Spring 6-10-2017

INFLUENCE OF NATIONAL CULTURE ON EMPLOYEES' INTENTION TO VIOLATE INFORMATION SYSTEMS SECURITY POLICIES: A NATIONAL CULTURE AND RATIONAL CHOICE THEORY PERSPECTIVE

Arage Tilahun
Addis Ababa University, tilahunmuluneh2006@yahoo.com

Tesema Tibebe
Addis Ababa University, tibebe.besha@gmail.com

INFLUENCE OF NATIONAL CULTURE ON EMPLOYEES' INTENTION TO VIOLATE INFORMATION SYSTEMS SECURITY POLICIES: A NATIONAL CULTURE AND RATIONAL CHOICE THEORY PERSPECTIVE

Research in Progress

Tilahun, Arage, Addis Ababa University, Ethiopia, Tilahunmuluneh2006@yahoo.com

Tibebe, Tesema, Addis Ababa University, Ethiopia, Tibebe.Besha@gmail.com

Abstract

The security of information systems has become one of the top agendas of business executives in economically developed nations. While the information systems security (ISS) world focuses on threats of external origin, most ISS breaches are caused by insiders. Both the amount of money allocated for ISS related activities and the number of ISS breaches are shown to increase in parallel. A majority of the investments and researches around ISS are limited to bring technically oriented solutions only. It is now realized that the technical approach alone couldn't bring the required level of ISS, and this led ISS researchers to embark on socio-technical approaches. In this respect, one of the critical social factors that has been given little emphasis is culture. Thus, this research investigates the impact of national culture on employees' ISS behavior. More specifically, it answers the question "what is the moderating impact of national culture on the influence of ISS countermeasures and other important variables on employees' intention to violate ISS policies?" We develop and test an empirical ISS compliance model, which is composed of security related rational choice theory and national culture constructs in the Ethiopian and USA context. Survey will be used to collect data.

Keywords: *General Deterrence Theory (GDT), Information Systems Security (ISS), Information Systems Security Policy (ISSP), Intention to Violate ISSP, National Culture, Rational Choice Theory (RCT), Insiders.*

1 Introduction

Despite the existence of security policies, protecting the ISS becomes a moving target for most organizations around the world (Sommestad et al., 2013). Most of the time, the ISS specialists and researchers have been focusing on threat of external origins (Magklaras et al., 2006); however, it is now becoming more apparent that most of the ISS threats are originated from insiders (D'Arcy et al., 2009; Hedstrom et al., 2013; Lowry and Moody, 2015).). The frequency or the number of occurrences is not the only indicator of the impact of insider incidents, but there are considerable financial costs attributed to legitimate user actions (Magklaras et al., 2006, Arage et al., 2016). Moreover, researchers like Magklaras et al. (2006) clearly stated that the internal incidents are here to stay and their mitigation should be a priority issue for IT professionals.

More recently, practitioners and academics have started to realize that ISS cannot be achieved through only technological tools and effective organizational ISS should emphasize users' ISS behavior (Hamill et al., 2005). Since this is a new area, the knowledge of end users' ISS behavior and factors affecting this behavior are at an embryonic stage (Herath & Rao, 2009b). In this regards, one of the most significant factors to shape human ISS behavior is culture (Schiffman & Kanuk, 1997). To this end, our study will bring rational choice theory (RCT) and national culture together to give a more behavioral explanation to the ISS problem.

Even though there exist some studies in the western culture that investigate the influence of national culture on employees' information systems security policy (ISSP) compliance, the literature is not very rich in this area. A few exceptions include the work of Dols & Silvius, 2010 (Europe) and D'Arcy et al., 2007 (USA and South Korea) that try to study how national culture influences the successful implementation of ISS countermeasures. Unfortunately, these two studies did not explicitly measure national culture at the individual level; rather they simply rely on the metrics given by Hofstede (1980) for the countries studied. Other researchers try to conduct cross-cultural studies of information security and privacy related issues. Examples include, Shore et al. (2001) studying attitudes toward intellectual property rights; Milberg et al. (1995) examining regulatory approaches to privacy; and Husted (2000) studying level of software piracy. But we need to bear in mind that these works did not explicitly study ISSP compliance at a broader level. Moreover, all of the above researches are conducted outside the developing country context (culture) and their output clearly show that measures that are found to be effective in one culture is found to fail in another culture. If an organization plans to develop a successful ISS culture, it should not be developed in isolation of national and organizational culture (Chaula, 2006). Thus, how can the output from these researches be applicable to a different culture like Ethiopia? This situation identifies a gap that needs to be bridged, and this study will be the first to address the issue by raising the question "To what extent, if any, national culture moderates the influence of security countermeasures (formal sanctions), perceived benefits, moral beliefs, and shame on employees' intention to violate ISSP?" To answer this question, this study will build and test an empirical model. The result of this research will have a paramount contribution to both the practical and theoretical world.

