Aug 9th, 12:00 AM

Investigating the Impact of Organizational Culture on Information Security Policy Compliance: The Case of Ethiopia.

Kibrom Tadesse Ejigu
Addis Ababa University, kibrom.tadesse@astu.edu.et

Mikko Siponen
University of Jyväskylä, mikko.t.siponen@jyu.fi

Tilahun Muluneh Arage
Addis Ababa University, tilahun.muluneh@aau.edu.et

Investigating the Impact of Organizational Culture on Information Security Policy Compliance: The Case of Ethiopia

Emergent Research Forum Papers (ERF)

Kibrom T. Ejigu
Addis Ababa University
kibromtadesse@gmail.com

Mikko T. Siponen
University of Jyväskylä
mikko.t.siponen@jyu.fi

Tilahun M. Arega
Addis Ababa University
tilahunmuluneh@gmail.com

Abstract

Information security is one of the organizations' top agendas worldwide. Similarly, there is a growing trend in the kinds and rate of security breaches. Information security experts and scholars concentrate on outsiders' threats; conversely, insiders are responsible for most of the security breaches in organizations. Further, the majority of information security research findings are limited to solutions that are technically focused. However, it is now recognized that the technological approach alone does not carry the security level needed. So this led researchers to embark on socio-technical approaches. Thus, this study explores organizational culture's effect on employees' intention to comply with information security policies (ISP). A rational choice theory and a computing value framework construct are used to build and evaluate an empirical ISP compliance model. A survey method used to collect data from Ethiopia.

Keywords

Information Security Policy compliance, Organizational Culture, Rational Choice Theory, Computing Value Framework

Introduction

Information Security (IS) has become the topmost concern of organizations though IS breaches continued (Vance et al. 2012). These breaches have a negative impact, and it is necessary to understand the causes and intentions of these breaches and then find suitable solutions. Thus, as one solution, organizations enact information security policies (ISPs) to direct employee behavior to combat possible IS threats. Unfortunately, employees' non-compliance with ISPs continues to be the main concern for organizations worldwide (Pahnila et al. 2007; Vance et al. 2012).

Various reasons are given to address the question, "Why do employees lack ISP compliance?" (Bulgurcu et al. 2010; Herath and Rao 2009). Although these studies have found many factors influencing ISP compliance (for example, perceived benefits, moral beliefs, formal sanctions, and informal sanctions) few have concentrated on the effect of culture on ISP. Moreover, an essential factor to consider is organizational culture (OC) (Chen et al. 2015). Moreover, the attention given to information security needs does not seem to be provided in every part of the world (Crossler et al. 2013). Little has been done to examine individual behavior's cultural dimensions towards ISPs for developing countries, especially in Africa (Tilahun and Tibebe 2017). It is also easy to understand that behavioral IS studies originate mainly from countries in Europe, Asia, and North America. For example (Chen et al. 2015; Connolly et al. 2017; Hooper and Blunt 2020; Johnston et al. 2016; Kim and Han 2019; Moody et al. 2018; Rajab and Eydgahi 2019; Siponen et al. 2010; Yazdanmehr and Wang 2016) gathered data from the United States, South

Korea, Finland, and New Zealand. How can the studies' output be adapted to countries with a particular organizational and national culture, such as Ethiopia?

The International Standardization Organization/International Electro technical Commission (IEC/ISO) is an international standardization body that issues standards in various fields, including information security. For example, ISO/IEC 27001-2 Security Compliance allows organizations to ensure compliance with organizational policies, rules and regulations, procedures, and standards (Schweizerische 2013). However, the question is, can we apply these kinds of ISP standards directly? We assume that the response is no, that if an organization plans to create an efficient atmosphere for information security, it does not separate organizational and national culture (Chaula 2006). All of this shows the gaps that studies need to resolve.

