International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12– No.33, September 2020 – www.ijais.org

A Theoretical Model for Information Security Policy Compliance Culture

Erick. O. Otieno
University of Nairobi

Agnes N. Wausi
University of Nairobi

Andrew M. Kahonge
University of Nairobi

ABSTRACT
This paper provides a different perspective on information security management by investigating information security policy compliance culture. The results in this paper are drawn from the thesis in which the researchers sought to address the gap by employing a mixed method in developing a theoretical model. The resulting theoretical model was then subjected to a validation process through Confirmatory Factor Analysis using JASP-analytical software. Hypotheses were derived from the emergent model that formed the basis of developing the questionnaire instrument. This paper, therefore, presents the results of the validation process and synthesizes the final theoretical model constructs that explain information security policy compliance culture. The results validated the theoretical model with factor loading all above (0.5) thresholds and significance of ($p < 0.001$). The resulting model showed that information security managers should consider organizational, behavioral, and external factors while developing information security policy compliance culture strategies.

Keywords
Confirmatory Factor Analysis, information security policy compliance, information security management, theoretical model, and information security policy compliance culture

1. INTRODUCTION
Information security management is increasingly becoming an issue that cannot be put into the back banner. This is not a surprise especially with the increased investment in information technology to accomplish virtually all aspects of many commercial and domestic needs. The quest to employ information systems to address all business functions means that more is also needed to safeguard the underlying information, data, and infrastructure. Policies, processes, and controls then become highly necessary. However, policies, processes, and controls can only be as effective as the compliance rates of target audiences. It has been suggested in various quarters that the weakest point of information security is the users who use the information systems assets. This, therefore, raises the aspect of compliance as an important component of an effective information security management strategy. Creating strong and robust information security policies, processes, and controls without a strategy to enhance compliance would not provide a sustainable solution. The pertinent question, therefore, is whether a compliance culture perspective is a future to sustainable information security.

It is from this premise that the researchers embarked on a study that aimed to seek the factors that influence information security policy compliance culture. There exist several extant studies that have provided very useful insights on information security mitigation through robust models. However, little has been covered in terms of information security policy compliance culture. The thesis, which this paper is drawn from, sought to expand this horizon by employing a mixed method in developing a theoretical model. The researchers explored the factors that contribute to information security policy compliance culture. The emergent relationships were then validating and synthesized to a theoretical model. This was accomplished by adopting a grounded theory approach to generate the theoretical model. The principle of rigor was enforced to ensure that the theoretical model was grounded on data. The resulting theoretical model was then subjected to a validation process through Confirmatory Factor Analysis using JASP-analytical software. Hypotheses were derived from the emergent model that formed the basis of developing the questionnaire instrument. This paper, therefore, presents the results of the validation process and synthesizes the final theoretical model constructs that explain information security policy compliance culture.

2. LITERATURE REVIEW
A study by [1] identified factors that could persuade an employee to have positive compliant behavior with regards to information system resources. Their findings showed that employees' attitude was impacted by the benefits, cost of compliance, and cost of non-compliance which could arguably be as a result of the consequences. A study by [2] on the other hand considered the role of top management, organizational culture, and employee behavior and how they interact to shape compliance vis-à-vis the subjective norms and perceived controls attributed to employee behavior. Another study that attempted to address compliance was a study by [3] whereby the authors looked at higher education institution compliance with information security. Their findings suggested that regulative pressure and social normative pressure were able to shape the compliance behaviors of employees in an organization in higher education. A model by [4] on the other hand provided a useful explanation of relationships between institutional, individual, and environmental factors on the general information security awareness. A study by [5] approached the compliance study by looking at the relationships between the organization, employee, and information technology.

Extant literature shows robust efforts to address the weakness of information security policy compliance, however, very little attention has been given to the compliance culture as a way of nurturing a higher policy compliance rate. This study, therefore, sought to address this existential gap by taking a different methodological approach.

To address the existential gap, this study followed a mixed-method approach. The thesis where this study was drawn from was divided into two phases namely the model development phase and model validation phase. The model development

phase achieved the generation of the model that the researchers have now validated.

2.1 Theoretical model and hypothesis development

This paper draws from the researcher's empirical study that generated constructs that explain information security policy compliance culture phenomena through grounded theory. **Error! Reference source not found.** illustrates the emergent relationships after a rigorous model development phase and of which the researchers sought to validate through this study.

Hypotheses were developed from the theoretical model emerging from the main exploratory sequential research. **Error! Reference source not found.** shows the individual hypothesis and the respective key indicators and coding that were extracted from the theoretical model in Figure 1. A structured questionnaire was adopted as a tool to conduct the survey. The online form was created on a google platform. The questionnaire was targeted towards all staff and students of the participating universities.

