C: According to the interviewees there was no efforts to raise awareness, which lead to around 50% (based on the questionnaire results) of the organization's members being unaware of the available policies. The organizational culture of Case C is IT aware, as the organization owns some large ICT companies. This has affected the culture of the organization when it comes to dealing with ICT. Nevertheless, the employees need greater awareness to ensure that they can behave securely. So far, no awareness-raising sessions have been conducted, yet the employees are informed of how to report an incident through calling a hotline or using the portal. The interviewees agreed that the employees are not yet well-informed about related polices, and enormous efforts using a variety of communication mediums are needed to deliver the message.

In regard to responsibility, according to the questionnaire, the employees feel accountable for their actions and accept being monitored in regard to information security. Until now, the employees' security behavior has not been a part of their performance measures, and even if their bad security behavior is tracked, there is no clear action taken against them (i.e., there is no reward or deterrence policy). That being said, the interviewees still believe that motivation through reward will have very positive effects. No training has been conducted in regard to preparedness. The reason, according to one interviewee, is that "*training was carried out only by HR, so the isolated departments issue makes it difficult*."

5. Discussion

The empirical study aims to evaluate and assess the level of information security culture in each case study. If the sample is valid, then the information security culture level determined in the assessment can be projected to the whole organization [1] which has been proved. In the three case studies, the use of IT technology in the organization is high to very high. In addition, all three cases possess valuable information assets. Organizations that have a high degree of usage of IT technology or hold valuable information assets will have a higher likelihood of being vulnerable to information-related misuse [32]. Consequently, in such organizations, it is crucial to establish an information security culture.

In general, the results show that more than 90% of the respondents positively perceived information security culture STOPE dimensions. The employees in the three cases believe that security strategies are important to create an effective information security environment. They also believe that the appropriate use of technical controls is vital to achieve information security. Moreover, the majority of the employees consider their organizations' security values, beliefs, assumptions, and knowledge to be important to shape employees' behavior. People dimension elements of preparedness, responsibility, and management have been positively received among the organizations' members. In addition, they felt positively toward applying environmental laws, rule, and regulations. This also reflects employees' positive perceptions toward the implementation of information security culture. In addition, information security specialists have strongly agreed on the importance and viability of information security cultures to their organizations.

The results of the empirical study indicate that the employees believe in the importance of information security for their organizations. This provides a very good foundation for the effective implementation of information security culture. In general, the majority of the employees in the three cases are unaware of their organizations' information security policies and strategies; further, they have no idea how to access them. Moreover, this study found that most of the managements' efforts are known only to those who work in

the IT department. This indicates a gap between the managements' efforts in planning security strategies and what the employees know and do, showing a need for more awareness-raising efforts. Information security strategies such as policies and guidelines should be convenient and accessible to all audience.

The three cases have good technical and personal support. On the downside, the employees are not well trained on how to efficiently use these technologies, increasing the risk of human error or reducing their effectiveness.

The appropriate artifacts, values, assumptions, and knowledge could be instilled through effective training, guidance, and awareness-raising. In general, most of the organizations' employees are aware of major information security concepts and believe in their importance. According to [4], this indicates a good foundation for information security culture at the individual level. Nevertheless, all three cases lacked effective awareness-raising initiatives, and employees were unaware of their information security responsibilities. The employees in the survey suggested different methods such as workshops, training, e-learning, email, newsletters, posters, screensavers, and flyers. Different communication methods could also open more chances for questions and answers to reduce gaps between what the organizations do and what the employees know.

The management's commitment plays a vital role in influencing the employees' good security behavior. It should set an example to the employees of how information security should be viewed [33]. Moreover, management should facilitate money, time, and other resources for information security learning and awareness-raising activities. Although reward and deterrence is very critical in motivating the employees to follow the correct information security practices and avoid bad security practices, no such policies exist in the three cases. Nevertheless, reward has been used successfully in one case to motivate the employees to attend short online awareness courses; it is believed that it had a positive effect, indicating its good influence in raising the level of information security culture.

In the environment dimension, the employees in general are not informed about related legislation, regulations, and standards. Therefore, there should be an extra effort to raise awareness about related laws and regulations to avoid any action that may cause the organization legal trouble. Moreover, respondents at three cases have agreed on the role of national culture in shaping the behavior of employees. A cultural analysis is very important to determine which assumptions need to be changed; thus, care should be taken in understanding cultural differences.

The five dimensions interact to create a secure environment for information assets. To exemplify, a strong password policy would be ineffective if the employees find the policy irrelevant because of their lack of awareness. With a proper information security culture, such a strategy should be accompanied by appropriate human preparedness and responsibility, such as training, reward and deterrence, communication, and so on. On the environment level, a cultural analysis should be performed to identify related assumptions that need to be changed. Any technology that might support the proper application of the policy would be a good investment. Therefore, we can conclude that the interaction of the five dimensions shapes an effective information security culture.