Research Background and Objective

Organizations provide more resources to create a stable IS environment. Often, they focused on the technological aspects of hardware and software (Ifinedo 2012). Since they believe that IS threats come primarily from outsiders of the organization, the technical aspects' application would cause the issue to disappear (Crossler et al. 2013). However, previous studies have recommended that more threats arise as a result of internal threats. (Bulgurcu et al. 2010; ifinedo 2012) studies also suggest that a favorable IS condition cannot be created solely using technical tools; equal attention must be paid to the human part and, more importantly, to internal threats. In this report, an insider threat is described as anyone who has the privilege of accessing data and information systems, facilities, and networks of the organization (Ngungoh 2020). Summary reports on insider risks and IS abuses from an international and local viewpoint are presented below.

According to the Ponemon Institute's 2020 Global report, the number of insider threats has increased by 47% in just two years, from 3,200 in 2018 to 4,716 in 2020. Simultaneously, from $8.76 million in 2018 to $11.45 million in 2020, these accidents' expenses rose by 31 percent (Saxena et al. 2020). Several reports worldwide have pointed out that insiders have been the most-cited culprits of information security breaches. For example, a survey by Egress (2020) found that, out of 5001 workers, 46% said they had deliberately violated organizational policy. Information security studies in Africa are relatively minimal (Tilahun and Tibebe 2017). A survey conducted by the Serianu Cyber Threat team in some African countries (Nigeria, Uganda, Tanzania and Kenya) found that 50 percent of losses of all direct costs and 32 percent of total costs are due to insider attacks, measured at USD 179,000,000 and USD 284,400,000 per year, respectively (Adomako et al. 2018).

The above reports presented how insider attacks pose a significant risk to their companies worldwide and in Africa. When we look at Ethiopia's experience, we saw the inadequacy of information security studies (Arage et al. 2015). Consequently, there is scarcely reported data showing the potential occurrence and exact impact of IS threats in Ethiopia. It is therefore hardly challenging to provide information on non-financial and financial damages incurred by insider attacks. As a result, the present researcher carried out a preliminary assessment through interviews with randomly selected managers and information security officers from commercial banks, universities, and other institutions. Based on the initial review of the response from the security officers listed above, there are indications that there are security breaches in the institutions. For example, a bank clerk from Ethiopia's commercial bank has revealed that he has built a fake user account to withdraw and move 9.9 million Birr from different accounts using his right of access. He also revealed that he had made fake user IDs to hack the bank's supervisors' passwords. In another case of the ISP breach, two bank workers removed cash from cash machines, misused access codes or passwords, or broken banking networks using stolen PINs (Hailu 2015). Besides, the non-compliance of an employee to the Ethiopian customs commission ISPs costs the customs commission 13,000,000 Birr (Arage et al. 2015).

This research is attempted to understand information security's human dimension using the relational choice theory (RCT) combined with the computing value framework (CVF). In this research, we use CVF for the following reasons. The first reason, we think it is more suitable parsimonious for the goals and background of this research, given our task of integrating two theoretical frameworks. Moreover, this model has served as a useful instrument to test the relationship between cultural values of organizational and individual behavior in IS and other quantitative studies (for example (Chang and Lin

2007; Jones et al. 2005; Whipple 2015). The second reason relates to the definition of organizational culture; according to Leidner & Kayworth's (2006) definition of OC, it "represents a manifestation of a culture that signifies espoused beliefs identifying what is important to a particular cultural group." Thus, this study follows this model because it's a value-based organizational culture framework. The CVF and its four key culture dimensions (innovativeness, cooperativeness, consistency, and effectiveness) were used to measure organizational culture. Therefore, our key research objective is to build and test an empirical model that illustrates the organizational culture's moderating impact on perceived benefits, formal sanctions, informal sanctions, shame, and moral belief in employees' intention to comply with the ISP. In addition, we set out to investigate the direct effect of these contracts on employees' intention to comply with ISPs. The research model and hypotheses are presented and described below.