2 Background

ISS threats that are caused by insiders are not limited to developing countries; rather, it is a global problem. Hence, in the following paragraphs, we summarize important information related to insiders and ISS breaches from global and local (in Ethiopia) perspectives. In this research, insider is defined as "a person that has legitimately given the capability of accessing one or more components of IT infrastructure" (Magklaras et al., 2006, pp. 3).According to Mercury (2003), companies all over the world are losing more than US $2 trillion due to ISS breaches. Most of the breaches are caused by insiders; between one-half and threequarters of all ISS incidents originate from within the organization (Ernst & Young, 2003; Information Week, 2005; as cited in D'Arcy et al., 2007). Since insiders do have better access to the companies' secured information, they can bring catastrophic consequences to their company in terms of financial as well as non-financial aspects, such as: reputation, customers' confidence, and more (D'Arcy et al., 2009). The Cyber Security Watch Survey (2010) annual report indicates more than US $2 billion in losses to organizations due to ISS breaches between 1997 and 2007. According to the report, companies may continue to suffer more losses in the future given that the overall types of attacks are doubled in the specified time period. More recently, the Cyber Security Watch Survey (2012) annual report indicates that insiders attack increased from 41% in 2004 to 53% in 2011. In addition to this, according to a report by Verizon (2012), the ISS breaches caused by insiders increased on average from 33% (2004 -2007) to 48% (2009). To make matters worse, insider abuse of company IS is the second most frequent (44%) ISS problem next to virus incident (49%) and well above outsiders (29%) (Richardson, 2008). Because only a fraction of ISS incidents is actually discovered, the figures from different reports and researches may be lower than the actual facts (Hoffer & Straub, 1989; Whitman, 2003).

The above discussion clearly shows how insiders pose great threats to their organizational ISS at a global perspective. When we come to countries in the developing economy, we find that there is a lack of research in the areas of ISS breaches in such countries (Salahuddin, 2011). Thus, it is difficult to find out the actual financial as well as non-financial losses attributed to ISS breaches caused by insiders. In the case of Ethiopia, according to Arage et al. (2015), Ethiopian Revenue and Custom Authority is one of the companies that suffer the consequence of an ISS breach caused by their own employees. The authors discussed that the noncompliance of an employee to his company ISS policy costs the company 13,000,000Birr. In another incident of ISS breaches, the Ethiopian Airlines has terminated eleven employees working in different departments citing violation of the ISSP rules and procedures they were expected to abide by and abuse of the IS that they had privileged access to (Ethio_News_24, 2013). The alleged abuse of the IS is connected to its frequent flyer program called ShebaMiles, whereby Ethiopian Airlines customers can accumulate miles that would result in awards of free tickets, gifts and privileges. In addition to the financial losses, the above incidents may have also damaged the reputation of the companies. When we come to the banking sector, research found that the major barriers the Ethiopian banking industry faces in the adoption of electronic banking is ISS risk (Devamohan, 2008; Bultum, 2012). According to the authors, many customers have reported that sharing of their confidential information by employees has become a common problem around the financial institutions. According to Yeshak (Personal Communication, June 12, 2015), who is the ISS officer of the Commercial Bank of Ethiopia, insider violations of ISSP is a very critical problem and it costs the bank a lot of money and time. What should companies do to counter the security risks posed on their systems by their own employees?" there are many things that could be done, but this research will try to shed light on one of the basic but important factors: national culture. As can be understood from the above information, the ISS breach problem is increasing at an alarming rate. To this end, some researchers in Europe and the USA try to address the noncompliance problem by giving some level of emphasize for both technical and social factors that may have an impact on reducing the current noncompliance problem. In this regards, we can mention the work of Dols & Silvius (2010) in Europe and the work of D'Arcy et al. (2007) in the USA that try to investigate the influence of national culture on employees' compliance with ISSP. But when we come to Ethiopia, it is very difficult to get researches that try to shed light on the behavioral perspective of ISS. There is a particular lack of attention in the current IS literature about developing countries, and also how factors such as national and organizational culture, the information security environment, and the level of information security awareness (ISA), relate to individual's attitudes towards ISS and its management (Salahuddin, 2011). Almost all of the ISS research works conducted in Ethiopia recommend technological solutions to solve the ISS problems (Gardachew, 2010; Bultum, 2012) but nowadays technological solution alone couldn't bring the required level of ISS. In this regards, the literature shows that ISS cannot be achieved through only technological tools and effective organizational ISS should give emphasis for users' ISS behavior (Hamill et al., 2005). Thus, researchers in developing countries are expected to strive to know more about the influence of human ISS behavior in the process of bringing ISS compliance in organizations.