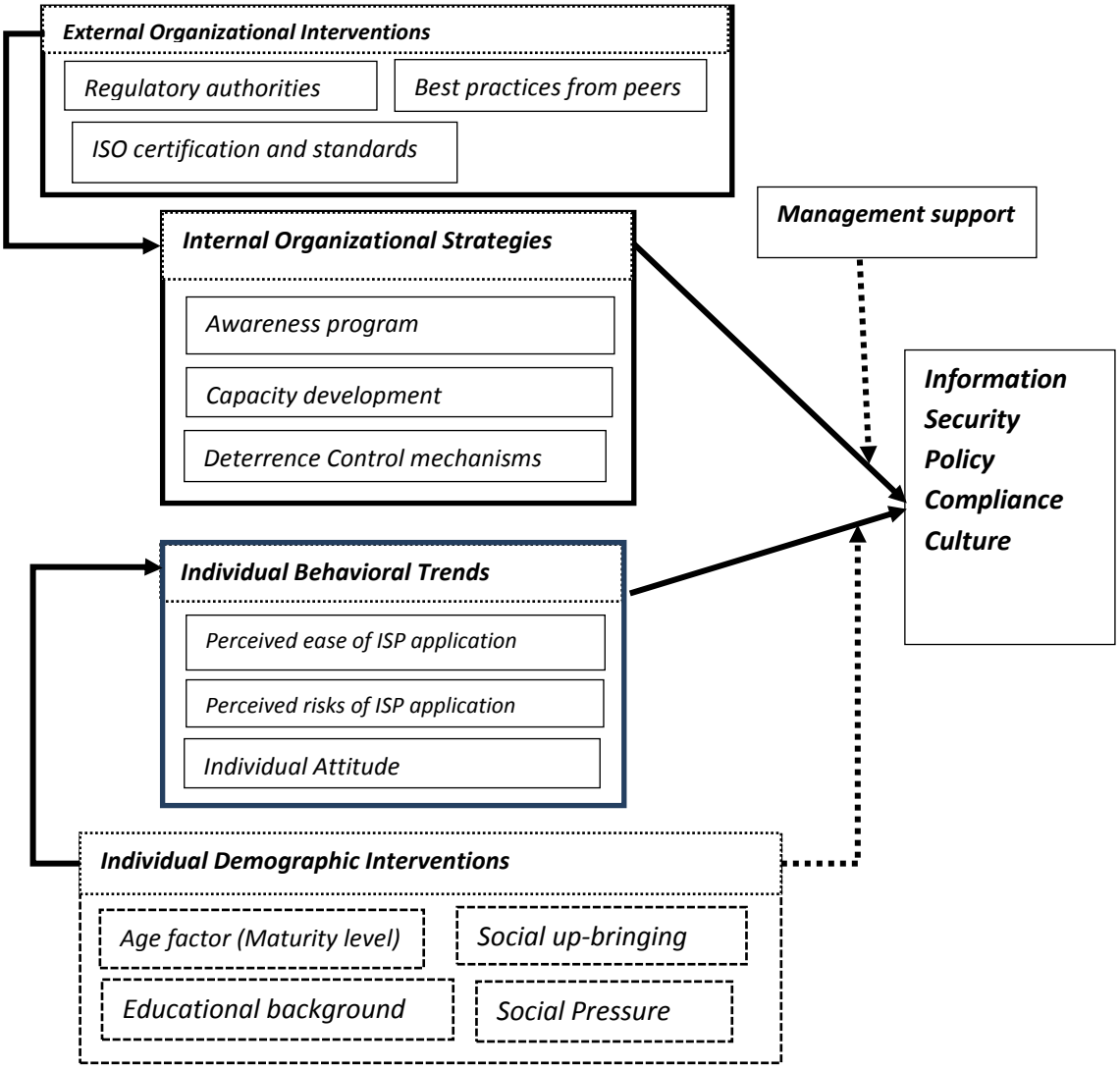

Figure 1: Theoretical Model illustrating the relationships between emergent constructs and information security policy compliance culture (Source: Research Thesis)

