Information and Knowledge Management
ISSN 2224-5758 (Paper) ISSN 2224-896X (Online)
Vol.10, No.5, 2020

Exploring the Factors That Contribute Towards Information Security Policy Compliance Culture

Erick O. Otieno* Agnes N. Wausi Andrew M. Kahonge
The University of Nairobi.

Abstract
There is over-reliance on information systems to run virtually all aspects of modern institutions. This has put more burden on information security managers to come up with more robust and efficient ways to enhance information security policy compliance. Therefore, despite existing efforts in the area of information security management, there remains a critical need for more research to be done. The existing research has also concentrated on hypothesis testing rather than a qualitative approach. So, there is an existential methodology gap that can give another alternative result that still needs to be covered. That is why we embarked on exploring the factors that influence information security compliance in organizations. The research was conducted in two universities with a diverse population. The research design was exploratory, encompassing qualitative in-depth case interviews with grounded theory as the analysis strategy. A total of 20 interviews were conducted and each analysis was done after every few batches of interviews in line with grounded theory principles. A theoretical model was generated and discussed. Implications for the research were also discussed and recommendations made. The study found individual factors, organizational factors, and external influence to be important factors in strategizing how to increase compliance with policies. The results also showed that practitioners need to factor in a combination of elements in their strategies in order to enhance compliance with information security policies.
Keywords: Information Security Policy Compliance Culture, Theoretical Model, Grounded Theory, Information systems security
DOI: 10.7176/IKM/10-5-05
Publication date: August 31st 2020

1. Introduction

Numerous attempts have been made to provide solutions concerning policies to provide guidance and frameworks on information security management. Despite heavy investment by institutions on ensuring robust policies, processes, and control, incidents of internally induced breaches still exist. Extant studies indicate that internal parties and stakeholders account for about 80% of information security breach incidents. A case in point is the study by (SANS Institute, 2017) which found that malicious employees accounted (43%) while (39%) of insider cases emerged as error or negligence from non-malicious counterparts. As a mitigation measure, after the necessary policies, processes and controls have been put in place, two questions should arise: Have we invested equally in policy compliance strategies? Can information security culture be the silver lining towards mitigation of internally instigated breaches?

ICT Policies are not made because of mistrust by information security managers towards those who interact with information assets. On the contrary, the policies are made to offer guidance and a framework on how to protect those who interact with the ICT assets and the organizational information systems assets. Since policies are heavily dependent on human interactions to succeed, we emphasize that "People are at the center of policies". This is especially true because for any mitigation to be effective, those who are expected to adhere must be seen, and be felt to be doing exactly that through full compliance with the requirements. How then do we inculcate a culture of ICT policy compliance?

Besides processes, controls, and policies, compliance culture is increasingly being considered as an important component in information security mitigation strategies. Many recent studies, such as (Ifinedo, 2014), (AlKalbani, et al., 2017), (Amankwa, et al., 2018) and (Sommestad, et al., 2019), have begun to consider information security policy compliance as part of information security management strategies. However, there is minimal coverage of information security culture as a way of information security policy compliance culture. Further, most of these studies have applied methodologies that draw from existing theories and models. For example, a study by (Ifinedo, 2014) applied an empirical study approach that considered socialization, influence, and cognition. Another study by (Safa, et al., 2016) also applied hypothesis testing to generate a model for information security compliance in organizations. Such an approach is also seen in (AlKalbani, et al., 2017). The authors approached their study from the hypothesis testing point of view while looking at institutional aspects of information security policy compliance. In the study by (Amankwa, et al., 2018) the authors factored in variables from the involvement theory and organizational behavior theory to develop their hypothesis. Taking a similar approach was the study by (Sommestad, et al., 2019), in which the authors considered variables emerging from a meta-analysis information security behavior test. However, in our study we considered a different methodological approach, that of using grounded theory, to study information security policy compliance culture.

By adopting Grounded Theory, our study enabled new concepts, (such as external organizational interventions, organizational strategies, management support, individual behavioral trends, and individual demographic interventions) to emerge that explain the relationships between information security culture and organizational factors, individual factors, and external influences. We submit that these relationships inform the critical issue at hand of enhancing information security compliance culture through the emerging multi-level model. This study therefore explores and explains the underlying factors that contribute to information security compliance culture in organizations.

2. Methodology

An exploratory research design was used. Grounded theory, as described by (Charmaz, 2008), was applied as the analysis strategy. An in-depth case study using interviews was used to identify patterns of what influenced information security compliance culture in the selected Higher education sector in Kenya, and specifically Universities. The choice of the universities was purposively made, firstly due to their richness in population with diverse backgrounds and cultures; and secondly, the diversity in professional cultures ranging from studentship to senior academic and administrative staff. We perceived this environment to provide a context that provided a rich pool of respondents on what influences information security compliance culture in the university.

A total of 20 in-depth-interviews were conducted in 3 phases. The first phase consisted of 10 interviews across the two cases; with 5 interviews for each case. The interviewees were purposively selected across students; academic and administrative staff who interact with the university's ICT assets. The choice of who to interview next was guided by theoretical sampling. This was arrived at after analyzing each interview data and determining which kind of information was to be gathered next to build on the emerging themes. The second phase of the in-depth-interviews were 6 in total, with 3 in each of the two cases. The focus was to get more information on the emerging themes from the first phase of interviews. The last phase consisted of 4 interviews from the two case universities. This last phase took more of a confirmatory approach to the themes that had already been developed from the previous interviews. At this point, there were no further themes that were emerging, and hence no further interviews were conducted.

