© Universiti Tun Hussein Onn Malaysia Publisher's Office

IJIE

http://penerbit.uthm.edu.my/ojs/index.php/ijie
ISSN : 2229-838X e-ISSN : 2600-7916

The International Journal of Integrated Engineering

Information Security Culture Concept towards Information Security Compliance: A Comparison between IT and Non-IT Professionals

Akhyari Nasir[1*], Ruzaini Abdullah Arshah[2], Mohd Rashid Ab Hamid[3], Syahrul Fahmy[4]

[1]Faculty of Computer, Media and Technology Management,
University College TATI, Terengganu, MALAYSIA

[2]Faculty of Computing,
Universiti Malaysia Pahang, Pahang, MALAYSIA

[3]Faculty of Industrial Management,
Universiti Malaysia Pahang, Pahang, MALAYSIA

[4]Big Data Institute,
University College TATI, Terengganu, MALAYSIA

*Corresponding Author

DOI: https://doi.org/10.30880/ijie.2022.14.03.017
Received 14 January 2022; Accepted 04 June 2022; Available online 20 June 2022

Abstract: This paper examines the factors determining a positive Information Security Culture (ISC) concept and the influence of ISC towards ISP compliance intention (INT) between IT and non-IT professionals in Malaysian public universities. Partial least square structural equation modelling, using PLS MGA, is used to assess the measurement and structural models, and to compare the results between the two groups. Results indicate all factors have significant contribution towards ISC in both groups, with two out of seven ISC factors have significant differences. This study has revealed that although both groups have the same ISC factors, IT and non-IT professionals have significant difference in terms of believe that Top Management Commitment and Information Security Knowledge are required for implementing a positive ISC. In addition, there is a significant difference between these two groups in terms of the influence of ISC towards ISP compliance intention. ISC has less influence towards INT for Non-IT professionals compared to IT professionals within the same ISC. These empirical findings would benefit in formulating better security strategies by providing appropriate efforts for different groups of employees in the organizations. This study also provides a total cyber security solution for improving information security culture and employees' compliance towards Information Security Policy.

Keywords: Information security culture, information security compliance, multi-group analysis

1. Introduction

Limitations in technical and technological controls have pushed organizations to cultivating and establishing a positive *Information Security Culture* (ISC) in managing *Information Security*. Although there are numerous studies conducted to assist organizations in formulating ISC strategies, majority focus on a particular type of organization, in addition to the

*Corresponding author: akhyari@uctati.edu.my

lack of focus the type of employees in the organization. ISC is an important aspect since it could be cultivated based on beliefs and perceptions, and thus, its knowledge would benefit organizations in implementing an effective ISC strategies amongst different type of employees.

Employees in an organization can be broadly classified into two main groups, namely *IT* and *non-IT professionals*. The first group refers to "*employee who has formal education in IT such as computer science, computer networking, business computing and other IT-related fields*". This group typically consists of programmers, network engineers, web developers, data analyst and other designations that directly utilize the use of IT technologies. The latter group refers to "*employees who do not have formal IT education with jobs that do not depend heavily on IT technologies"*. This group consists of human resource management, accounting, finance and others. In an ideal world, IT professionals would have stronger ISC and ISP compliance because they have acquired more skills, understanding and awareness (of information security). However, there is lack of empirical evidence to confirm this in addition to no clear indication on how ISC would influence both groups towards ISP compliance. This paper aims to investigate this issue and presents empirical findings on the relationships.

2. Conceptual Model and Hypotheses Development

Information Security Culture (ISC) is a culture that emphasizes on the security of information assets by improving employees' information security behavior [1]. ISC should be cultivated to guide and influence employees' security behavior to comply with *Information Security Policy* (ISP) [2]. ISC implementation in organizations could improve employees' security behavior [3].

Approaches for ISC implementation differs greatly based on the definitions of ISC concept used [4]. There are, however, common factors and dimensions found in literature. Reference [1] has defined and validated ISC as a concept that consist of seven factors, which are PCM, RM, SETA, TMC, MON, ISK and ISKS. Although these factors are significant in influencing ISC, there is no clear indication on how these factors would influence ISP compliance intention for different types of employees.