Table 1

Hypothesis	Key Indicators and Coding
H1: Age has a moderating effect between *Individual Demographic Interventions* and *Information security policy compliance culture*.	• Mature staff are more likely to reason and comply with information security policies in place **(DMF-AF1)** • Handling a diverse age group provides a challenging environment when enforcing information security policy **(DMF-AF2)**
H2: Social upbringing to some extent influenced how users complied with information security policies	• The difference in social upbringing provides a big challenge when enforcing information security policies **(DMF-SU1)**
H3: Social pressure has a moderating effect between *Individual Demographic Interventions* and *Information security policy compliance culture*.	• Handling members under seer pressure is challenging when enforcing information security policy compliance **(DMF-SP1)**
H4: Education background influences information security policy compliance	• We have challenges enforcing information security policy when dealing with members with a technology background **(DMF-EB1)**
H5: Management support has a moderating effect between *Organisational External Interventions* and *Information security policy compliance culture*.	• Management support improves the execution of information security policies **(OMF-MS1)** • I feel motivated to comply with information security when management also complies **(OMF-MS2)** • It is easier to create awareness when management gets involved in the process **(OMF-MS3)**
H6: Regulatory authorities influence organizational initiatives towards information security policy compliance	• We are obliged to follow the regulatory authorities' requirements **(EOI-RA1)**
H7: ISO certification and standards influence organizational initiatives towards information security policy compliance	• External certification obligations increase the level of responsibility to enforce compliance with information security policies **(EOI-ISO-CS1)**
H8: Best practices from peers influence organizational initiatives towards information security policy compliance	• Learning from peers encourages a well-planned information security policy compliance initiative **(EOI-BP1)**
H9: Awareness program initiative by organizations influences the compliance with information security policies	• A conscious society increases the level of compliance with information security policies **(OI-AP1)**
H10: Capacity development initiatives by organizations influence information security culture	• Constant training and capacity development encourage members to comply with information security policies **(OI-CD1)**
H11: The deterrent control initiatives by organizations influences information security policy compliance culture	• Our deterrent initiatives discourage noncompliance behavior **(OI-DC1)** • Our control mechanism reduces incidents of non-compliance with information security policies **(OI-DC2)** • Our monitoring initiatives enables detection of information security breaches in time **(OI-DC3)**
H12: Perceived ease of ISP application influences the information security compliance culture in organizations	• I am more likely to comply when the policies are interventions are easy to understand and use **(IBT-PEIA)**
H13: Perceived risks of ISP application influences information security policy compliance culture in organizations	• I am more likely to avoid complying with information security policies if I perceive them to be a risk to me or my privacy **(IBT-PRIA)**
H14: Individual attitude influences information security policy compliance culture	• Rebellious members will more likely violate information security policies **(IBT-IA1)** • My attitude towards the policies will impact on how I comply **(IBT-IA2)**

3. METHODOLOGY

The research design was descriptive. This paper presents the validation outcome of the model development phase. The study adopted a Confirmatory Factor Analysis (CFA) approach to validate the emergent model. The constructs were operationalized to enable the development of a questionnaire. This was vital for the development of how indicators were to be measured in the study. In operationalizing the constructs, the researchers identified which constructs were reflective and which constructs were moderating factors. The nature of reflective operationalization was also identified in terms of whether they were negative or positive.

3.1 Sampling Design

The researchers considered 8 chartered universities in Kenya. This included both public and private universities. The universities were considered based on the longevity criteria of 20 years in operations. The choice of the target population was due to its diversity.

The study adopted Cochran's formula in calculating the estimated sample size. Cochran's formula has been considered in several studies dealing with an infinite population [6]. The researchers assumed an infinite population because it would be difficult to estimate the number of respondents in the selected university at any given moment.

$$s0 = \frac{z2pq}{e2}$$

Where:

s_0 is the sample size, z is the selected critical value of desired confidence level, p is the estimated proportion of an attribute that is present in the population, q=p−1 and e is the desired level of precision.

Therefore, assuming the maximum variability was equal to 50% (p=0.5) while considering confidence level as 95% with ±5%, precision, the researchers calculated the required sample size as below.

p = 0.5 and hence q =1-0.5 = 0.5; e = 0.05; z =1.96

s0 = (1.96)2 (0.5) (0.5) / (0.05)2 = 384.16

s0 Rounded off to the nearest 5 = 384

The researchers, therefore, estimated the sample population to be 384 respondents that were targeted.

3.2 Pilot study

We administered a draft questionnaire to 10 respondents outside the participating universities in the pilot study. The result of the pilot study went smoothly and did not show any difficulties in understanding the line of questions. There was also an indication that the research protocols were satisfactory. Besides, the data collection instruments met the standard as originally anticipated. This means that the researchers proceeded with the data collection stage without any further modifications.