The interview sessions were conducted in 60 days. The interviews were based on an interview guide with each interview taking averagely 25 minutes. Even though the interview guide varied in form and structure, the broader contextual approach was maintained. This was done by ensuring that all questions remained within the context of organizational culture regarding information security policy compliance. With each next interview, the questions were refined, and clarifications sought if necessary. Non-verbatim transcription was done to elicit clarity behind the spoken and the numerous written field notes. We employed the use of an online tool, (oTranscribe, n.d.) to transcribe our audio interview recordings into a coherent and understandable flow.

The emergent themes were then passed through the second coding process of axial coding to put the themes into categories. The saturation point was reached in the 20th interview. At this point, there were no more new emergent categories even after further interviews. Preston and Jorgen's proposition argued in extant literature that a saturation arrived at between **15** and **30** interviews would be considered enough, (Preston & Jorgen, 2016). We, therefore, stopped further data collection. The interviews were spread across two universities which have been coded with **University A** and **University B** respectively.

At the point of saturation, we had 6 major categories. We then performed the third coding process to group the categories or merge some categories. This was an iterative process until we could not identify any more emergent themes or categories from the interviews and the coding process. We tracked all the processes through constant memoing in three major phases namely; definition of categories from the basic emerging themes during the open coding stage, the clustering phase during the axial coding stage, and the construction of concept phase during the selective coding stage. The resulting concepts were then congregated for the theoretical model that explains the information security policy compliance which we discuss in the next sections.

3. Results

3.1 Emergent themes from interview data

We set to understand the level of information security maturity within the universities that we interviewed. Out of the 20-interview data analyzed, there was a total of 97 selective codes emerging. From the 97 selective codes, we were able to establish a total of five theoretical themes. Figure 1 Figure *1*summarizes the contribution in the percentage of total selective codes to building the theoretical theme. The following sections will look at the five theoretical themes namely: ***Individual Behavioral Trends, Individual Demographic Interventions***, ***Internal Organizational Strategies, Management support***, and ***External Organizational Interventions.*** The results showed strong evidence of information security policy compliance culture in both universities under study. Out of the 20 interviews, a total of 15 participants mentioned some semblance of a compliance culture in their respective universities. Most of those interviewed ranging from staff to students indicated "…*few experiences of violations*…" according to the university administration, and "…*Belief in the existence of culture*…" according

to some staff and students alike. These results showed information security policy compliance cultural phenomenon in the universities that were engaged.

3.2 Individual Behavioral Trends (Perceived ease of ISP application, Perceived risks of ISP Application, and Individual Attitude)

Individual behaviors emerged as a factor that influenced how the universities shaped their strategies towards ensuring policy compliance as seen in Figure 2. This also emerged as an influencer on how individuals complied with the information security policies. Individual behavioral trends were evident from those interviewed, showing that how one perceived the ease of applying the various Information Security Policies (ISP) influenced their compliance actions to some extent. Those who perceived risks towards themselves while applying the various ISPs also indicated some level of reluctance in complying with the ISPs. Results also showed that individual attitudes towards the ISPs and the management infused to some extent the net compliance actions by individuals.

3.2.1 Perceived ease of ISP application

The sentiments shared by some informants indicated that users would easily comply when the policies are easy to understand and easy for users to implement. One informant added that *"...Policies are designed to be followed by individuals and this, they said could lead to policy circumvention if it made their lives difficult thereby leading to some form of policy violations..."*. The results indicated a direct relationship between Perceived ease of information security policy application and information security policy compliance culture (ISPCC).

3.2.2 Perceived risks of ISP Application

One other emerging factor was the perceived risks as an influencer of information security policy compliance. For example, the majority of those interviewed agreed on the existing concerns among their peers concerning the risks involved when the policies are perceived to expose them to the administration. Such sentiments were said to involve situations where it was considered that their details were being captured on every website they accessed. As such, the informants *"...were more inclined to use online firewall blockers...."* Without considering the risks they were exposing the institution to external compromises.

3.2.3 Individual Attitude

Respondents from the interview also indicated that students' and staff's attitude towards the actions by the administration affected the culture of compliance. An example can be drawn from the several informants, who echoed what was a common sentiment among the youthful generation who were more concerned about their inhibitions to access certain sites such as video and games sites. This, in turn, created a negative attitude towards the policy of fair usage in the universities. Therefore, members of staff and students who ended up forming an attitude were perceived by their peers to be more likely to violate the policies.

3.3 Individual Demographic Interventions (Age factor (Maturity level), Social upbringing, Social Pressure, Educational background)

As seen in Figure 3, individual demographic factors emerged as another important factor that moderated how individuals behaved towards information security policies. Age factor, social upbringing, educational background, and Social pressure emerged as important variables towards individual demographic interventions.

3.3.1 Age factor (Maturity level),

According to several informants, Age, (maturity level), was found to be a factor by managers strategizing on how to handle younger and senior students and staff in the universities. The respondents argued that the generational grouping mattered in coming up with approaches. For example, the one informant indicated "*…how the younger generation had become increasingly inquisitive with the technological reliance and therefore, a more accommodating approach based on reason….*" was a better approach to handle them.