3 Theoretical Foundation and Prior Researches

To study employees ISS behavior, a number of theories have been used over the years. In this regards, theories such as: protection motivation theory (PMT) (e.g. Pahnila et al., 2007, Siponen et al., 2006; Workman et al., 2008), general deterrence theory (GDT) (e.g. Kankanhalli et al., 2003; D'Arcy & Hovav, 2007; D'Arcy et al., 2009; Harrington, 1996; Straub, 1990), and agency theory (e.g. Herath & Rao, 2009) are some of the main theoretical lens used to study ISS behavior. According to Li et al. (2010), the majority of studies in the ISS compliance area is based on GDT and /or PMT, which are mainly fear based strategies; that is, fear of sanction and threat to organization ISS. This will only give a partial explanation to the problem of ISSP violation (Vance & Siponen, 2012). Thus, in order to have a better view on "why employees violate ISSP?" we need to use theories that go beyond this scope. In this regard, RCT goes beyond this limitation and includes perceived benefits and moral beliefs as additional determinants of ISS compliance. On the other hand, there exist some scholars that criticize the RCT. In this instance, MacCumber argues that RCT is failing because it is not ethically neutral. He explained that RCT encourage individuals to engage in power and wealth collection, however, not all choices are economically driven and it might be driven by other values. But, as can be seen from the different constructs of RCT (particularly perceived benefits), we infer that the theory does not only focus on perceived economic benefit rather it encompass all sorts of benefits an individual might get by disobeying the rules and according to Bukaty (2012), MacCumber has oversimplified rationality. The RCT states that individuals will always go through a utilitarian calculation of perceived benefits, moral beliefs, shame, formal and informal sanctions when they make decisions towards obeying or violating rules (Vance & Siponen, 2012). Therefore, we believe that use the RCT as one of our theoretical lenses is justified and also appropriate. When we come to prior research works, there exists few studies in the area of ISS compliance that use RCT. In this regard, some works (e.g. Bulgurcu et al., 2010; Li et al., 2010; Siponen & Vance, 2012) go beyond the norm and analyze the ISS issues by using RCT into their empirical researches. All of these researches use samples from western cultures and hence the result of their research may not be valid for other cultures. According to D'Arcy et al. (2008), given the difference in terms of cultural dimensions, it is very important to bear in mind that users from different cultures might respond differently to the same types of ISS measures. In addition to this, Dinev et al. (2009) reported that national culture dimensions moderate the relationship between protective technologies and compliance, and they advise the inclusion of national culture when designing ISSP practice and technology. Hence, we believe that the choice of national culture as one of the theoretical lenses is appropriate. In this regards, to the best of our knowledge, our research is the first research to investigate ISSP violation issue from RCT and national culture perspective.