There are various types of employees in a typical organization with different knowledge and skills in IT. According to [5], different background of professions may offer different effect of security culture including their beliefs on what constitutes information security and the likelihood of their compliance. Reference [6] found significant variations in security culture across professions of *Information Systems*, *Marketing*, *Human Resource* and *Accounting*. Interestingly, it is also revealed that *Accounting* has a strong security culture than *Information Systems* employees and *Information Systems* employees have weaker intention to comply with ISP. Although these are crucial findings, there is still no indication on the factors that contribute to positive ISC based on different types of employees and towards SP compliance.

The conceptualization of ISC as a concept can be measured by various factors [1][7][9] and these factors can be utilized in ISC implementation strategies. However, there is still lack of studies that highlight the influence of employee types to ISC. Based on the ISC concepts in [1], it is hypothesized that

- H1: There is a significant difference on the influence of PCM towards ISC between IT and Non-IT professionals.
- H2: There is a significant difference on the influence of RM towards ISC between IT and Non-IT professionals.
- H3: There is a significant difference on the influence of SETA towards ISC between IT and Non-IT professionals.
- H4: There is a significant difference on the influence of TMC towards ISC between IT and Non-IT professionals.
- H5: There is a significant difference on the influence of MON towards ISC between IT and Non-IT professionals.
- H6: There is a significant difference on the influence of ISK towards ISC between IT and Non-IT professionals.
- H7: There is a significant difference on the influence of ISKS towards ISC between IT and Non-IT professionals.

Although there are findings confirming that ISC will influence ISP compliance behavior such as [1][8][9][10], there is little knowledge on this relationship with regards to a particular group of employees. The knowledge on how ISC effects the security behavior of a particular group of employees will provide clearer understanding on how to establish ISC in the organization.

ISC is not only dependent on organizational type, but also on employees' professions in the organization [5-6]. In an organization, there are various types of employees such as accountants, marketing and information system professionals who use information systems in their daily works. Reference [5] have proved that different types of employees have different ISC. In addition, there are also studies proving ISC influence ISP compliance [1][8][9]. Since this study conceptualizes ISC based on the concepts of *Organizational Culture* [11][12], ISC is referred to a sub-culture that depends on various professions in the organization. According to [12], organizations are "*cultural units that have within them powerful subcultures based on occupations and common histories*".

Since ISC is a subculture of OC, ISC could influence the security behavior of employees with regards to ISP compliance. Based on the arguments above, it is also hypothesized that:

- H8: There is a significant difference on the influence of ISC towards intention to comply with ISP between IT- and Non-IT professionals.

3. Methodology

Two groups of employees were analyzed to determine ISC and how ISC influences the intention to comply with ISP using *Multi-Group Analysis* (MGA). The population were the employees at Malaysian public universities, categorized to IT and non-IT professionals. Data were collected through online questionnaire for the duration of two weeks involving 14 public universities. This study used the same constructs and measurements in [1].

The questionnaire was designed using Google form and all responses were stored in Google drive. The invitations to participate were sent to respondents via e-mail with the survey's questionnaires attached. The survey consists of seven sections: demographics, ISC factors, attitudes, normative belief, self-efficacy and intention to comply with ISP. The sample includes 113 responses from IT professionals and 113 responses from non-IT professionals.

SmartPLS 3 was used to estimate the model and MGA. PLS-SEM is a multivariate analysis approach used to estimate path models with latent variables and to carry out multigroup analyses. The total number of samples (113) for both IT and non-IT professionals met the requirements of PLS-SEM. According to [13], the minimum sample for PLS-SEM analysis is based on the maximum number of arrowheads pointing at a particular construct in the measurement model. As the research model has 7 arrowheads pointing at ISC, the minimum sample for this study is calculated to be 70 (70 x 10). Using the G*power program [14] for minimum sample size, 103 observations were needed to achieve a statistical power of 80% for a medium effect size of 0.15 with a 5% probability of error. Reference [13] suggests following more elaborative recommendations such as those provided by [15] that take statistical power and effect sizes into account. Therefore, 113 samples for both groups are considered enough in this study.