3.3 Data Collection Method

The study shared the online google form with a few representatives within the participating universities. The representatives then shared within their networks and peers. The online form was considered because it offered a wider reach with minimal resource barriers. The researchers made follow-up calls to the first line of volunteers who also followed up with their network to enhance response rates. Out of the envisaged 380 responses, the study managed to garner a total of 364 respondents across 8 universities. This represented a satisfactory response rate of 95.79%.

3.4 Data Analysis Approach

The study employed the use of JASP software to conduct the Confirmatory Factor Analysis. In addition to the fact that it was open-source software, JASP was adopted because of its capability of conducting Structured Equation Modeling – Confirmatory Factor Analysis to validate and perform other model fitness tests.

4. RESULTS

4.1 Distribution of respondents per Universities

Out of the total respondents from all the universities enrolled, gender representation was recorded as male respondents being 53.6% and female 46.4%. Most of the respondents were within the 20-30 age group at 53.8%, with the age groups of 31-40 being 33.5%, while the age group of 41-50 was 12.1% of the respondents. The results also had the respondents over the age of 50 being only 0.5% of the total respondents. Table 2 summarizes the responses in percentage.

Table 2: Distribution of respondents per Universities

University	Number of respondents	Percentage of the total
African Nazarene University	44	12.1%
Daystar University	26	7.1%
Egerton University	64	17.6%
JKUAT University	59	16.2%
Kenyatta University	49	13.5%
Maseno University	46	12.6%
Moi University	24	6.9%
Strathmore University	52	14.3%
Total	364	

4.2 Reliability test

To test the reliability of the study, the researchers conducted a Crobach's alpha test. The results indicate a reliable study as seen in table 3 with a value of 0.956.

Table 3: Table showing Cronbach's α value

Scale Reliability Statistics	
	Cronbach's α
scale	0.956
Note. **Of the observations, 364 were used, 0 were excluded listwise, and 364 were provided.**	

4.3 Model fit Measure

The study assessed the Chi-square test to validate the model.

The result of the indicated a statistically highly significant value of $p < .001$, Table 4.

Table 4: Table detailing the Chi-square test

Chi-square test			
Model	**X^2**	**df**	**p**
Baseline model	6239.15	190	
Factor model	533.944	160	< .001

4.4 Additional fit measures

The results indicated the Comparative Fit Index (CFI) as 0.938 and Tucker-Lewis Index (TLI) 0.927. Concerning information criteria, the results indicated the Log-likelihood of -6740.580. The finding showed Root mean square error of approximation (RMSEA) as 0.080 and Goodness of fit index (GFI) as 0.983.

4.5 Parameter estimates

The study also presents the factor loading for all parameters in which all the factor loadings were beyond the threshold as shown in Table 5.

Table 5: Table showing factor loading for each of the parameters

			95% Confidence Interval		
Factor	**Indicator**	**p**	**Lower**	**Upper**	**Std. Est. (all)**
Individual Demographic Interventions	DMF-AF1	< .001	0.648	0.833	0.73
	DMF-AF2	< .001	0.763	0.935	0.839
	DMF-SU1	< .001	0.716	0.901	0.776
	DMF-SP1	< .001	0.731	0.898	0.836
	DMF-EB1	< .001	0.748	0.913	0.85
External Organisational Interventions	EOI-RA1	< .001	0.82	0.964	0.952
	EOI-ISO-	< .001	0.79	0.933	0.936
	EOI-BP1	< .001	0.704	0.852	0.865
Management Support	OMF-	< .001	0.733	0.885	0.884
	OMF-	< .001	0.701	0.868	0.814
	OMF-	< .001	0.671	0.831	0.812
Organizational Strategies	OI-AP1	< .001	0.579	0.737	0.748
	OI-CD1	< .001	0.552	0.703	0.746
	OI-DC1	< .001	0.64	0.798	0.794
	OI-DC2	< .001	0.633	0.792	0.788
	OI-DC3	< .001	0.616	0.762	0.811
Individual Behavioural Trends	IBT-PEIA	< .001	0.622	0.739	0.923
	IBT-PRIA	< .001	0.591	0.74	0.786
	IBT-IA1	< .001	0.556	0.705	0.758
	IBT-IA2	< .001	0.605	0.732	0.87

5. DISCUSSION

5.1 Individual Behavioral Trends

We considered the Individual Behavioral Trends variable to be very strong because the variable indicators displayed a factor loading that the researchers considered significant, Table 5. The factor loadings for the variable indicators ranged between (0.758) and (0.923) when standardized. This fell within the threshold level of (0.50). With an observed statistical significance of ($p < 0.001$), the convergent validity was therefore concluded in the affirmative.