4 Research Model and Hypotheses

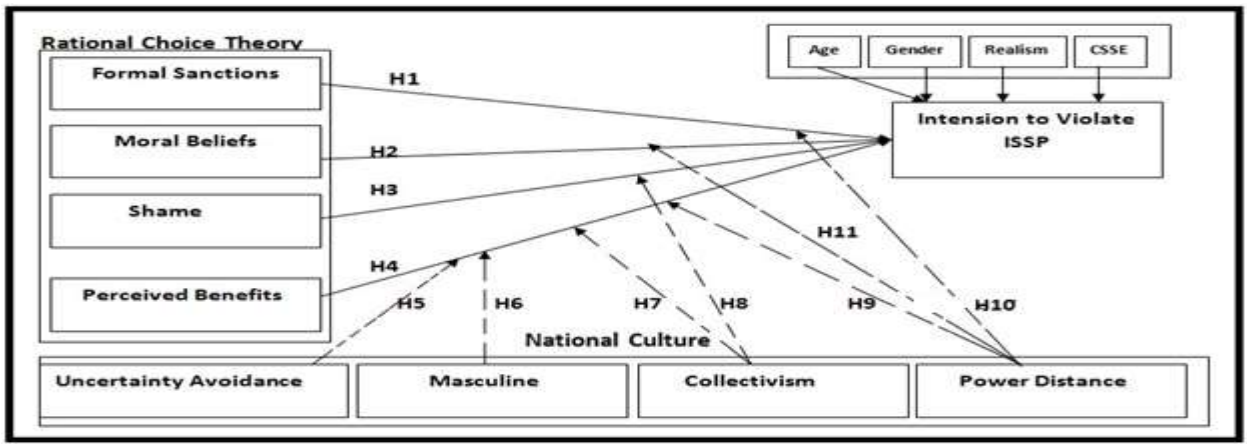

Figure 1: The Proposed Research Model

Straub (1990) reported that Formal sanctions have a high impact on reducing IS abuse. In addition to this, considerable number of researchers (e.g. Tudor, 2000; Kankanhalli, 2003; Herath & Rao, 2009a; Siponen et al., 2007) tried to investigate whether the use of sanction reduce ISS problems or not, and found that these deterrent measures improve the security level and reduce the abuse level. In another study by Harrington (1996), IS-specific codes of ethics are found to have an impact on reducing employees' intention to violate companies ISSP.

H1: There is a negative association between formal sanctions and employees' intention to violate ISSP

Criminological studies show that moral beliefs explain individuals intention to engage in a deviant behavior like corporate crime (Paternoster & Simpson, 1996), tax evasion (Wenzel, 2004), and sexual abuse (Bachman et al., 1992). Studies in Psychology (e.g. Greenberg, 2002; King & Mayhew, 2002) also reported the considerable influence of moral beliefs in policy violation decision. When we come to ISS area, researchers (e.g. Myyry et al., 2009; Li et al., 2010; Vance & Siponen, 2012) suggest that moral reasoning and individuals' values can be predictors of individuals' compliance with ISSP.

H2: There is a negative association between moral beliefs and employees' intention to violate ISSP

According to the deterrence literature (Grasmick & Bursik, 1990; Nagin & Paternoster, 1993; D'Arcy et al., 2011) shame is found to have an impact in reducing undesirable actions. Shame or social disapproval might deter people from engaging in illegal activities (Tibbetts, 1997).

H3: Shame is negatively related to employees' intention to violate ISSP

Since ISSP is considered to slow peoples work by bringing many guidelines, people preferred to violate the ISSP to save time (Puhakainen, 2006). Perceived benefits is found to have significant positive impact on employees' intention to violate ISSP (Li et al., 2010; Siponen & Vance, 2012).

H4: There is a positive association between perceived benefit and employees' intention to violate ISSP

Since people in low uncertainty avoidance society do not fear the risk of becoming jobless or making a wrong choice, they more often change jobs, with an intention of getting a better job, than the high uncertainty avoidance society (Timo, 2009). With a similar logic, since ISSP violations may bring a number of unknown consequences or threats to individuals, high uncertainty avoidance society prefers not to go to that state, even if there are some benefits of violation.

H5: The higher the degree of uncertainty avoidance, the weaker the impact of perceived benefits on employees' intention to violate ISSP

Masculinity has a slightly negative effect on ISS compliance (Timo, 2009; Doupnik & Tsakumis, 2004). A study conducted by Husted (1999) reported that masculine society is highly prone to corruption. This could mean if there exists any benefit of breaking the rule, then the masculine society may not hesitate to break the law more often than their feminine counterparts.

H6: The higher the degree of masculinity, the stronger the impact of perceived benefits on employees' intention to violate ISSP

A research conducted by Timo (2009) shows that collectivism is negatively correlated with a high level of ISS. Higher level of tax evasion exists in collectivist than individualist society (Tsakumis, 2007). Most of the time individuals from collective national cultures don't want to expose their group members' wrong doing to their supervisor to maintain harmony with their group (Leidner & Kayworth, 2006). This could mean in collective society if someone sees his/her friend breaking rule or asked him/her to violate ISSP then he/she may do it for the perceived benefit of being in harmony with friends.

H7: The higher degree of collectivism, the stronger impact of perceived benefits on employees' intention to violate ISSP

In collectivism society, transgression of norms leads to shame feeling while in an individualist society breaking norms resulted in guilty feeling (Hofstede, 1980). If we consider violation of ISSP as transgression of norms, shame will have a more deterrent impact on collective society than their individualistic counterparts.