The employees' knowledge level could be linked to the level of awareness infinitives within the organization. The results revealed that information security knowledge highly affects information security behavior. This is similar to the findings of [21] that employees with no security knowledge or skills will not be able to act securely in the desired way.

The use of assessment instrument to evaluate information security culture has been used successfully in some studies such as [1, 21]. However, the goal of the assessment was to design awareness program. In this study, the assessment has shown to be comprehensive to evaluate the strategy, technology, organization, people and environment issues in order to provide broad list of recommendations.

Implementing an information security culture may require the employees to change some of their working practices to ensure information security. The results indicate the employees' willingness to do so in order to ensure information security. This would contribute to the successful implementation of information security cultures in the organizations. Moreover, there is a positive relationship between the information security culture and the application of change management principles. Thus, it can be concluded that change management principles are valuable in creating an effective information security culture, and the ISCF with the change management incorporated is practical and valid.

In short, the statistical analysis and the interview analysis confirmed that the assessment instrument was valid and applicable in assessing the cases' information security cultures. This was further assured by the agreement of information security specialists in the three cases on the developmental and positive areas identified in the assessment results. Other organizations can therefore use the assessment instrument to assess and cultivate an effective information security culture.

6. Conclusion

The ISCF provides a comprehensive structure for organizations to assess and cultivate an effective information security culture in order to protect information and IT systems from internal threats. The application of the ISCF to any organization would improve its employees' behavior by guiding their behavior, changing their values and assumptions based upon the outcome of the assessment, and providing all the necessary support. The results derived from the assessment can guide organizations with the issues that require improvement with regard to information security in order to direct them to focus only on these issues in order to save the costs.

As assessment instrument based on the ISCF was tested in an empirical study to evaluate and assess the level of information security culture in three case studies. Data was collected using a combination of employees' questionnaire and information security specialists' interviews. The findings show that the five STOPE dimensions interact to create a secure environment that guides the behavior and provides all the necessary support to achieve that. It also supports the important role of change management to ensure the employees' compliance and acceptance of the information security requirements.

Moreover, it can be noted that the level of sensitivity and criticality of the organization's business activities usually determines the level of efforts that management pays to protect the information assets. However, information security should be integrated in all business functions, regardless of the type of business activity. An information security culture takes care of raising employees' awareness of the correct methods for dealing with information assets. Moreover, it can be derived from the empirical study that the level of information security culture is strongly linked to the availability of an information security team and the authority given to that team.

The empirical study was useful in illustrating and validating the ISCF. It showed that the framework was valid and reliable in assessing the participating cases' information security culture. Therefore, other organizations can find it beneficial to utilize the framework to assess and cultivate their own information security culture.

This research could be expanded in the future to develop a statistical model that would identify the relationships between framework components. Furthermore, knowledge management could be integrated to develop a model that would assist organizations to cultivate the culture efficiently and predict how the information security culture could be improved.