Research Methodology and Hypothesis Development

This study follows the positivist epistemological view since this research aims to build and evaluate a model that contains a testable hypothesis. This research uses Cheng and Ling's (2007) OC-adapted CVF model from Quinn (1999) to integrate the frameworks. We assume that it is more fitting and economical for the aims and context of this study. It has also been rigorously validated in previous IS and OC studies (Di Stefano et al. 2019; cheng and Ling's 2007). This research uses a form of questionnaire-based data collection. In addition to the traditional survey technique, the current research will investigate employees' intention towards ISPs using a scenario method. Scenario-based research is well suited to studying issues that measure or involve ethical/unethical behavior (Tilahun and Tibebe 2017). The sample will come from organizations that have developed ISPs in the cities of Ethiopia. Respondents will be chosen randomly from each organization. We will use the Structural Equation Modeling (Tilahun and Tibebe) and the Statistical Package for the Social Sciences (SPSS) package with Analysis of Moment Structures (Amos) to run various SEM models.

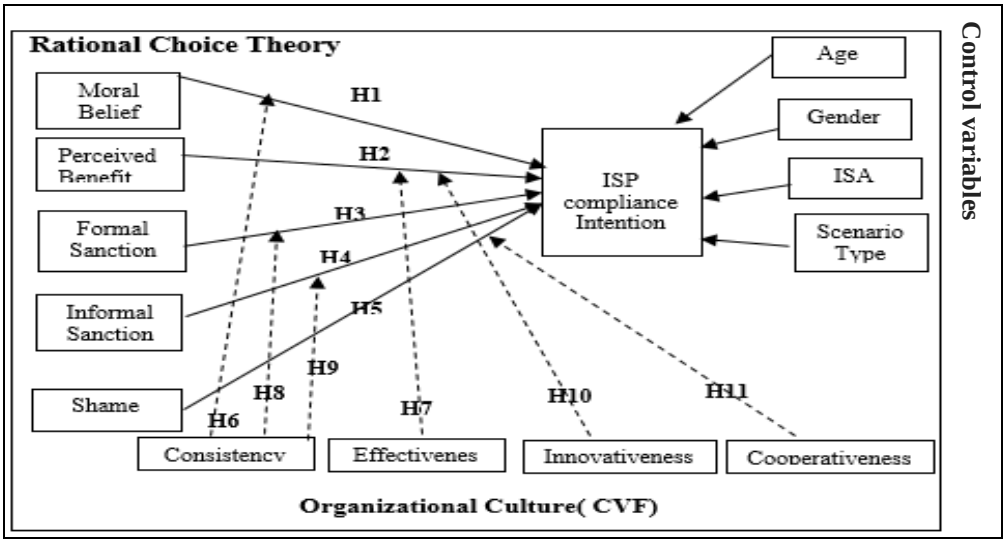

Figure 1: The Proposed Research Model

Moral beliefs are essential to the context of information security in the ISP compliance literature since choices regarding information security policies include a moral dimension (Myyry et al. 2009). Similarly, Vance et al. (2012) have analyzed compliance and confirmed that moral belief is a strong predictor of individual compliance with the ISP. Thus, the following hypothesis is posited: **H1: Moral belief is positively related to employees' intention towards ISP compliance.**

Various empiric research in many fields, such as the unsafe computing environment, compliance with information security policies, and Internet abuse, show that individuals abide by rules and regulations when they know the perceived advantage of compliance is high. Besides, the research focused on rational

choice theory often indicates that perceived benefits have been a good predictor of compliance (Bulgurcu et al. 2009; Vance et al. 2012). The following hypothesis is therefore posited:

H2: Perceived benefit of compliance is positively related to employees' intention towards ISP compliance.

Researchers have tried to identify whether or not the formal sanction reduces information security issues and have found that the more undesirable behaviors avoided by implementing formal sanctions, the more severe or effective the sanction. In this regard, multiple studies have shown that formal sanctions have a high impact on reducing security breaches (Herath and Rao 2009; Pahnila et al. 2007a). In other words, it increases compliance with information security policies. Thus, the following hypothesis is posited: **H3: Formal sanction is positively related to employees' intention towards ISP compliance.**