3.3.2 Social upbringing

Concerning social upbringing, some informants mentioned social upbringing as a factor they felt contributed to how one behaves towards policies. Some expressed the role played by "*…being exposed to the social media and how some of their colleagues were brought up…*" as one important way of looking at the behavior. By being fused into the environment of social media where everything goes and factoring in the pressure that comes with peer influence, managers were at pains to ensure information security compliance.

3.3.3 Social Pressure

Social influence among students of the same educational background or social background came up as one of the factors that shaped individual student behavior. Several informants narrated the craze among the younger generation to be considered as the *"IT guru"* who influenced others among them. This social pressure to fit accounted for most of the younger generation's eventual violations of existing policies. For example, the ability to install a cracked software or pirated software within the university network against the policies expressed as common among the technically oriented students.

3.3.4 Educational background

Some of the informants also explained the effect on the educational background on how students and the staff behaved. Engaging those who were "*…more knowledgeable in the area of information systems…*" proved to be tricky because it bordered on both extremes. Handling members who knew how to evade the processes as well as handling those who understood the rationale towards certain measures these extremes.

3.4 Internal Organizational Strategies (Awareness program, Capacity development, Deterrence Control mechanisms)

The results also showed that international organizational strategies played a role in shaping how policies were complied with to some extent. As seen in Figure 4*Figure 4*, initiatives such as awareness programs, capacity development, and deterrence control mechanism emerged as variables that enabled policy compliance behavior.

3.4.1 Awareness program

Several informants mentioned that there was a strong awareness program by the management. For instance, several informants highlighted the *"…existence of several awareness programs…*" that were implemented during new members' initiation which drove compliance to information security policies.

3.4.2 Capacity development,

Other informants expressed the capacity development as among the initiatives that their respective universities initiated to raise the level of compliance. It emerged that the universities empowered their members to be champions of information security policy compliance through awareness training. In support, several informants asserted that they have had "*…fewer incidents of information security breaches because they are well equipped with the knowledge to understand how to be proactive while performing their jobs*." Another informant also narrated how "*The security section that deals now strictly with one of the things to enact is that they have been undertaking a lot of training on security and they are also implementing international standards in terms of a framework on security*".

3.4.3 Deterrence Control mechanisms

Institutional control mechanisms and processes were also expressed as one other way that contributed to the success of information security policy compliance. Many of the informants expressed the roles played by deterrence efforts such as "*…usage of staff ID number and student ID numbers as a way of logging in to the network…*" as a one way to deter would-be violators.

3.5 Management support

Management support came out as one of the strong pillars that several interviewees said was crucial to the success of the initiatives that were in place as shown in Figure 5. This, according to the interviewees, was complemented by the "*…culture of management leading by example to support information security initiatives…*" For instance, comments such as *"…The management also is in full support and this gives us the best environment to succeed…"* and *"…Management is very keen on ICT because the way ICT works here, much as it is a department in central administration is more [or] less an independent entity which is funded, and it has a budget…." Among others was very prominently* pronounced among staff and students alike.

3.6 External Organizational (Regulatory authorities, ISO certification, and standards, Best practices from peers)

As seen in Figure 6, external influence emerged as one other factor that informed how organizations strategized on internal policy compliance. Variables such as regulatory authorities, ISO certification standards, and best practices from peers emerged.

3.6.1 Regulatory authorities

Regulatory authorities emerged as one influencer of how the university management formulated its policy and strategies regarding policy compliance. Informants suggested that the management would consider what they are bound by from the legislative and regulative perspective before they decided on a strategy. One informant would put it this way, *"…we identify a list of documents that we think would be important in impacting the process from the constitution to specific standards concerning ICT that are given by the ICT…."*

3.6.2 ISO certification and standards

External certification standards also emerged as a factor that "*…played a role in shaping how the management formulated their policies and ensures compliance….*" Cognizant of the underlying fact that the policies are not made in a vacuum, to be at the top of the standard, processes, and control need to be evident as laid out in various certification standards. As such, the universities seemed to have opted to consider these standard rules as part of the basis to shape their initiatives and strategies.

3.6.3 Best practices from peers

Another emerging aspect of *external factors* came in the form of peer influence and best practices. The management expressed the role played by "*…other equal institutions in the industry and outside on how best to manage information security-related issues….*" The "*…learning experience…*" was expressed as key in

planning and strategizing on how best to enhance information security culture within the universities.

4.0 Discussion and Implications

The two case universities had an established information security policy compliance culture as supported by the results. We also established the various factors and their relationship that established information security culture. Based on the above results, we established a theoretical model that explains the relationships between various constructs and information security policy compliance culture, depicted in Figure 7.

Our findings broaden the existing models by incorporating the behavioral, organizational, and external drivers towards information security policy compliance construct. The results indicate explanatory evidence of how information security policy compliance culture (ISPCC) can be achieved in organizations.

Figure 7: Theoretical Model for Enhancing Information Security Policy Compliance CultureThis multi-level theoretical model explains the key relationships between ISPCC and behavioral trends, demographic traits, internal organizational initiatives, management support, and external organizational influences, which is discussed in this section.

