International Journal of Business Analytics & Intelligence
10 (1) 2022, 29-47
http://publishingindia.com/ijbai/

Investigating the Influence of Ethiopian National Culture on Information Security Policy (ISP) Violation: The Case of the Ethiopian Financial Institutions

Dakito Alemu Kesto*, Tilahun Muluneh**

Abstract

Nowadays, it is clear that information security is one of the most basic issues that organisations need to focus on. Despite huge investments made by companies to keep their information systems safe, there are many information security breaches that infiltrate companies' systems; consequently, these cost them their reputation, affect customers' confidence, and bring huge financial losses. Ethiopian companies are not immune to this security problem, and there are many signs of information security breaches. The literature suggests that almost all investments in information security related issues are for technological solutions. However, this type of solutions alone do not work well, and according to some researchers, there is one significant element that has been given very little attention, the human factor. Most of the information security breaches are caused by employees who are legitimate users of the company's systems. So 'how can we counter the illegal action of our own employees?' is the main objective this study tried to address. The findings showed strong evidence on the influence of contextual factors and national culture, on employees' information security behaviour, and consequently, it highlighted the importance of taking some level of precaution when organisations introduce new policies or standards that are copied from abroad. Policy makers and ISS managers in Ethiopia, particularly at the Information Network Security Agency (INSA), can learn how important it is to modify or adapt their ISP, which was copied from ISO 27002, based on the findings of this study.

Keywords: Contextual Factors, National Culture, Employees' Information Security Behaviour, Financial Institutions, Information Systems Security

Introduction

Many organisations around the world are faced with an increasing number of information security attacks on their systems. While the ISS world often focuses on analysing and counteracting threats of external origin (Magklaras et al., 2006), most of these threats originate from insiders (D'Arcy et al., 2009). The frequency of occurrence is not the only indicator of the impact of insiders' incidents; there are also considerable financial costs attributed to legitimate user actions (Magklaras et al., 2006). Many researchers (Magklaras et al., 2002; Theoharidou, 2005; Warkentin et al., 2009) report that the insider threat remains the greatest single risk to organisations, and most security experts agree that more successful attacks usually come from inside the organisation rather than from outside, and that insider attacks are potentially more costly (Schultz, 2002; Shaw et al., 1998). The internal incidents are here to stay and their mitigation should be a priority for IT professionals (Magklaras et al., 2006).

When we explore the information security breach problems in Ethiopia, due to lack of studies in the areas of information system security (ISS), it is difficult to know the exact figure with respect to the financial losses of the

* Head, Accounting & Finance Program Unit, School of Commerce, CoBE, Addis Ababa University, Ethiopia. Email: dakito.alemu@aau.edu.et
** Addis Ababa University, Ethiopia. Email: dalemu22@gmail.com

incidents. Interestingly, we tried to have an interview with IT security officers of different banks located in Addis Ababa, but they were not willing to state financial losses they incurred by ISS breaches. Even though there is lack of documented and published information with respect to security breaches in Ethiopia, there are some indications which show us the critical level to which ISS breaches reach the country. For example, according to a special programme that was broadcasted by the Ethiopian Radio and Television Agency (2012), the Ethiopian Revenue and Custom Authority junior database administrator used the password provided to him by his boss (because she went abroad), to deliberately delete the data related to a tax which the company is expected to collect from its customers. In return, he received 800,000 Birr, and this single incident cost the company 13,000,000 Birr.

In another instance of information security policy (ISP) violation, the Ethiopian Airlines terminated 11 employees working in different departments, citing violation of rules and procedures they were expected to abide by and abuse of the systems that they had privileged access to (Ethio_News_24, 2013). The alleged abuse of the systems is connected to its frequent-flyer programme called ShebaMiles, whereby Ethiopian Airlines customers can accumulate miles that would result in awards of free tickets, gifts, and privileges. The sources indicated that the alleged wrongdoing was uncovered following a complaint by a customer enrolled in the ShebaMiles programme, regarding irregularities in the frequent-flyer's account. Obviously, this incident may have damaged the good image of the airlines, which in turn may bring some kind of financial loss to the company.