Study findings present mixed results on the impact of informal sanctions. Studies have shown the effect of informal sanctions on reducing non-compliance (Pahnila et al. 2007a; Pratt et al. 2006). However, several researchers have indicated that informal sanctions have little effect on ISP compliance (Li et al. 2010; Pahnila et al. 2007b). Therefore, the following hypothesis has been posited: **H4: Informal sanction is positively related to employees' intention towards ISP compliance.**

In the D'Arcy et al. (2011) research, shame had a positive impact on reducing the likelihood that a person will participate in criminal activities. Siponen & Vance (2010) also illustrated the effect of shame on reducing computer abuse. Therefore, the following hypothesis is posited: **H5: Shame is positively related to employees' intention towards ISP compliance.**

Consistency culture emphasizes control orientation, and the expected behavior here is strict compliance behavior to the various policies and procedures. When an employee feels that their company is behaving in a manner compatible with their moral values, they are motivated to comply with ISPs. Conversely, in organizations where actions are contradictory to ISPs but perceived by people as not immoral, it is more challenging to get people to comply with ISPs (Tyler and Blader 2005). Similarly, employees determine the morality of corporate policies and practices and respond to these policies and procedures in moral terms (Paternoster and Simpson 1996). Thus, the following hypothesis is formulated: **H6: Consistency culture strengthens the positive effect between moral beliefs and compliance intention.**

Effectiveness culture is conceptually close to the norm of competition since it is a practice whereby one attempts to damage others even at the expense of losing one's earnings (Di Stefano et al. 2019). Yukl (2002) supports this view and argues that unethical behavior can occur more frequently in organizations with increased productivity and intense competition for rewards and promotion. Moreover, these behaviors are logical for employees because they estimate expected costs and benefits. In another study, Tyler, Callahan, and Frost (2007) showed that perceived values significantly affect law enforcement officers' rule compliance behaviors. Hence, we argue that this culture influences employees' intention to comply with ISP because of employee characteristics competing for accomplishing organizational objectives and get rewards and promotion. Thus, the following hypothesis is formulated: **H7: Effectiveness culture strengthens the positive effect between perceived benefits and compliance intention.**

The culture of continuity stands for control and adherence. It seeks continuity and control through adequate information and communication management within a company. In this kind of organization, the leadership style focuses on controlling employee's behavior through sanctions to ensure staff compliance with organizational policies (Di Stefano et al. 2019). According to Vance et al. (2012), a sanction is classified into formal sanctions known as explicit penalties and informal sanctions known as unstated social penalties for specific misbehavior forms. In the current study, both sanctions are considered. Hence, the following hypotheses are posited: **H8: Consistency culture strengthens the positive effect between formal sanctions and compliance intention.**

H9: Consistency culture strengthens the positive effect between informal sanctions and compliance intention.

In an Innovative-type organization, personnel who believe new ideas are operating do not want to adopt excessively restrictive policies. Additionally, employees continue their efforts as long as the efforts spent and the benefits are advantageous to push for innovation (Vance et al. 2012). Likewise, in ISP compliance studies, perceived benefits positively affect intention to violate ISPs because time-saving has been

described as the most significant incentive to break ISPs (Puhakainen 2006). Thus, we argue that innovative type organizations are resistant to efforts that block creativity, so the following hypotheses are posited: **H10: Innovativeness culture weakens the positive effect between Perceived benefits and compliance intention.**

Studies have shown that cooperation and group rewards are given more importance than individual contributions in a cooperativeness culture (Di Stefano et al. 2019). Employees choose to act for the interest of the groups. Collective harmful behaviors are strongly discouraged while rewarding prosocial behaviors (Di Stefano et al. 2019). Then, in the cooperativeness culture breaking groups' norms and beliefs lead to shame or guilty feeling. D'arcy, J., and Herath, T (2011) found that it deters individuals from engaging in illicit activities. Siponen and Vance (2010) hypothesized that shame has a negative effect on ISP violations within an organization. Thus, if we consider non-compliance with ISPs as breaking norms in the group, we can say that shame has a more substantial impact on cooperativeness culture to deter ISP non-compliance. We, therefore, hypothesize: **H11: Cooperativeness culture strengthens the positive effect between shame and compliance intention.**