4.1 Individual Behavioral Trends

Institutions can enhance compliance culture by inwardly looking at its members' behavioral tendencies. Perceptions of how information security policies will impact on their security appear to be an important factor to be considered. By making it easier for their members to follow the processes and protocols touching on information security, institutions will be reducing non-compliance practices. Similarly, by ensuring a positive attitude towards information security policies facilitated by the management that understands its members, institutions would be helping in enhancing compliance culture due to inculcation of positive attitude from its members. These would make it possible for members to shift from non-compliance to increased rate of compliance because of the: perceived ease of applying the policies; perceived reduced risks of complying with policies; and positive attitudes towards management.

Similar findings have also been argued by (Workman, et al., 2008) in which the authors highlighted how perception by employees could shape the net acceptance of a situation in an organization. With regards to attitude, findings by (Ifinedo, 2014) and (Safa, et al., 2016) depict individual attitude as an important aspect that can shape information security compliance by individuals. Another study that also supports our finding is that of (Johnston & Warkentin, 2010) perceived threat severity as a contributor to information security compliance behavior. The same kind of narrative can be seen in the work by (Sommestad & Hallberg, 2015) in which the authors discussed at length the role threat appraisal process played in improving information security compliance intention.

4.2 Individual Demographic Interventions

We submit that moderators of an individual's behavior would equally be important. As evident from the findings, handling of members of different maturity levels, either age-wise or reasoning, by managers would be critical to successfully enhance policy compliance. Understanding the social background of all members would enable information security managers to factor in contingencies to understand how to shape their policy strategies. The findings also suggest that information security managers need to consider the environment that members are into a factor in the social pressure that may be exerted upon the members. These could help the practitioners to avert possible vulnerabilities that would be as a result of social pressures upon members. The educational background of the members also appears to be an important factor to consider. From the findings, we observe that by understanding the educational background, managers would be able to foresee the probable hotspots for violations and strategies on mitigation steps.

Similar studies also exist that support our findings on demographic trends. For example, (Whitty, et al., 2015) found that individuals at lower age were more likely to pose vulnerabilities of information security compliance than more senior employees. With regards to social upbringing, (Herath & Rao, 2009), (Siponen & Vance, 2010), and (Hu, et al., 2011) all closely agree to the role society plays in informing individual's choices and interactions. Social pressure has been discussed at length (Herath & Rao, 2009) in which social pressure is depicted as a moderating factor in individuals' interactions with information security policies. Another pointer to the relationship that social pressure has on information security policy compliance was discussed by (AlKalbani, et al., 2015).

4.3 Internal Organizational Strategies

Our findings also show that awareness remains a vital component in creating an information security policy compliance culture. Information security managers, therefore, need to create more intuitive awareness campaigns to convert more members into champions of policy compliance. This goes hand in hand with capacity building. The more members are empowered to know how to respond to information security challenges the better

equipped they will be to fight non-compliance. However, this study also finds that deterrence plans are equally important to push back any would-be violators of the policy. This way, information security violations are constantly minimized.

Awareness programs in organizations have been linked to the success of information security management in organizations, (D'Arcy, et al., 2009). Similarly, (Bulgurcu, et al., 2010) and (Puhakainen & Siponen, 2010) support the same line of discussion by indicating that the awareness program in organizations enhances information security-conscious behavior and compliance behavior respectively. Regarding capacity building, building employees' capabilities initiatives, was argued to be a factor in influencing information security compliant behavior (Ifinedo, 2014). In applying the General Deterrence Theory, (Chen, et al., 2014) found that deterrence controls with reward and punishment acted in a way to enhance compliance with information security policies. Penalties, according to (Herath & Rao, 2009) was also considered to shape an individual's compliance behavior. A study by (Siponen & Vance, 2010) also related informal sanctions to information security violations.

4.4 Management support

One important moderator to internal organizational strategies was management support. This is important because the findings suggest that good policies excel when there is strong support from top-level management. Financial backing, leading from the front, adoption of key performance indices among others are just some of the examples of how top-level management can support information security initiatives.

Similar supporting work exists that management role is crucial. For example, Herath and Rao argue that the availability of resources, especially in the form of financial and budgetary allocation, to some extent, has an impact on information security compliance strategies, (Herath & Rao, 2009). Similarly, (Hu, et al., 2012) argued that individual top management actions influenced how others in the hierarchy behaved. This supports the notion that leading from the front would act as a moderating factor to successful organizational initiatives.

4.5 External Organizational

The findings also suggest that organizations need not only to look inwardly but also to consider what the outside does or demands. This was evident in the results that showed that the two universities' management was always conscious of what the regulatory authorities expected of them. The same was also the case with the standards that the two universities subscribed to. Learning from peer institutions also would help information security managers to get the best of practices out there and adopt or modify to shape how its members comply.

Other studies that also support our findings can be found in a study by Hu, Hart, and Cooke on coercive pressure such as the one by regulatory authorities. In their argument, coercive pressure was found to impact on management's decisions to streamline actions and strategies towards what is required at large, (AlKalbani, et al., 2017). According to (Hu, et al., 2007), coercive pressure such as those from regulatory was fronted as influencers of how organizations strategized. Normative pressure can also be seen in the extant work by (Hu, et al., 2007). The authors highlighted the role played by external normative pressure that forces managers to adopt the strategies geared towards achieving what is perceived as normal. Similar arguments are made by (Cavusoglu, et al., 2015) in which the authors found normative pressure to have some influence on organizational strategies. According to (AlKalbani, et al., 2017) mimetic pressure was found to influence organizational individual strategies.