4. Results and Analysis

4.1 Descriptive Analysis

Table 1 shows the profile of respondents classified into IT and non-IT professionals. The results show that 49.6% of IT professionals were male and 50.4% were female, while 35.4% of non-IT professionals were male and 64.6% female. In terms of age, most of the respondents were in in the category of 25 - 34 years and 35 - 44 years old respectively. 32.7% and 28.3% of the respondents holds a PhD with most of them holding at least a diploma. Finally, most of the respondent from both groups have 5 – 20 years of experience.

Table 1 - Profile of respondents

Characteristics	Frequency		Percentage (%)	
	IT Professionals	Non-IT Professionals	IT Professionals	Non-IT Professionals
Gender				
Male	56	40	49.6	35.4
Female	57	73	50.4	64.6
Age				
25 - 34	30	45	26.5	39.8
35 - 44	64	46	56.6	40.7
45 - 54	19	18	16.8	15.9
55 and above	0	4	0	3.5
Level of education				
PhD	37	32	32.7	28.3
Master	28	36	24.8	31.9
Degree	12	18	10.6	15.9
Diploma	29	17	25.7	15.0
STPM/College	5	3	4.4	2.7
SPM	2	7	1.8	6.2
Experience				
Less than 2 Years	7	12	6.2	10.6
2 to 5 Years	14	19	12.4	16.8
5 to 10 Years	28	37	24.8	32.7
10 to 20 Years	56	27	49.6	23.9
20 Years and over	8	18	7.1	15.9

4.2 Model Assessment using PLS-SEM

4.2.1 Assessment of measurement model and invariance measurement across two groups

In order to assess the model for IT and non-IT professionals and to compare the results of the estimated path coefficients, a three-stage approach was employed: assessment of measurement models, assessment of structural models, and MGA. Since the ISC used in this study was conceptualized as second-order, the measurement model assessments involved two aspects, first order and second order constructs. Table 2 shows the assessment of measurement model for first order.

Table 2 - Assessment of the Measurement model (First order)

Construct	Item	Loading		AVE		CR	
		IT	Non-IT	IT	Non-IT	IT	Non-IT
PCM	PCM1	0.772	0.816	0.712	0.743	0.908	0.92
	PCM2	0.916	0.916				
	PCM3	0.898	0.898				
	PCM4	0.778	0.778				
RM	RM1	0.878	0.872	0.810	0.793	0.927	0.92
	RM2	0.925	0.887				
	RM3						
	RM4	0.896	0.911				
SETA	SETA1	0.927	0.796	0.865	0.706	0.962	0.906
	SETA2	0.956	0.891				
	SETA3	0.916	0.825				
	SETA4	0.922	0.846				
TMC	TMC1	0.889	0.939	0.853	0.899	0.959	0.973
	TMC2	0.959	0.964				
	TMC3	0.953	0.970				
	TMC4	0.891	0.918				
MON	MON1	0.861	0.840	0.794	0.751	0.939	0.923
	MON2	0.892	0.852				
	MON3	0.890	0.916				
	MON4	0.920	0.855				
ISK	ISK1	0.862	0.856	0.786	0.757	0.948	0.94
	ISK2	0.910	0.898				
	ISK3	0.883	0.863				
	ISK4	0.902	0.882				
	ISK5	0.886	0.851				
ISKS	ISKS1	0.831	0.867	0.758	0.657	0.94	0.905
	ISKS2	0.880	0.817				
	ISKS3	0.923	0.887				
	ISKS4	0.904	0.789				
	ISKS5	0.812	0.675				
INT	INT1	0.947	0.954	0.918	0.743	0.978	0.971
	INT2	0.972	0.910				
	INT3	0.950	0.959				
	INT	0.963	0.958				

*Item RM3 was removed due to low factor loading

The model's reliability was assessed by examining the loadings. Most of the indicator loadings were higher than the acceptable value of 0.7 [17] except for ISKS5. However, CR and AVE for all constructs met the acceptable value of 0.7 and 0.5 [18] respectively. Therefore, the measurement model for both data groups were reliable and item ISKS5 was not removed. Results of AVE and CR for both data groups also indicate that the convergent validity and discriminant validity were established.