Contribution

This study has several contributions. It applies a well-established theoretical framework that has mainly been employed in other countries' contexts but not in the Ethiopian context. So this is a novel contribution by offering a non-technological solution to ISP's practices in Ethiopian companies. Nowadays, Ethiopia's government has recently approved the National Digital Transformation Strategy – Digital Ethiopia 2025. Therefore, the model's constructs are essential in the Ethiopian context since the current research is one of the first studies in the Ethiopian context. Besides, it is believed that the research output in the African/Ethiopian context would make a valuable input to the development of IS theory and practice. The study results will allow security personnel, leaders, and policymakers to make better decisions to induce staff to comply with ISPs and develop ISPs that best fit their organizational culture. It also contributes to the IS problem to give a more behavioral explanation.

REFERENCES

Adomako, K., Mohamed, N., Garba, A., and Saint, M. 2018. "Assessing Cybersecurity Policy Effectiveness in Africa Via a Cybersecurity Liability Index," TPRC.

Arage, T., Bélanger, F., and Beshah, T. 2015. "Influence of National Culture on Employees' Compliance with Information Systems Security (Iss) Policies: Towards Iss Culture in Ethiopian Companies,").

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2009. "Effects of Individual and Organization Based Beliefs and the Moderating Role of Work Experience on Insiders' Good Security Behaviors," 2009 International Conference on Computational Science and Engineering: IEEE, pp. 476-481.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," MIS quarterly), pp. 523-548.

Chaula, J. A. 2006. "A Socio-Technical Analysis of Information Systems Security Assurance: A Case Study for Effective Assurance." Institutionen för data-och systemvetenskap (tills m KTH).

Chen, Y., Ramamurthy, K., and Wen, K.-W. 2015. "Impacts of Comprehensive Information Security Programs on Information Security Culture," Journal of Computer Information Systems (55:3), pp. 11-19.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," computers & security (32), pp. 90-101.

Di Stefano, G., Scrima, F., and Parry, E. 2019. "The Effect of Organizational Culture on Deviant Behaviors in the Workplace," The International Journal of Human Resource Management (30:17), pp. 2482-2503.

Hailu, H. 2015. "The State of Cybercrime Governance in Ethiopia," Article published on ResearchGate, available at https://www. researchgate.com

Herath, T., and Rao, H. R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," European Journal of Information Systems (18:2), pp. 106-125.

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," Computers & Security (31:1), pp. 83-95.

Li, H., Zhang, J., and Sarathy, R. 2010. "Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice Theory," Decision Support Systems (48:4), pp. 635-645.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study," European Journal of Information Systems (18:2), pp. 126-139.

Ngungoh, D. J. 2020. "Insider Threat in Government Organizations." Capitol Technology University.

Pahnila, S., Siponen, M., and Mahmood, A. 2007a. "Employees' Behavior Towards Is Security Policy Compliance," 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07): IEEE, pp. 156b-156b.

Pahnila, S., Siponen, M., and Mahmood, A. 2007b. "Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study," Pacis 2007 Proceedings), p. 73.

Paternoster, R., and Simpson, S. 1996. "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime," Law and Society Review), pp. 549-583.

Pratt, T. C., Cullen, F. T., Blevins, K. R., Daigle, L. E., and Madensen, T. D. 2006. "The Empirical Status of Deterrence Theory: A Meta-Analysis,").

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.-K. R., and Burnap, P. 2020. "Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses," Electronics (9:9), p. 1460.

Schweizerische, S. 2013. "Information Technology-Security Techniques-Information Security Management Systems-Requirements," ISO/IEC International Standards Organization).

Tilahun, A., and Tibebe, T. 2017. "Influence of National Culture on Employees' intention to Violate Information Systems Security Policies: A National Culture and Rational Choice Theory Perspective,").

Tyler, T. R., and Blader, S. L. 2005. "Can Businesses Effectively Regulate Employee Conduct? The Antecedents of Rule Following in Work Settings," Academy of Management Journal (48:6), pp. 1143-1158.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory," Information & Management (49:3-4), pp. 190-198.