4.6 Summary of the Discussion

We summaries by identifying a new factor that explains the information security compliance culture. demographic interventions appear to be minimally covered in extant literature. We also find the educational background to be minimally covered in the extant literature. As already observed in the extant literature, many studies have not dwelt a lot on demography factors that might have had impacts on information security policy compliance. Likewise, few have considered to explore the aspect of educational background in terms of how it can impact on behavior towards ICT policy compliance.

4.7 Contribution of this Study to the Body of Knowledge

In terms of theoretical mapping, we submit that our research attempts to address several theoretical entry points and elicits further queries that would provide a rich niche to be explored further. Several theories have been applied in the study of information security compliance such as the ***Deterrent Theory***, (Kennedy, 1983), ***Institutional Theory***, (DiMaggio & Powell, 1983)., ***Theory of Planned Behavior***, (Ajzen, 1991), among others as can be seen in works by, (Pahnila, et al., 2007), (Shareef, et al., 2009), (Bulgurcu, et al., 2010), (Gundu & Flowerday, 2013). Our study has attempted to provide a model that integrates from these theories in one theoretical multi-level model.

Secondly, our Grounded Theory approach allowed new constructs namely, (Individual Demographic Interventions), to emerge from rich qualitative and theoretical outcomes grounded in data. In practice, this will

also open the research doors to many other researchers to consider this approach as well.

5. Conclusion and Recommendations

It is our submission that based on the explorative study, information security policy management needs to factor in more than just the usual technological processes. Based on our findings, an integrated approach would serve best to address the mitigation strategies by injecting a clearer initiative on how to handle information security non-compliance. This would include considering various behaviors of the organization, their risk attitude, behavior as well as the general demographics. Further, the role of managerial interventions in the usual arena of competing resources would enhance the uptake of ISP projects within organizations. Another important consideration is the consideration of the external influences to the entire ISP strategy and the emergence of organizations.

For practitioners, the research comes in handy to enhance the already expected roles of improving information security. This can be accomplished by looking at multiple ways of handling cases of demography, individual behavior, organizational strategies, and external influences to shape their policy strategies. For example, practitioners can adopt strategies that identify demographic interventions that would have positive moderation effects of individual behaviors. Individual behavioral trends can be taken into consideration by practitioners to enhance compliance by the members and in coming up with strategies that will create buy-in for the ICT policies. Practitioners can also keep open to best practices while keeping a keen eye for the external interventions that may shape how best to strategize on ICT policy compliance. Organizational strategies based on external factors and behavioral trends of the members can help the practitioners be more forward-looking on how they strategize their ICT policy compliance strategies. Practitioners can also benefit from the model by encouraging management support to boost the morale of the members towards ICT policy compliance.

Further work could involve proceeding with validating the developed model quantitatively. Also, since this study covered only institutions of higher learning, we recommend that future studies can consider other populations that are not in the academic. This would address the triangulation component of the results and build on what we generated.

References

Ajzen, I., 1991. *The Theory of Planned Behavior.* s.l.:s.n.

AlKalbani, A., Deng, H. & Kam, B., 2015. *Organisational Security Culture and Information Security Compliance for E-Government Development: The Moderating Effect of Social Pressure. PACIS.*. s.l., s.n.

AlKalbani, A., Deng, H., Kam, B. & Zhang, X., 2017. Information Security Compliance in Organizations: An Institutional Perspective. *Data and Information Management,* 1(2), p. 104–114.

Amankwa, E., Loock, M. & Kritzinger, E., 2018. Establishing information security policy compliance culture in organizations. *Information and Computer Security,* 26(4), pp. 420-436 .

Bulgurcu, B., Cavusoglu, H. & Benbasat, I., 2010. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly,* 34(3), pp. 523-548.

Cavusoglu, H., Cavusoglu, H., Son, J. & Benbasat, I., 2015. Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management,* 52(4), pp. 385-400.

Charmaz, K., 2008. *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis.* New Delhi: SAGE Publications Inc..

Chen, Y., Ramamurthy, K. & Wen, K., 2014. Organizations' Information Security Policy Compliance: Stick or Carrot Approach?. *Journal of Management Information Systems,* 29(3), pp. 157-188.

D'Arcy, J., Hovav, A. & Galletta, D., 2009. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research,* 20(1), pp. 79-98.

DiMaggio, P. J. & Powell, W. W., 1983. The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review,* 42(2), pp. 147-160.

Gundu, T. & Flowerday, S. V., 2013. Ignorance to Awareness: Towards an Information Security Awareness Process. *South African Institute af Electrical Engineers,* pp. 69-79.

Herath, T. & Rao, H. R., 2009. Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. *Decision Support Systems,* 47(2), pp. 154-165.

Herath, T. & Rao, R. H., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems,* 18(2), pp. 106-125.

Hu, Q., Dinev, T., Hart, P. & Cooke, D., 2012. Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences Journal,* 43(4).

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

Hu, Q., Xu, Z., Dinev, T. & Ling, H., 2011. Does Deterrence Work in Reducing Information Security Policy Abuse By Employees?. *Communications of the ACM,* 54(6), pp. 54-60.

Ifinedo, P., 2014. Information systems security policy compliance: An empirical study ofthe effects of socialisation, influence, and cognition. *Information & Management,* 51(1), p. 69–79.

Johnston, A. C. & Warkentin, M., 2010. Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly,* 34(3), pp. 549-566.