References

[1] A. Da Veiga and J. Eloff, "A Framework and Assessment Instrument for Information Security Culture," *Computers & Security*, vol. 29, no. 2, (**2010)** March**,** pp. 196–207.
[2] K. Parsons, A. McCormac, M. Butavicius, and L. Ferguson, "Human Factors and Information Security: Individual, Culture and Security Environment," *Command, Control, Communications and Intelligence Division, Defenses Science and Technology Organization, Department of Defense, Australian Government*. Australia, **(2010)**.
[3] B. Schneier, "*Secrets and Lies: Digital Security in a Networked World"*, Indianapolis, IN: John Wiley & Sons, Inc., **(2000)**.
[4] A. Martins and J. Eloff, "Information security culture," in *Security in the information society*, Boston: Kluwer Academic Publishers, **(2002)**, pp. 203–214.
[5] T. Schlienger and S. Teufel, "Information security culture: from analysis to change," *South African Computer Journal*, vol. 31, **(2003),** pp. 46–52.
[6] A. Da Veiga, N. Martins, and J. Eloff, "Information security culture-validation of an assessment instrument," *South. African Business Review*, vol. 11, no. 1, **(2007),** pp. 146–166.
[7] A. AlHogail and A. Mirza, "Information security culture: a definition and a literature review," in *proceedings of IEEE World Congress On Computer Applications and Information Systems*, **(2014)**, pp. 1–7.
[8] S. Maynard, A. Ruighaver, and P. Chia, "Exploring Organisational Security Culture: Developing a comprehensive research model.," *Proceedings of IS ONE World Conf. USA*, **(2002),** pp. 1–13.
[9] S. Alfawaz, K. Nelson, and K. Mohannak, "Information security culture: a behaviour compliance conceptual framework," *Proceedings of 8th Australasian Information Security Conference (AISC 2010)*, **(2010)**, pp. 47–55.
[10] O. Zakaria, Gani. A., M. Nor, and N. Anuar, "Reengineering information Security culture formulation through management perspective," *Proceedings of the International Conference on Electrical Engineering and Informatics, Institute Teknologi , June 17-19*, **(2007)**, pp. 638–641.
[11] A. Ruighaver, S. Maynard, and S. Chang, "Organisational security culture: Extending the end-user perspective," *Computers & Security*, vol. 26, no. 1, **(2007),** February, pp. 56–62.
[12] O. Zakaria, "Internalisation of Information Security Culture amongst Employees through Basic Security Knowledge," in *IFIP International Federation for Information Processing, Volume 201, Security and Privacy in Dynamic Environments*, S. Fischer-Hubner, K. Rannenberg, L. Yngstrom, and S. Lindskog, Eds. Boston: Springer, **(2006)**, pp. 437–441.
[13] D. Bess, "Understanding Information Security Culture for Strategic Use: A Case Study," *Proceedings of AMCIS 2009*, **(2009)**, paper 219.
[14] S. Furnell and K. Thomson, "From culture to disobedience: Recognising the varying user acceptance of IT security," *ComputerFraud Security*, vol. 2009, no. 2, **(2009)** February**,** pp. 5–10.
[15] K. Knapp, T. Marshall, R. Rainer, and F. Ford, "Information security: management's effect on culture and policy," *Information Management & Computers Security*, vol. 14, no. 1, **(2006),** pp. 24–36.
[16] S. Dojkovski, S. Lichtenstein, and M. Warren, "Enabling information security culture : influences and challenges for Australian SMEs," *Proceedings of the 21st Australasian Conference on Information Systems, ACIS*, **(2010)**, p. 61.
[17] A. AlHogail and A. Mirza, "A Proposal of an Organizational Information Security Culture Framework," in *Proceeding of the 8th IEEE International Conference on Information, Communication Technology and Systems ICTS 2014*, **(2014)**.
[18] P. Chia, S. Maynard, and A. Ruighaver, "Understanding organizational security culture," in *Information systems: the challenges of theory and practice*, Hunter M. and Dhanda K, Eds. Las Vegas, USA: Information Institute, **(2003)**, pp. 335–365.
[19] S. Chang and C. Lin, "Exploring organizational culture for information security management," *Industrial Management & Data Systems*, vol. 107, no. 3, **(2007),** pp. 438–458.
[20] J. Lim, S. Chang, S. Maynard, and A. Ahmad, "Exploring the Relationship between Organizational Culture and Information Security Culture," in *Proceedings of the 7th Australian Information Security Management Conference*, **(2009),** pp. 88–79.
[21] J. Van Niekerk and R. Von Solms, "Information security culture: A management perspective," *Computers & Security*, vol. 29, no. 4, **(2010)** June, pp. 476–486.
[22] M. Alnatheer, T. Chan, and K. Nelson, "Understanding And Measuring Information Security Culture," in *Proceedings of the Pacific Asia Conference on Information Systems PACIS 2012*, **(2012)**, p. paper 144.
[23] I. Okere, J. van Niekerk, and M. Carroll, "Assessing Information Security Culture: A Critical Analysis of Current Approaches," in *in the proceedings of IEEE conference on Information Security for South Africa (ISSA)*, **(2012)**, pp. 1 – 8.
[24] T. Schlienger and S. Teufel, "Tool supported management of information security culture," *Proceedings of IFIP Advances in Information and Communication Technology*, **(2005)**, pp. 65–77.
[25] A. AlHogail, "Design and Validation of Information Security Culture Framework," *Computers in Human Behavaior*, vol. 49, no. August, **(2015),** pp. 567–575.

[26] A. AlHogail and A. Mirza, "A framework of Information Security Culture Change," *Journal of Theoretical and Applied Information Technology*, vol. 64, no. 2, **(2014),** pp. 540–549.
[27] L. Ngo, W. Zhou, and M. Warren, "Understanding Transition towards Information Security Culture Change.," in *Proceeding of the 3rd Australian Computer, Network & Information Forensics Conference, Edith Cowan University, School of Computer and Information Science*, **(2005)**, pp. 67–73.
[28] J. Bennett, "Effectiveness Of Using A Change Management Approach To Convey The Benefits Of An Information Security Implementation To Technology Users, Unpublished PhD thesis," Capella University, **(2012)**.
[29] O. Zakaria, "Understanding Challenges of Information Security Culture: A Methodological Issue.," in *the 2nd Australian Information Security Management Conference, Securing the Future*, **(2004)**, pp. 83–93.
[30] D. Hooper, J. Coughlan, and M. Mullen, "Structural Equation Modelling : Guidelines for Determining Model Fit," *The Electronic Journal of Business Research Methods*, vol. 6, no. 1, **(2008),** pp. 53–60.
[31] J. Pallant, *SPSS Survival Manual: A Step by Step Guide to Data Analysis using SPSS for Windows*. Berkshire, England: Open University Press., **(2010)**.
[32] A. Martins, "Information Security Culture," Unpublished PhD thesis, Rand Afrikaans University, **(2002)**.
[33] A. Martins and J. Eloff, "Assessing Information Security Culture.," in *Proceedings of the ISSA 2002 Information for Security for South-Africa 2nd Annual Conference, 10-12 July 2002*, **(2002)**, pp. 1–14.