The second order construct was assessed using a repeated indicator approach. The higher-order construct in this study, ISC, was created using the indicators of lower-order constructs, namely PCM, RM, SETA, TMC, MON, ISK and ISKS. A bootstrapping procedure was employed using 5000 sub-samples to assess the significance of formative indicators. Table 3 shows the assessment of ISC as second-order construct. The indicators' weights were above the value of 0.10 as recommended by [19]. All the weights of formative indicators also have significant t-values. This provides an empirical support to retain all the indicators [17]. These results suggest that all dimensions were relevant and significant in contributing to the underlying concept of ISC [20][21].

Table 3 - Testing of significance of weights

Relationship	Weight/Original Sample (O)		t-value (|O/STDEV|)		p-values	
	IT	Non-IT	IT	Non-IT	IT	Non-IT
PCM -> ISC	0.142	0.449	***11.248	***5.409	p<0.001	p<0.001
RM -> ISC	0.129	0.161	***15.746	***11.73	p<0.001	p<0.001
SETA -> ISC	0.164	0.145	***14.973	***13.223	p<0.001	p<0.001
TMC -> ISC	0.183	0.165	***17.827	***11.102	p<0.001	p<0.001
MON -> ISC	0.155	0.230	***12.722	***15.078	p<0.001	p<0.001
ISK -> ISC	0.201	0.122	***19.924	***6.073	p<0.001	p<0.001
ISKS -> ISC	0.200	0.239	***15.526	***20.242	p<0.001	p<0.001

Note: Critical t values ***2.33 (significance level= 1%)

Table 4 shows the confidence intervals and p-values for both models. It provides additional evidence regarding the significance of weights as 0 did not occur between the higher and lower values of the confidence intervals.

Table 4 - Confidence intervals

Second-Order Construct	Formative Indicators	p-value		Confidence Interval		Significance (p≤0.05)?	
		IT	Non-IT	IT	Non-IT	IT	Non-IT
ISC	PCM -> ISC	p<0.001	p<0.001	0.116, 0.166	0.136, 0.190	Yes	Yes
	RM -> ISC	p<0.001	p<0.001	0.114, 0.146	0.126, 0.169	Yes	Yes
	SETA -> ISC	p<0.001	p<0.001	0.144, 0.187	0.135, 0.193	Yes	Yes
	TMC -> ISC	p<0.001	p<0.001	0.165, 0.206	0.203, 0.264	Yes	Yes
	MON -> ISC	p<0.001	p<0.001	0.132, 0.179	0.079, 0.157	Yes	Yes
	ISK -> ISC	p<0.001	p<0.001	0.183, 0.224	0.219, 0.266	Yes	Yes
	ISKS -> ISC	p<0.001	p<0.001	0.176, 0.227	0.134, 0.210	Yes	Yes

To determine the reliability of ISC as a formative construct, the VIF value for each construct was examined by assessing the collinearity of indicators. Table 5 shows that VIF values for each construct is below than 5 for both IT and non-IT models, indicating collinearity of the formative constructs [13][18]. This also suggests that each dimension represents a distinct aspect of ISC in contributing to the overall concept of ISC.

Table 5 - VIF values

Construct	VIF value	
	IT	Non-IT
PCM	2.532	1.903
RM	3.989	2.567
SETA	4.04	3.255
TMC	3.476	3.578
MON	2.513	1.769
ISK	4.84	4.746
ISKS	2.37	1.582

4.2.2 Assessment of the Structural Model and Multi Group Analysis

Prior to testing the structural model, the invariance of the measurement items was examined to check if item measurements differed across the two groups. According to [13], at least two items should not differ in the measurement items of each construct. Since this study used the same measurement items for all constructs, these criteria was met and the structural model can be further tested.