Kennedy, K. C., 1983. *A Critical Appraisal of Criminal Deterrence Theory.* s.l.:Michigan State University College of Law.

oTranscribe, n.d. *oTranscribe.* [Online] Available at: https://otranscribe.com/

Pahnila, S., Siponen, M. & Mahmood, A., 2007. *Employees' Behavior towards IS Secur ity Policy Compliance.* s.l., IEEE.

Preston, T. & Jorgen, S., 2016. Constraining or Enabling Green Capability Development? How Policy Uncertainty Affects Organizational Responses to Flexible Environmental Regulations. *British Journal of Management,* 28(4), pp. 649-665.

Puhakainen, P. & Siponen, M., 2010. Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly,* 34(4), pp. 757-778.

Safa, N. S., Solms, R. V. & Furnell, S., 2016. Information security policy compliance model in organizations. *computers & security 56,* 56(2016), pp. 1-13.

SANS Institute, 2017. *Defending Against the Wrong Enemy: 2017 SANS Insider Threat Survey,* s.l.: SANS Institute.

Shareef, M. A., Kumar, V., Kumar, U. & Hasin, A. A., 2009. *Theory of Planned Behavior and Reasoned Action in Predicting Technology Adoption Behavior.* Hershey, PA: IGI Global.

Siponen, M. & Vance, A., 2010. Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly,* 34(3), pp. 487-502.

Sommestad, T. & Hallberg, J., 2015. The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information and Computer Security,* 23(2), pp. 200-217.

Sommestad, T., Karlzén, H. & Hallberg, J., 2019. The Theory of Planned Behavior and Information Security Policy Compliance. *Journal of Computer Information Systems,* 59(4), pp. 344-353.

Whitty, M., Doodson, J., Creese, S. & Hodges, D., 2015. Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychol Behav Soc Netw,* 18(1), p. 3–7.

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

Table 1: Profile of interviewees indicating their role at the university as students, ICT, and normal staff

	University	Role at the University
Informant 1	University A	Staff (Administrative)
Informant 2	University B	Staff (Administrative)
Informant 3	University B	Staff (Management level, ICT)
Informant 4	University A	Staff (Management level, ICT)
Informant 5	University B	Staff (Technician Level, ICT)
Informant 6	University B	Student (ICT)
Informant 7	University A	Staff (Administrative)
Informant 8	University A	Staff (Technician Level, ICT)
Informant 9	University A	Student
Informant 10	University A	Student
Informant 11	University B	Student (ICT)
Informant 12	University B	student
Informant 14	University B	Student
Informant 15	University A	Student
Informant 16	University A	Staff
Informant 17	University B	Staff (Technician Level, ICT)
Informant 18	University A	Staff
Informant 19	University B	Student
Informant 20	University B	Student

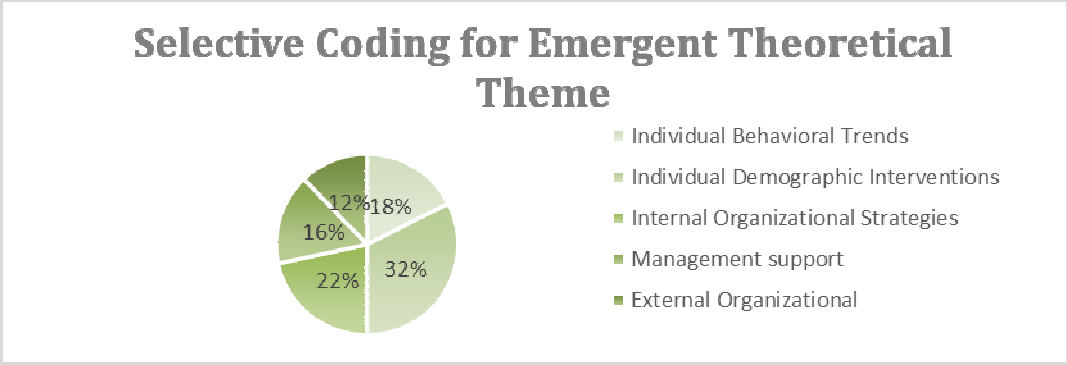

Figure 1: Chart showing Number of Supporting Selective Coding for Emergent Theoretical Themes

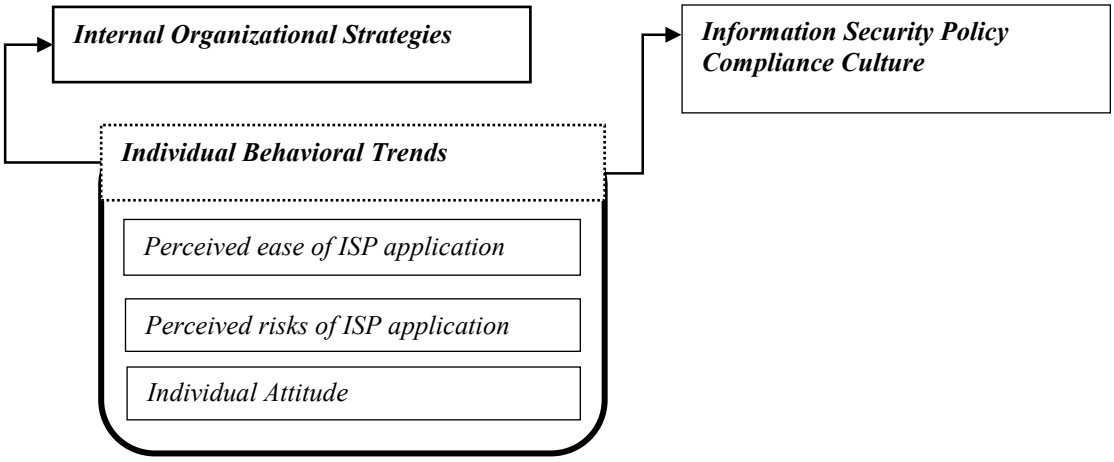

Figure 2: Influence of individual behavioral trend on internal organizational strategies, and information security policy compliance culture (Source: Research)