The findings show that individual behavior is an essential factor when strategizing on how to enhance compliance. It is not only important to have information security policies in place, but the net behavior of those interacting with the policy is equally important. Users may comply if they have a notion that the policies will not complicate their lives than it is in the current form. The users also appear to worry so much about the risks of applying and following the policies. This implies that users would more likely to circumvent the policies if the perceived risks are higher. The attitude towards the leadership, the policies, and the environment in which the members are also mean a lot for the information security compliance culture. The results, therefore, imply that management needs to take a keen interest in individuals' behavioral trends since the behaviors would impact on both the strategies and actual compliance culture.

Similar supportive works can be seen in the studies by [7] who argued that perceived ease of use of technology had some influencers towards the adoption of information security measures. Similarly, [8], [9], [7], [10], and [11] who identified risk perceptions as important factors when addressing violations of policies. Studies by [12], [1], [13], and [14] also found that attitudes of the employees affected the general intentions to comply with information security.

5.2 Individual Demographic Interventions

All the factor loadings for the Individual Demographic Interventions indicators ranged from 0.73 to 0.85 after standardization, Table 5. This depicted a statistically greater value than the threshold level of 0.50. All indicators were significant at $p < 0.001$ level, which indicated a convergent

validity.

We, therefore, submit that the maturity level of members' impacts to some extent on information security management by moderating an individual's behavior actions. It is equally important that part of the checklist would factor in the social pressure aspect that the members may be experiencing. The researchers believe this would be important because as a manager, understanding the social pressure components in your institution would provide foresight into the challenges that can be averted. By taking account of possible maturity level and reasoning levels of your audience, it would provide an insight on how to proceed in enforcing the policy compliance and enhancing understanding strategies. Similarly, if the institution has a more diverse membership with a range of social upbringing background, the management can have a tailored information security environment that fosters a culture of compliance. Educational background may provide a difference in comprehension and handling of technology-related policies. Therefore, information security managers need to have different approaches that maximize the strengths and weaknesses of the members with different educational backgrounds.

Our findings differ to some extent from existing studies concerning individual demographic interventions. This is especially concerning educational background. Though many studies agree with the findings of this study in terms of the role played by indicators such as maturity level, social pressure, none of the extant studies have covered the component of social education background as a factor in information security policy compliance culture. Studies by, [15] argued that age played a role in the net behavior of individuals concerning information security. On the social up-bringing front, [16] argued that social interactions had the possibilities of moderating impact on an individual's behavioral tendencies. Individuals' moral beliefs were also portrayed by [8], as a factor just like [10] who also argued on the same as a moderating factor in individuals' interactions with information security policies.

5.3 Organizational Strategies

The factor loadings of Organizational Strategies variables showed a strong loading across all the indicators, Table 5. All the factor loadings for the indicator variables ranged from 0.746 to 0.811 with standardization. This showed a statistical threshold that is greater than the level of 0.50. A significant value of $p < 0.001$ level was also recorded for all indicators showing a convergent validity.

We looked at the import of organizational strategy findings from the perspective of the importance of organizational initiatives in creating a long-lasting culture of compliance. The values, artifacts, norms, and institutionalization of practice become the rallying call for new members and existing members. This implies that for these rallying calls to be engraved in the current members, initiatives of awareness, capacity building, and deterrence mechanisms initiatives need to be robust, and effective. This would in the end implore and incentivize information security policy compliance behavior. It is the submission of this study that when this gets engraved to the inner conscience of the members, the management would succeed in creating a long-term ISPCC.

We also see supporting findings in the studies by [17], [18], [1], and [19] who all underscored the importance of awareness programs in information security compliance. Similarly, in support of the capacity development finding, [13] argued the benefit of individual competence and capabilities as a good input towards a successful information security management strategy. Studies by [10], [20], [21], and [22] on the other hand supported the deterrence and control mechanisms. The respective studies discussed the role of deterrence in the form of penalties and control components preventive measures of information security management.

5.4 Management Support

Management Support showed a strong loading across all the indicators, Table 5. All the factor loadings for the three indicators ranged from 0.812 to 0.884 after standardization. This was statistically greater than the threshold level of 0.50. All indicators were all significant at $p < 0.001$ level, which indicated a convergent validity.

The finding shows that for a successful strategy as devised by information security practitioners, management support is an important pillar. Though not a direct impact, it would provide a support base for the initiatives of the experts in the intuition. This, in the long run, contributes to the greater organizational culture. It is this paper's submission that the organizational culture would more likely to percolate deeper into the environment that promotes information security compliance culture. This could be argued to be supported by the members who perceived management support to be inspirational. Members also felt that they would readily comply if the top management also complied as seen in Figure 2.