The R^2 of the two structural models revealed that the values are at a satisfactory level as shown in Figures 1 and 2. For IT professionals, the path coefficient of the relationship between ISC and INT is significantly strong (beta = 0.672) at $p<0.01$, and 45.2% variance in ISP compliance intention. For non-IT professionals, the relationship between ISC and INT is weaker but still significant at $p<0.01$, and 20.1% of variance in ISP compliance intention. These results indicate that ISC has significant influence towards ISP compliance intention of employees regardless of IT background.

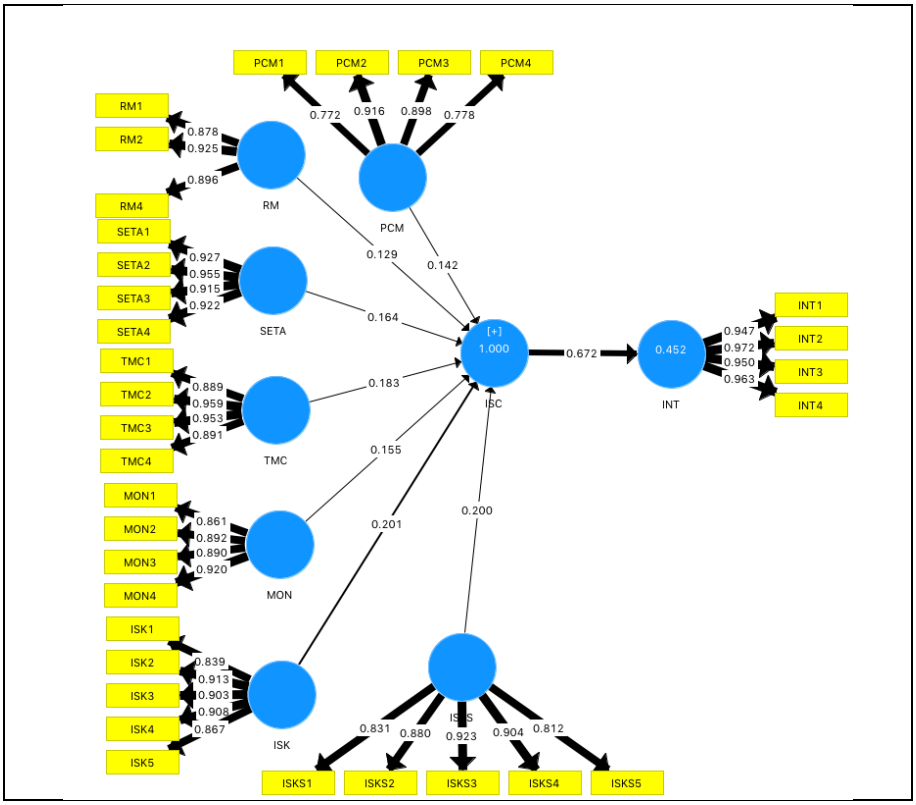

Fig. 1 - Results of structural model (IT professionals)