H8: The higher the degree of collectivism, the stronger the impact of shame on employees' intention to violate ISSP

Countries with high power distance are found to be associated with a high level of tax evasion and corruption (Tsakumis, 2007; Husted, 1999). This could mean, if there exists any benefit of breaking the rule, then the high power distance society may engage in illegal activity more than their low power distance counterparts. In the ISS area, Bjork & Jiang (2006) reported that the way how ISS related risks in high power distance society handled increases the occurrence of ISS breaches. Moreover, some empirical works show employees in high power distance society break IT rules more often than low power distance society (D'Arcy et al., 2007; Dols & Silvius, 2010). This means the fear of formal sanctions in high power distance society is less strong than low power distance society.

H9: The higher the degree of power distance, the stronger the impact of perceived benefits on employees' intention to violate ISSP

H10: The higher the degree of power distance, the weaker the impact of formal sanctions on employees ISSP violation

Solms (2004) stated that one of the most critical factors to create an effective ISS culture is to encourage employees to take part in the process of setting up ISS management goals, which gradually boost the morale of individuals. In this respect, close communication between supervisors and employees is usually common in low power distance society (Moores, 2003) and it is believed that this participative management improves employees' job satisfaction (Kim, 2002), which in tern associated with a higher degree of compliance with organizational rules (Organ & Konovsky, 1998). This means employees' morale in low power distance society can be more easily cultivated and contribute to ISSP compliance than the high power distance society.

H11: The higher the degree of power distance, the weaker the impact of moral beliefs on employees' intention to violate ISSP

5 Research Methodology

The underlying approach used here lies in the positivist paradigm. The choice for the positivist paradigm is done because of the fact that the purpose of the research is to develop and validate an empirical model. The research will utilize questionnaire-based data gathering technique. In addition to the traditional survey method, we assess intention to violate ISSP and RCT constructs by using a scenario method. Scenario is well suited to study issues that measure or asks ethical/unethical behavior(Pogarsky, 2004). In this respect, scenario method offers an indirect way of measuring the intension of people to commit socially undesirable act, which may be difficult to measure by using the traditional questionnaire method, because an individual will most likely conceal his/her real intention and respond in a way that is acceptable by the society (Trevino, 1992). We use the Hofstede's model of cultural dimensions, because it has been rigorously validated in previous cross-cultural studies over time (Sondergaard, 1994). SEM based analysis will be used to evaluate the hypotheses. Since this research is a cross-cultural study, we are expected to take samples at least from two different culture. Hence, the research population includes companies in Ethiopian and the USA, which have an established information systems security policy. The reason for choosing the USA and Ethiopia is due to the fact that the two countries do have

cultural difference in the Hofstede's national culture index, and the second reason is due to the convenience of getting the required data from both countries. To select potential respondents, first we will select major cities around Ethiopia followed by a selection of organizations that do have some form of ISSP and, in the USA we will use the service from Amazon Mechanical Turk (MTurk). Amazon's MTurk is a relatively new website that contains the major elements required to conduct research. The data obtained are at least as reliable as those obtained via traditional methods and generally MTurk can be used to obtain high-quality data inexpensively and rapidly (Buhrmester et al., 2011). For the final survey, planned to dispatch large number of questionnaires in each country, and from these if we subtract a reasonable number of non-response rate and incomplete responses, we can get enough responses for analysis. Anderson & Gerbing (1984) suggest that a sample size of 150 or more will be needed to obtain parameter estimates that have standard errors small enough to be of practical use. On the other hand, Kline (2005), and Weston & Gore (2006) recommended to have a minimum sample size of 200 for any SEM based analysis and thus we strive to get a minimum of 200 usable responses. We use previously validated instruments for the different constructs (see Appendix A). Researchers should use previously validated instruments wherever possible, without revalidating instrument content, constructs, and reliability (Boudreau et al., 2001). SPSS Amos software will be used to run confirmatory factor analysis for the measurement and structural model.

6 Result from Pilot Study

Since this is a research in progress, at this point in time, we only conduct a pilot study and the full scale study will follow soon. To conduct this pilot study, we collect 230 usable response from employees working in Virginia Tech University (USA) and Addis Ababa University (Ethiopia). After the psychometric properties of the instrument are established through a rigorous procedure involving confirmatory factor analysis, we proceed with the hypotheses testing. As can be seen from Figure 2, the variables age, the reported realism of the scenario, and computer security self-efficacy(CSSE) are used as control variables and their effect on intention to violate ISSP is small and insignificant.