We draw supporting findings from similar endeavors such as studies by [18] and [10] who identified management support such as an important component in implementing successful information security management strategy. Similarly, studies by [23] and [24] also supported the findings on management support by indicating that upper management leading by example fostered a positive environment to enhance positive followership. This in the end encouraged those being led to follow positive actions emerging from their leaders.

5.5 External Organizational Interventions

The External Organizational Interventions were supported by strong factor loading for the variable indicators that ranged between (0.865) and (0.952) when standardized, Table 5. This fell within the threshold level of (0.50). With an observed statistical significance of ($p < 0.001$), the convergent validity was concluded in the affirmative.

We, therefore, argue that external influences on information security strategies are important in enhancing information security policy compliance. The findings remind us that institutions do not exist in a vacuum. Since what the members of the institutions do might have an impact on the external partners and stakeholders, recognizing that there are standards, best practices among peers, and regulatory obligations provide the step in the right direction to improve information security policy compliance. If the information security managers make it a culture to be conscious of what are the obligations, then it would create a positive environment to have what has worked well that can be adopted.

Similar findings also support the results as evident in studies by [25] and [26] who fronted coercive pressure as contributors to robust organizational strategies. On the normative front, [25] and [27] highlighted the role played by normative pressure such as the quest to be fitting within the norm.

certification and standardizations emerged as a trend that managers wanted to adopt in their strategies. The researchers also found similarities in the findings from the studies of [25] and [26]. The studies also identified mimetic pressure as important factors in influencing individual organizations in terms of how management formulated their strategies. Best practices within and organizational environment would shape how peers in the industry adapt their strategies such as policy management strategies.

5.6 Synthesis of the theory

We adopted the guidance of (Whetten, 1989) in assessing this paper's theoretical contribution. The researchers synthesized the theory by considering key components of what wakes a sound theory and what needs to be considered as a peripheral indicator. Therefore, the researchers drew from the characteristics of what is a theory and synthesized a high-level relationship towards information security policy compliance culture (ISPCC), Figure 2.

We classify the constructs and their relationships towards information security policy compliance culture (ISPCC) as follows:

- Organizational strategies have a direct relationship with how information security culture is natured over time. It is classified as a mediating variable since it has a mediating effect between External Organizational Interventions in the relationship denoted as (c) and ISPCC, Figure 2. The variable also mediates between the Individual Behavioral Trends with the relationship denoted as (d) and ISPCC.
- Management support on the other hand provides a foundation for the organizational strategies to flourish and succeed in its objectives. The variable is classified as a moderating variable between Organizational Strategies and ISPCC and is denoted as (e) in Figure 2.
- Individual behavior has a direct relationship with how information security culture is natured overtime and directly influences organizational strategies. The variable is classified as an independent variable towards the mediating variable Organizational Strategies, which is denoted as (d) and is also independent towards the outcome variable ISPCC with the relationship denoted as (b) in Figure 2.
- Individual demographic interventions have a moderating component between individual behavior and the ISPCC. The moderation relationship is denoted as (f) in Figure 2.
- External organizational interventions shape how an organization and its management formulate strategies to enhance compliance. The variable is classified as an independent variable with the relationship denoted as (c) in Figure 2.

5.7 Path analysis summary

b = direct effect of Individual Behavior Trends on ISPCC

d = direct effect of Individual Behavior Trends on Organizational Strategies

a = direct effect of Organizational Strategies on ISPCC

d*a = indirect effect of Individual Behavior Trends on ISPCC

b+(d*a) = total effect of Individual Behavior Trends on ISPCC

c*a = indirect effect of External Organizational Interventions on ISPCC

e = moderating effect Management Support between Organizational Strategies and ISPCC

f = moderating effect of Individual Demographic Interventions between Individual Behavioral Trends and ISPCC