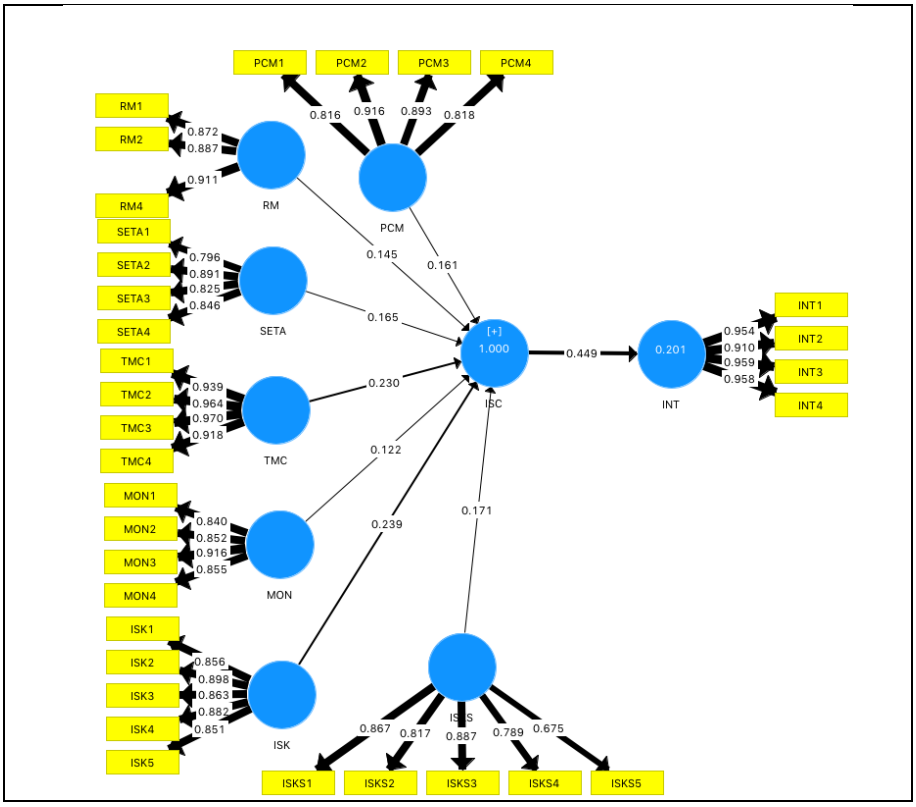

Fig. 2 - Results of Structural Model (Non-IT Professionals)

In order to compare whether there are differences between IT and non-IT groups in terms of factors influencing ISC and ISC relationship with INT, PLS MGA was performed. PLS-based MGA is suggested over the traditional t-test method for examining the differences among path coefficients. Furthermore, MGA has no restriction over normality distribution.

Table 6 shows the hypothesized weight and path coefficient and their bootstrap values (t-value). There is no significant difference between the groups for factors influencing ISC and therefore, H1, H2, H3, H5 and H7 were not supported.

Table 6 - Path weight comparisons (IT professionals and non-IT professionals)

Hypotheses	Weight/Path	IT	Non-IT	CI (IT)	CI (Non-IT)	Path coefficient Difference	*P*-value Henseler's MGA	*P*-value Permutation test	Supported
H1	PCM -> ISC	0.142	0.161	0.118, 0.167	0.136, 0.190	-0.020	0.284	0.187	No/No
H2	RM -> ISC	0.129	0.145	0.115, 0.147	0.126, 0.169	-0.016	0.243	0.369	No/No
H3	SETA -> ISC	0.164	0.165	0.145, 0.188	0.137, 0.195	-0.002	0.917	0.902	No/No
H4	TMC -> ISC	0.183	0.230	0.165, 0.205	0.204, 0.265	-0.047	0.008***	0.002***	Yes/Yes
H5	MON -> ISC	0.155	0.122	0.132, 0.180	0.076, 0.157	0.032	0.152	0.335	No/No
H6	ISK -> ISC	0.201	0.239	0.182, 0.221	0.219, 0.266	-0.038	0.011**	0.005***	Yes/Yes

H7	ISKS -> ISC	0.200	0.171	0.177, 0.277	0.134, 0.213	0.029	0.214	0.141	No/No
H8	ISC -> INT	0.672	0.449	0.522, 0.783	0.249, 0.587	0.224	0.031**	0.028**	Yes/Yes

However, there are significant differences for TMC and ISK between the groups. ISC for non-IT professionals are more influenced by TMC and ISK compared to IT professionals. P-value MGA revealed that the significant value is at $p<0.01$ for TMC and $p<0.05$ for ISK. The P value of Permutation test was also significant at $p<0.01$ for both TMC and ISK. Therefore, H3 and H6 were supported. This indicates that although all factors are significant in contributing to the concept of ISC for both groups, some factors are significantly different between IT and non-IT professionals. These results are consistent with [6]. This suggests that while there are same ISC factors for all employees, there are significant differences on the level and magnitude for each factors.