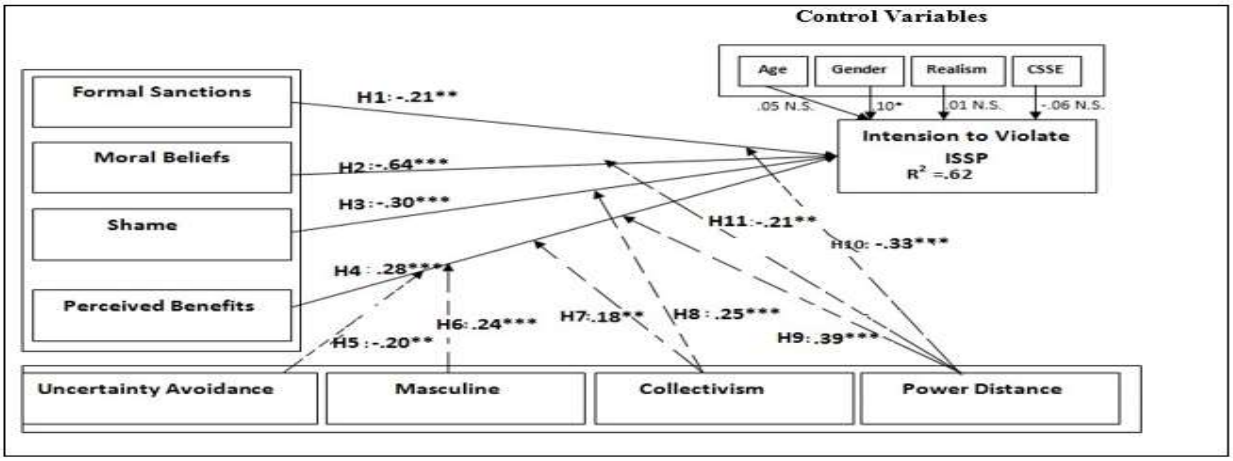

*Figure 2: Results of the pilot study. Notes: N.S.= non-significant; *** p-value < 0.01; ** p-value < 0.05; * pvalue < 0.10*

As can be seen from the result of the pilot test, all the hypotheses except H7, H10, and H11 are supported. In the case of H7, the moderating effect of collectivism between perceived benefit and intention to violate ISSP is significant but at .18, which is lower than the minimum threshold of .20(Chin, 1998). While H10 and H11 are found to be significant but in the opposite direction to what has been hypothesized and we do believe that it need further investigation and explanation which will be actually done in the final completed paper.

The result from the pilot study clearly indicates the considerable influence of RCT constructs on employees' intention to violate ISSP. In addition to this, the result also indicates how strongly cultural dimensions moderate the impact of ISS countermeasures(formal sanctions), moral beliefs, shame, and perceived benefits on employees' intention to violate their company's ISSP. Thus, we believe that ISS managers need to keep in mind how the

cultural dimensions of the society could positively or negatively shape employees' ISS behavior and try to take into account this factor when they design and implement ISS policies or strategies.

As a final note we are currently finalizing the collection of data for the full scale analysis from both USA and Ethiopia and that will be included in the completed research paper.

7 Contribution

Despite years of investments in technology and processes, truly protecting data remain a distant goal for information security officers (Al-Awadi & Renauld, 2007). Nowadays, it becomes clear that technology alone cannot lead to sufficient solutions and the human aspects cannot be isolated from technology (Slay, 2003). In this respect, increasing numbers of researchers argue that, in order to better prepare to tackle the ISS problem, the human element need to be well studied and addressed (Bjork & Jiang, 2006; D'Arcy et al., 2007; Timo, 2009). Thus, in this study, we will contribute in investigating national culture as one of the most important human related factors that is believed to have an impact on employees' ISS compliance behavior. Some researchers indicate the importance of considering national culture in IT related issues. For example, a review of the existing literature by Dol & Silvius (2010) has clearly identified culture as one of the five factors that are considered to have an influence on employees' ISS policy compliance behavior. If we look at the ISS literatures, specifically in Africa, there is hardly any attempt to this end (Salahuddin, 2011), and this creates an opportunity for researchers to conduct researches on the influence of culture on individual's ISS compliance behavior. In this regards, this research will bring the knowledge of how national culture influence employees' intention towards ISSP violation and it gives insight on how to improve employees' ISS compliance. On the other hand, this research is the first study to see the ISS problem from the perspective of RCT and national culture perspective, and this will contribute to the cumulative theory building effort in the field of ISS. In addition to this, the output from this research can serve as an input for the development of ISSP and different types of ISS awareness and training programs by providing further understanding of the factors that affect the successful implementation of ISSP. Moreover, this research output could also be an important input for companies that do have an outsourcing ambition of IT related services in Ethiopia. Knowing the impact of cultural dimensions on ISSP violation, service providers from abroad can identify and manage potential problems and risks (Timo, 2009).