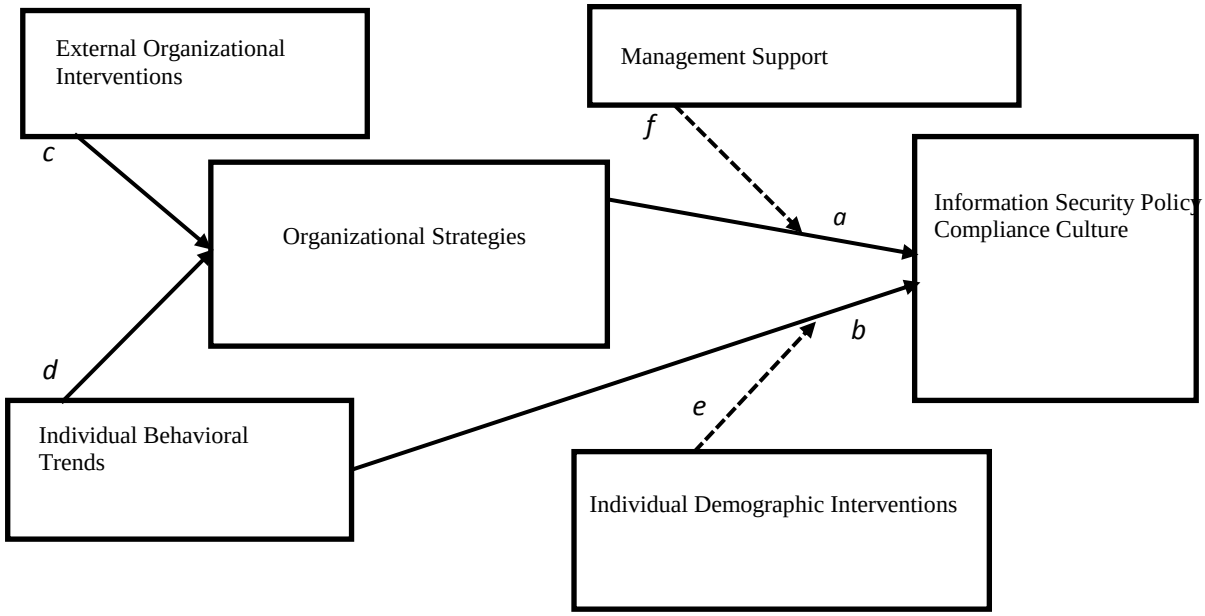

Figure 2: Top-level theoretical model depicting the relationships between Individual Behavioural Trends, Individual Demographic Interventions, Organizational Strategies, External Organisational Interventions, Management Support, and

5.8 How does it relate to other theories already in existence?

Existing theoretical models have focused more either modeling on compliant behavior or policy compliance intentions. For example, models by [1], [24], and [4] all focused on behavioral intentions to comply but little information security policy compliance culture. This could be argued to be the same as the model by [28] in which the resulting model focused mainly on compliant behavior. The resulting model attempts to expand the scope of information security compliance study by contextualizing constructs to explain information security policy compliance culture. Therefore, to the best of the researcher's knowledge, this study is the first attempt to generate a theory that provides a set of propositions towards understanding information security policy compliance culture. This is achieved by setting and presenting a systematic view of information security policy compliance culture. The theory, therefore, provides a foundation for future information security research by providing a broad variable base for future studies to explore.

6. CONCLUSION

The purpose of this paper was to validate the generated theoretical model explaining information security policy compliance culture (ISPCC). The researchers elaborate on the relationships that have been identified in the previous section in terms of a theory that explains ISPCC. The researchers submit that there must be a precursor that promotes an environment where the existing information security policy is complied with. Without this precursor, the managers might face a dilemma of why robust policies do not translate to good information security mitigation results. The conducive environment for compliance with time breeds a culture of compliance. This might be visible in action or might not be visible as would be the case of perception. These conducive environments then in turn develops into an information security culture as a sub-culture of the greater organizational culture. With the culture already in place, the researchers conclude that it would be easy for newer members and existing members to continue with the values and norms.

Our theoretical model explains this phenomenon starting from the precursor in the form of Individual Behavioral Trends which are moderated and influenced directly by Individual Demographic Interventions; Organizational Strategies that are influenced by External Organizational Interventions; and moderated by Management Support. The researchers postulate a theory for future study of information security policy compliance culture (ISPCC) based on the emergent theoretical model.

This study has implications for both theory and practice. For theoretical contribution, this study has contributed to a theory that explains the relationships between organizational, individual, and external interventions and information security policy compliance culture (ISPCC). Future researchers can adopt the developed theoretical model when inquiring about areas related to organizational strategies and information security-related studies. For practitioners, this study provides building blocks to support information security policy compliance. This has been achieved by provisioning checklists to information security managers on what they need to consider when nurturing ISPCC.

6.1 The Study Limitation and recommendation

The study had some limitations that the researchers would recommend for future researchers to tackle. The study was limited to universities only and as such, can only be generalized within the context of higher learning institutions. This paper's recommendation therefore would be to urge future researchers to explore other contexts such as commercial institutions, or other organizations not in the higher education institutions categories.

7. REFERENCES

[1] B. Bulgurcu, H. Cavusoglu and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," MIS Quarterly, vol. 34, no. 3, pp. 523-548, 2010.