As for the relationship between ISC and INT, the analysis found that there is significant difference between the groups at $p<0.05$ for both MGA and Permutation test. This suggest that the influence of ISC towards ISP compliance intention is different between IT and non-IT professionals where the former are more influenced by ISC that the latter. Therefore, H8 is supported. Interestingly, this result is not consistent with findings by [5-6]. According to [5-6], IT professionals have lower compliance compared to other professionals. One explanation for this finding is the different ISC concept used.

5. Discussion

Despite different IT background and skills, there is no major differences noticed on the factors that contribute to positive ISC between IT and non-IT professionals. This study found that PCM, RM, SETA, TMC, MON, ISK and ISKS have significant influence towards ISC for both groups. This indicates that all seven factors are important in cultivating ISC in the organization regardless of the employees' IT background. However, since non-IT professionals have less knowledge, awareness and skills in IT, they are found to be more influenced by most of the factors compared to IT professionals. To some extent, there are significant differences on factors such as ISK and TMC. Compared to IT, non-IT professional have stronger beliefs that ISK and TMC are important for a positive ISC in the organization. Non-IT professionals are more influenced by ISC if they have more knowledge of information security and their leaders show a good commitment of ISC efforts. While this consistent with [5] that found different professions have different effect of security culture, these findings revealed more specific results on the particular ISC factors involved.

These findings suggest that ISC needs to be improved among non-IT professionals. Due to the limited cybersecurity skills of non-IT professionals, they would be "*the weakest link*" in the cybersecurity chain [16] and as such, needs to be trained and provided with adequate knowledge of information security. In addition, the management should demonstrate commitment to information security in order to boost the beliefs of non-IT professionals that ISC is an important aspect in the organization. With these efforts, it is believed that information security culture and the ISP compliance will improve effectively in the organizations. Since human behavior is determined by culture [22], improvement in ISC would improve the ISP compliance behavior. It would give a significant impact to sustainable development goals in terms of secure and conducive work environment that finally would provide platforms for a decent work and economic growth.

6. Limitation and Future Work

The sample in this study are employees in Malaysian public universities and as such, would limit the generalization of the results to other government agencies or for-profit organizations. For a more comprehensive and generalizable results, an extensive list of organizations should be included. Future investigations into this relationship should also include *behavioral theories* such as the *Theory of Planned* behavior and *Protection Motivation Theory* to better understand the relationships based on professions.

7. Conclusion

From the perspectives of IT and non-IT professionals, ISC is a concept that consist of seven dimensions. Non-IT professionals have stronger belief that ISC is contributed by TMC and ISK. In the same ISC, non-IT professionals have less intention to comply with ISP compared to IT professionals. This study has proven that ISC is a multi-dimensional concept that needs to be properly implemented based on the type of employees in the organization to improve ISP compliance behavior. Since this study has conceptualized ISC based on seven dimensions, it provides a new perspective on the relationship between ISC and ISP compliance for different group of professions in the organizations.

Acknowledgment

The authors would like to acknowledge the University Collee TATI for sponsoring this study (GPJP 1/2020 UCTATI [9001-2006]).