8 Limitations

The output from this research may not be applicable for countries that do have a different cultural dimensions. Thus, caution should be taken in generalizing the findings to countries outside Ethiopia and the USA. On the other hand, even though there are five national cultural dimensions (Hofstede, 1980), our cultural hypothesis will address only four of them, namely: power distance, uncertainty avoidance, individualism/collectivism, and masculine/feminine. This decision is based on the fact that Ethiopia does not have a score for the long term orientation dimension in Hofstede's study. Since it is not possible to include organizations that do not have ISSP, the research population for the study is limited to employees who work only in companies that have a well-established ISSP. Even though culture can be studied at different label (national, organizational, and subunit level), this research is limited to national culture. National culture is more powerful than organizational culture in influencing employees' behavior (Robbins, 2005). In addition to this, due to the difficulty of measuring actual behavior, we use intention as a dependent variable. The use of intention as the dependent variable may raise the question of "whether intention indicates the actual behavior of employees?" By many researchers it is considered to be appropriate to use intention as the valuable approximation for behavior (Pogarsky, 2004). The theory of planned behavior suggests that, people frequently behave as they predict (Ajzen, 1991).

Appendix A: The Initial Measurement Items and Their Sources

Constructs	**Source**
National Culture (Power distance, Collectivism/Individualism, Uncertainty Avoidance, Masculine/Feminine	Derived from Yoo, Donthu and Lenartowicz (2012); Srite, M. (1999)
RCT (Formal sanction, Shame, Perceived Benefits, Moral Beliefs)	Derived from Vance and Siponen(2012)
CSSE (Computer Security Self Efficacy)	Herath and Rao(2009a)

References

Anderson J.C.,& Gerbing, D.W. 1984. The effect of sampling error on convergence, improper solutions , and goodness-of-fit indices for maximum likelihood confirmatory factor analysis. Psychometrika, 49, 155-173.

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

Bachman, R., Paternoster, R., & Ward, S. 1992. Testing a deterrence/rational choice conception of sexual assault. Law and Society

Arage, T. M., Belanger, F., & Tesema, T. B. (2016). Investigating the Moderating Impact of

National Culture in Information Systems Security Policy Violation: The Case of Italy and Ethiopia.

Bjork & Jiang. 2006. Information Security and National Culture: Comparison between ERP system security implementations in Singapore and Sweden. Unpublished master thesis.

Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk a new source of inexpensive, yet high-quality, data?. Perspectives on psychological science, 6(1), 3-5.

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), 523-548.

Chaula, J. 2006. A socio-technical analysis of information systems security assurance. Stockholm University, Stockholm Sweden.

Cyber Security Watch Survey, 2010 & 2012 . CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte. Available at URL: http://www.cert.org/insider_threat/

D'Arcy, Hovav, A., Galletta, D., 2009. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse

D'Arcy, J. and Herath, T., 2011. A review and analysis of deterrence theory in the IS security literature:

making sense of the disparate findings.European Journal of Information Systems, 20(6), pp.643-658.

Dols, T. and Silvius, A.J., 2010. Exploring the Influence of National Cultures on Non-Compliance Behavior. Communications of the IIMA, 10(3), p.11.

Doupnik, T. S., & Tsakumis, G. T. 2004. A critical review of tests of Gray's theory of cultural relevance and suggestions for future research. Journal of Accounting Literature, 23, 1.

Grasmick, H. G., & Bursik Jr, R. J. 1990. Conscience, significant others, and rational choice: Law and society review, 837-861.

Greenberg, J., 2002. Advances in organizational justice. Stanford University Press.

Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding

information security non-compliance in hospitals: The importance of user rationale. Information

Management & Computer Security, 21(4), 266-287.

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

Herath, T. and Rao, H.R. 2009b. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems 47 (2009) 154–165.available at URL: www.elsevi e r.com/locate/dss.

Hoffer, J.A. and Straub Jr, D.W., 1989. The 9 to 5 underground: are you policing computer crimes? Review, 30(4), p.35.

Hofstede, G., 1980. Culture's consequences. Beverly Hills.

Husted, B. W. (1999). Wealth, culture, and corruption. Journal of International Business Studies, 30, 339– 359.