[2] Q. Hu, T. Dinev, P. Hart and D. Cooke, "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture," Decision Sciences Journal, vol. 43, no. 4, 2012.

[3] H. Kam, P. Katerattanakul, G. Gogolin and S. Hong, "Information Security Policy Compliance in Higher Education: A Neo-Institutional Perspective," in PACIS 2013 Proceedings. 106, 2013.

[4] F. J. Haeussinger and J. J. Kranz, "Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior," in International Conference on Information Systems ICIS 2013, Milan, 2013.

[5] S. David, M. Marlys, B. David and W. Mark, "A Theory of Employee Compliance with Information Security," in MWAIS 2014 Proceedings. Paper 1, 2014.

[6] W. G. Cochran, Sampling Techniques, 3rd ed., 1977.

[7] M. Workman, W. H. Bommer and D. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test," Computers in Human Behavior, p. 2799–2816, 2008.

[8] Q. Hu, Z. Xu, T. Dinev and H. Ling, "Does Deterrence Work in Reducing Information Security Policy Abuse By Employees?," Communications of the ACM, vol. 54, no. 6, pp. 54-60, 2011.

[9] A. C. Johnston and M. Warkentin, "Fear Appeals and Information Security Behaviors: An Empirical Study," MIS Quarterly, vol. 34, no. 3, pp. 549-566, 2010.

[10] T. Herath and H. R. Rao, "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," Decision Support Systems, vol. 47, no. 2, pp. 154-165, 2009.

[11] T. Sommestad and J. Hallberg, "The sufficiency of the theory of planned behavior for explaining information security policy compliance," Information and Computer Security, vol. 23, no. 2, pp. 200-217, 2015.

[12] S. Pahnila, M. Siponen and A. Mahmood, "Employees'

Behavior towards IS Security Policy Compliance," in Proceedings of the 40th Hawaii International Conference on System Sciences - 2007, 2007.

[13] P. Ifinedo, "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition," Information & Management, vol. 51, no. 1, p. 69–79, 2014.

[14] N. S. Safa, R. V. Solms and S. Furnell, "Information security policy compliance model in organizations," Computers & Security, vol. 56, pp. 1-13, 2016.

[15] M. Whitty, J. Doodson, S. Creese and D. Hodges, "Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords," Cyberpsychol Behav Soc Netw, vol. 18, no. 1, p. 3–7, 2015.

[16] T. Herath and R. H. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," European Journal of Information Systems, vol. 18, no. 2, pp. 106-125, 2009.

[17] J. D'Arcy, A. Hovav and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," Information Systems Research, vol. 20, no. 1, pp. 79-98, 2009.

[18] M. Karydaa, E. Kiountouzisa and S. Kokolakis, "Information systems security policies: a contextual perspective," Computers & Security, vol. 24, no. 3, pp. 246-260, 2005.

[19] P. Puhakainen and M. Siponen, "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study," MIS Quarterly, vol. 34, no. 4, pp. 757-778, 2010.

[20] M. Siponen and A. Vance, "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," MIS Quarterly, vol. 34, no. 3, pp. 487-502, 2010.

[21] Y. Chen, K. Ramamurthy and K. Wen, "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?," Journal of Management Information Systems, vol. 29, no. 3, pp. 157-188, 2014.

[22] T. Virtue and J. Rainey, "Information Risk Assessment," in HCISPP Study Guide, 2015.

[23] M. Chan, I. Woon and A. Kankanhalli, "Perceptions of Information Security at the Workplace: Linking Information Security Climate to Compliant Behavior," Journal of Information Privacy and Security, vol. 1, no. 3, pp. 18-41, 2005.

[24] Q. Hu, T. Dinev, P. Hart and D. Cooke, "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture," Decision Sciences Journal, vol. 43, no. 4, 2012.

[25] Q. Hu, P. Hart and D. Cooke, "The role of external and internal influences on information systems security – A Neo-Institutional perspective," Journal of Strategic Information Systems, vol. 16, pp. 153-172, 2007.

[26] A. AlKalbani, H. Deng, B. Kam and X. Zhang, "Information Security Compliance in Organizations: An Institutional Perspective," Data and Information Management, vol. 1, no. 2, p. 104–114, 2017.

[27] H. Cavusoglu, H. Cavusoglu, J. Son and I. Benbasat, "Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources," Information & Management, vol. 52, no. 4, pp. 385-400, 2015.

[28] M. Chan, I. Woon and A. Kankanhalli, "Perceptions of Information Security at the Workplace: Linking Information Security Climate to Compliant Behavior," Journal of Information Privacy and Security, vol. 1, no. 3, pp. 18-41, 2014.