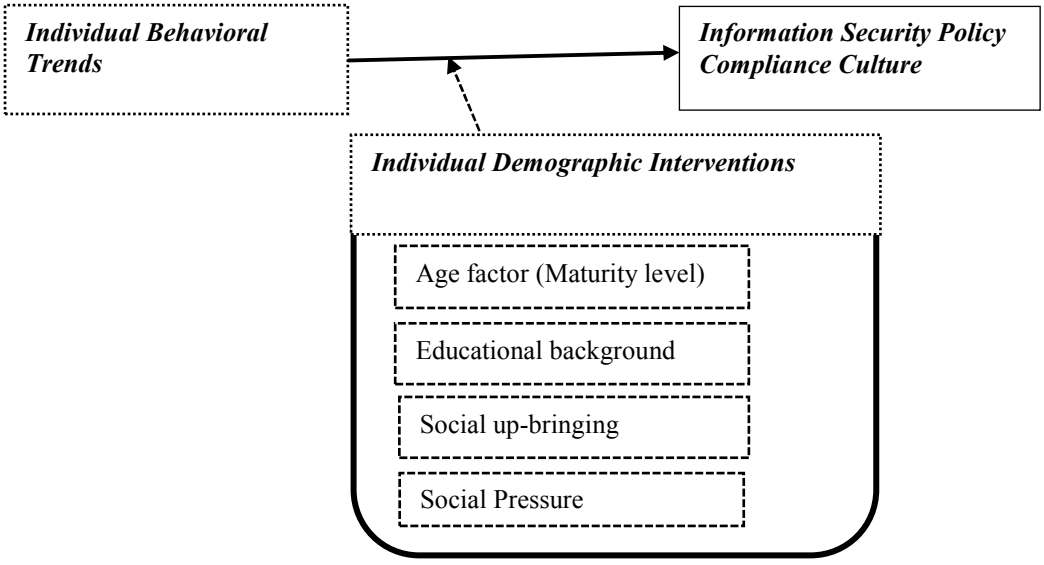

Figure 3: Influence of individual demographic interventions on the relationship between individual behavioral trends and information security policy compliance culture

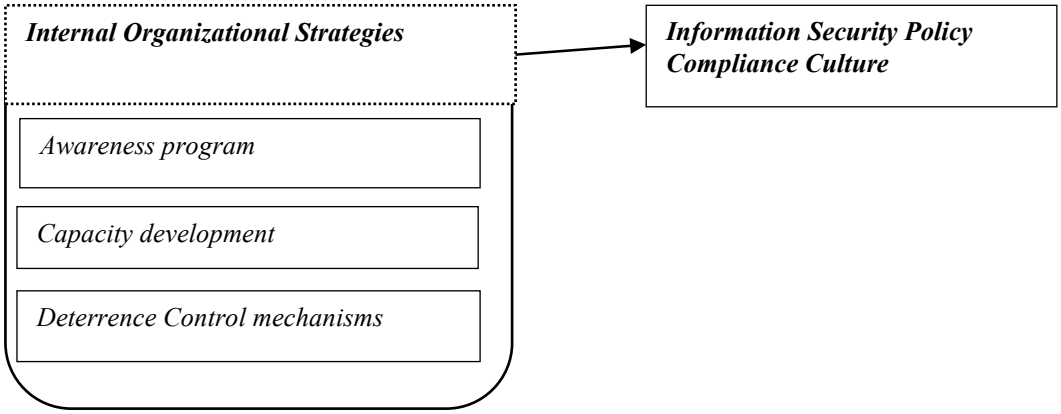

Figure 4: Relationship between information security policy compliance culture.

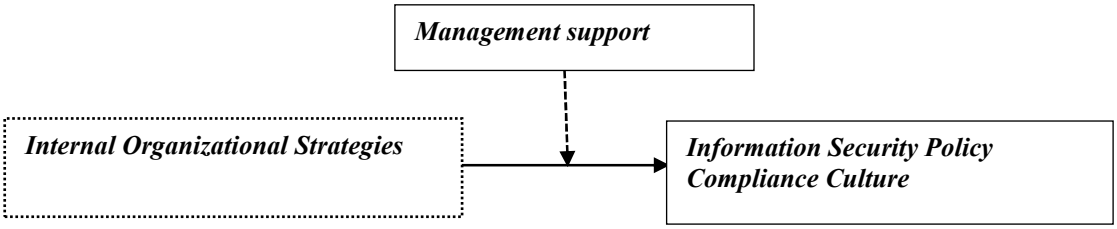

Figure 5: Influence of management support on the relationship between internal organizational strategies and information security policy compliance culture