Husted, B.W., 2000. The impact of national culture on software piracy.Journal of Business Ethics, 26(3), pp.197-211.

Kankanhalli, A., H.H. Teo, B. C. Y. Tan, K.-K.Wei. 2003. An integrative study of information systems security effectiveness. Internat. J. Inform. Management 23(2) 139–154.

Kim, S. 2002. Participative management and job satisfaction: Lessons for management leadership. Public administration review, 62(2).

Kline, R. B. (2005). Principles and practice of structural equation modelling: methodology in social sciences, 2nd edn, Guilford Press, New York.

Li, H., Zhang, J., & Sarathy, R.2010. Understanding compliance with internet use policy from the perspective of rational choice theory. Decision Support Systems, 48(4), 635-645.

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. Information Systems Journal, 25(5), 433-463.

McCumber, J., 2011. "The Failure of Rational Choice Philosophy," *The New York Times Opinion Pages Opinionator*

Magklaras, G. B., S. M. Furnell. 2002. Insider threat prediction tool: Evaluating the probability of IT misuse. Security 21(1)62–73

Magklaras, G.B. and Furnell, S.M. 2006. Towards an insider threat prediction specification language (Information Management &Computer Security Vol. 14 No. 4, 2006 pp. 361-381. Emerald Group Publishing Limited 0968-5227

Moores, T.T., 2003. The effect of national culture and economic wealth on global software piracy rates. Communications of the ACM, 46(9), pp.207-215.

Organ, D. W., & Konovsky, M. A. 1989. Cognitive versus affective determinants of organizational citizenship behavior. Journal of Applied Psychology, 74: 157-164.

Pahnila, S., Siponen, M., & Mahmood, A. 2007. Employees' behavior towards IS security policy compliance. In System Sciences, 2007. HICSE 2007. 40th Annual Hawaii International Conference on (pp. 156b-156b). IEEE.

Pogarsky, G. 2004. "Projected Offending and Implications for Heterotypic Continuity," Criminology (42:1), pp. 111-135.

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.

Richardson, R., 2008. CSI computer crime and security survey. Computer Security Institute, 1, pp.1-30.

Salahuddin, M. Alfawaz, 2011. Information security management: A case study of an information security culture. Queensland University of Technology. Unpublished PhD dissertation. Faculty of science and technology

Schiffman, L.G. and L.L. Kanuk (1997), Consumer Behaviour, Englewood Cliffs, New Jersey: PrenticeHall International, Inc.

Shore, B., Venkatachalam, A.R., Solorzano, E., Burn, J.M., Hassan, S.Z. and Janczewski, L.J., 2001. Softlifting and piracy: Behavior across cultures.Technology in Society, 23(4), pp.563-581.

Siponen, M., 2006. ISS standards focus on the existence of process, not its content. Communications of the ACM, 49(8), pp.97-100.

Siponen, M. and Pahnila, S. and Mahmood, A. 2007. Employees' Adherence to Information Security Policies: An Empirical Study.

Siponen, M. and Vance 2010. A Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly 34, 2 (2010).

Sommestad, T., Ekstedt, M., & Holm, H. (2013). The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures. Systems Journal, IEEE, 7(3), 363-373. Sondergaard, M.(1994). "Hofstede's consequences: A study of reviews, citation and replications," organization studies, 15(3), 447-456.

Straub Jr, D. W. (1990). Effective IS security: An empirical study. Information Systems Research, 1(3), 255-276.

Tan, B. C. Y., Smith, H. J., and Keil, M. 2003. "Reporting Bad News about Software Projects: Impact of Organizational Climate and Information Asymmetry in an Individualistic and Collectivist Culture," IEEE Transactions on Engineering Management . pp. 65-77.

Tibbetts, S. G. 1997. Shame and rational choice in offending decisions.Criminal Justice and Behavior, 24(2), 234-255.

Tsakumis, G. T., Curatola, A. P., & Porcano, T. M. 2007. The relation between national cultural dimensions and tax evasion. Journal of International Accounting, Auditing and Taxation, 16(2), 131-147.

Vance, A., & Siponen, M. T. 2012. IS security policy violations: a rational choice perspective. Journal of Organizational and End User Computing (JOEUC), 24(1), 21-41.

Wenzel, M. 2004. An analysis of norm processes in tax compliance. Journal of economic psychology, 25(2), 213-228.

Weston, R. & Gore, PA (2006). A brief guide to structural equation modelling. The

counseling psychologist. 34(5), 719- 720.