References

[1] Nasir, A., Abdullah Arshah, R., & Ab Hamid, M. R. (2019). A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions. Information Security Journal, 28(3), 55–80. https://doi.org/10.1080/19393555.2019.1643956

[2] Padayachee, K. (2012). Taxonomy of compliant information security behavior. Computers and Security, 31(5), 673–680. https://doi.org/10.1016/j.cose.2012.04.004

[3] von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371–376. https://doi.org/10.1016/j.cose.2004.05.002

[4] Nasir, A., Arshah, R. A., Hamid, M. R. A., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. Journal of Information Security and Applications, 44, 12–22. https://doi.org/10.1016/j.jisa.2018.11.003

[5] Ramachandran, S., Rao, S. V., & Goles, T. (2008). Information security cultures of four professions: A comparative study. Proceedings of the Annual Hawaii International Conference on System Sciences. https://doi.org/10.1109/HICSS.2008.201

[6] Ramachandran, S., Rao, C., Goles, T., Dhillon, G., & Rao, V. S. (2013). Variations in Information Security Cultures across Professions: A Qualitative Study. Communications of the Association for Information Systems, 33(11), 163–204.

[7] Akhyari, N., & Ruzaini, A. A. (2016). Information Security Culture Dimensions in Information Security Policy Compliance Study: A Review. Proceedings of the 3rd International Conference on Computational Science and Technology (ICCST2016) in: Advanced Science Letters (ISSN: 1936-6612 (Print): EISSN: 1936-7317 (Online)), American Scientific Publishers (Accepted) ISI/Scopus, IF 1.253.

[8] D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. Information Management & Computer Security, 22(5), 474–489. https://doi.org/10.1108/IMCS-08-2013-0057

[9] Alkalbani, A., Deng, H., & Kam, B. (2015). Organisational Security Culture and Information Security Compliance For E-Government Development: The Moderating Effect of Social Pressure. Pacific Asia Conference on Information System (PACIS 2015).

[10] D'Arcy, J., & Greene, G. (2009). The Multifaceted Nature of Security Culture and Its Influence on End User Behavior. IFIP TC 8 International Workshop on Information Systems Security Research, 145–157.

[11] Niekerk, J. Van, & Solms, R. Von. (2006). Understanding Information Security Culture: A Conceptual Framework. Proceedings of ISSA 2006, 1–10.

[12] Schein, E. H. (2004). Organizational Culture and Leadership. Leadership, 7, 437. https://doi.org/10.1080/09595230802089917

[13] Hair, Joseph F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2014). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). In Long Range Planning (Vol. 46, Issues 1–2). https://doi.org/10.1016/j.lrp.2013.01.002

[14] Faul, F., Erdfelder, E., Buchner, A., & Lang, A. (2009). Statistical power analyses using G * Power 3 . 1 : Behavior Research Methods, 41(4), 1149–1160. https://doi.org/10.3758/BRM.41.4.1149

[15] Cohen, J. (1992). A power primer. Psychological Bulletin, 112(1), 155–159. https://doi.org/10.1037/0033-2909.112.1.155

[16] Carlton, M., & Levy, Y. (2015). Expert assessment of the top platform independent cybersecurity skills for non-IT professionals. Conference Proceedings - IEEE SOUTHEASTCON, 2015-June(June), 1–6. https://doi.org/10.1109/SECON.2015.7132932

[17] Hair, Joe F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet. The Journal of Marketing Theory and Practice, 19(2), 139–152. https://doi.org/10.2753/MTP1069-6679190202

[18] Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017). A primer on partial least squares structural equation modeling (PLS-SEM). Sage Publications.

[19] Lohmöller, J.-B. (1989). Latent Variable Path Modeling with Partial Least Squares. In Physica-Verlag, Heidelberg. https://doi.org/10.1007/978-3-642-52512-4_5

[20] Becker, J.-M., Klein, K., & Wetzels, M. (2012). Hierarchical Latent Variable Models in PLS-SEM: Guidelines for Using Reflective-Formative Type Models. Long Range Planning, 45(5–6), 359–394. https://doi.org/10.1016/j.lrp.2012.10.001

[21] Wetzels, M., Odekerken-Schröder, G., & Oppen, C. van. (2009). Using Pls Path Modeling for Assessing Hierarchical Construct Models : Guidelines and Empirical Illustration. MIS Quarterly, 33(1), 177–195. https://doi.org/Article

[22] Wiley, A., Mccormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. Computers & Security, 88, 101640. https://doi.org/10.1016/j.cose.2019.101640