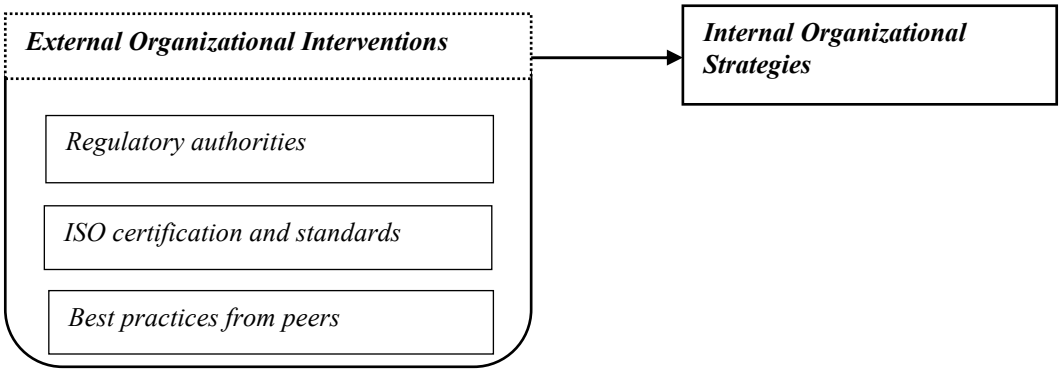

Figure 6: Relationship between external organizational interventions and internal organizational strategies.

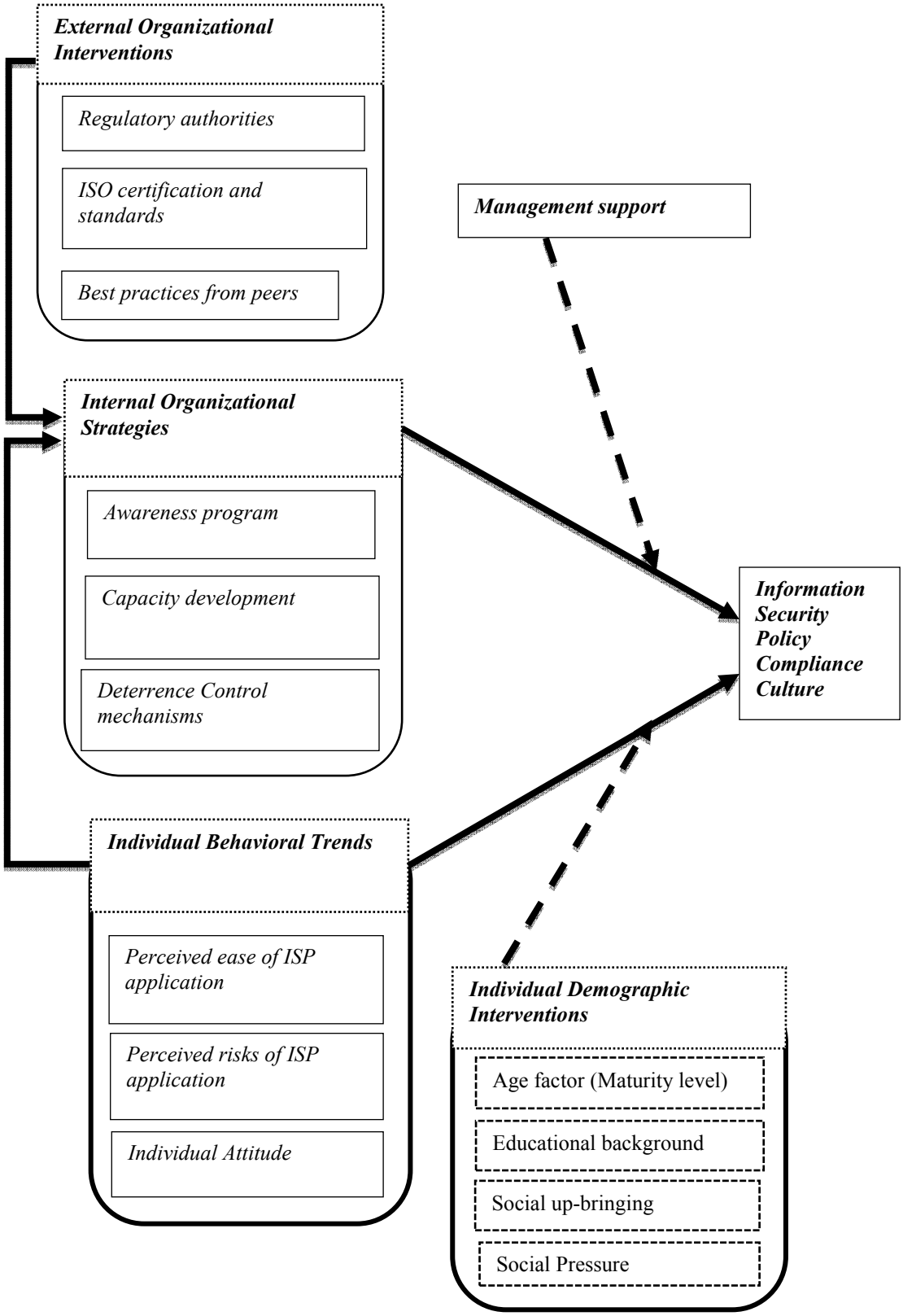

Figure 7: Theoretical Model for Enhancing Information Security Policy Compliance Culture