The main research problem that initiated this research work was the lack of studies in every corner of the world in general, and Africa in particular, that investigates how national culture moderates the influence of formal sanctions (in this research we use security counter measures interchangeably with formal sanctions), perceived benefits, moral beliefs, and shame on employees' intention to violate ISSP. Despite critical ISS problems in Africa, and particularly in Ethiopia (Gardachew, 2010; Bultum & Ayana, 2012; Taddesse & Kidan, 2005), there is hardly any research that tries to consider non-technical solutions to the problem. Specifically, one of the non-technical elements gaining increasing attention is the human element. According to researchers, one of the most common factors to shape human behaviour is culture, and to this end, there is hardly any attempt to explore the influence of national culture on ISSP compliance.

To clearly show the ever-increasing number of ISS breaches, it is important to see some figures in the global perspective. The ISS threat that is caused by insiders or employees' non-compliance is not limited to Africa; literature shows the existence of many information security breaches problems all over the world. According to Garg (2003), companies all over the world are losing more than $2 trillion due to security breaches. This problem will be more frustrating when we realise that most of the breaches are caused by insiders. Between one-half and three-quarters of all information security incidents originate from within the organisation (Ernst & Young, 2003; Information Week, 2005). Since only a fraction of information security incidents are actually discovered (Hoffer & Straub, 1989; Whitman, 2003), the figures from different reports and studies may be lower than the actual fact. As insiders 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 destroying the good image of the company, customers' confidence, and many more (D'Arcy et al., 2009). In this research, an insider is defined as a person that is legitimately given the capability of accessing one or more components of IT infrastructure (Magklaras et al., 2006, pp. 3). The CyberSecurity Watch Survey (2010) annual report indicates more than $2 billion in losses to organisations due to ISS breaches between 1997 and 2007. According to the survey, companies may continue to suffer more losses in the future, if the overall types of attacks are doubled in the specified time period. More recently, CyberSecurity Watch Survey (2012) annual report indicates that insider attacks increased from 41% in 2004 to 53% in 2011. In addition to this, according to a report by Verizon (2012), the security breaches caused by insiders increased on average from 33% (2004-2007) to 48% (2009). To make matters worse, insider abuse of company systems is the second-most frequent (44%) security problem, next to virus incident (49%), and well above outsiders (29%) (Richardson, 2008). Therefore, the objective of this study is to identify the moderating impact of national culture on the influence of information formal sanctions (security countermeasures), perceived benefits, moral beliefs, and shame on employees' intention to violate ISSP. This valuable output allows information security personnel and managers to make better decisions

on 'how to develop and implement ISSP that best fit one's (Ethiopian) culture?'.

Research Questions

The major purpose of this study was to examine whether cultural differences moderate the influence of formal sanctions (security countermeasures), perceived benefits, moral beliefs, and shame on employees' intention to violate ISSP. In addition to this, we investigated the influence of formal sanctions (security countermeasures), perceived benefits, moral beliefs, and shame on employees' ISSP violation. Thus, the following research questions guided this research:

RQ1: What is the influence of security countermeasures (formal sanctions), perceived benefits, moral beliefs, and shame on employees' intention to violate their organisational ISSP?

RQ2: What is the moderating impact of national culture on the influence of security countermeasures (formal sanctions), perceived benefits, moral beliefs, and shame on employees' intention to violate their organisational ISSP?

Hypotheses

To answer the research questions mentioned above, we formulated several hypotheses. Even though there are five national cultural dimensions according to the Hofstede (1980) model of national culture, our cultural hypotheses addressed only four of them, namely power distance, uncertainty avoidance, individualism/collectivism, and masculinity/femininity. This decision was based on the fact that Ethiopia does not have a score for the long-term orientation dimension in Hofstede's study. In addition to the cultural dimensions, we include four RCT (rational choice theory) constructs, namely formal sanctions, perceived benefits, moral beliefs, and shame. As can be seen from the research model (Fig. 1) there are 11 hypotheses.

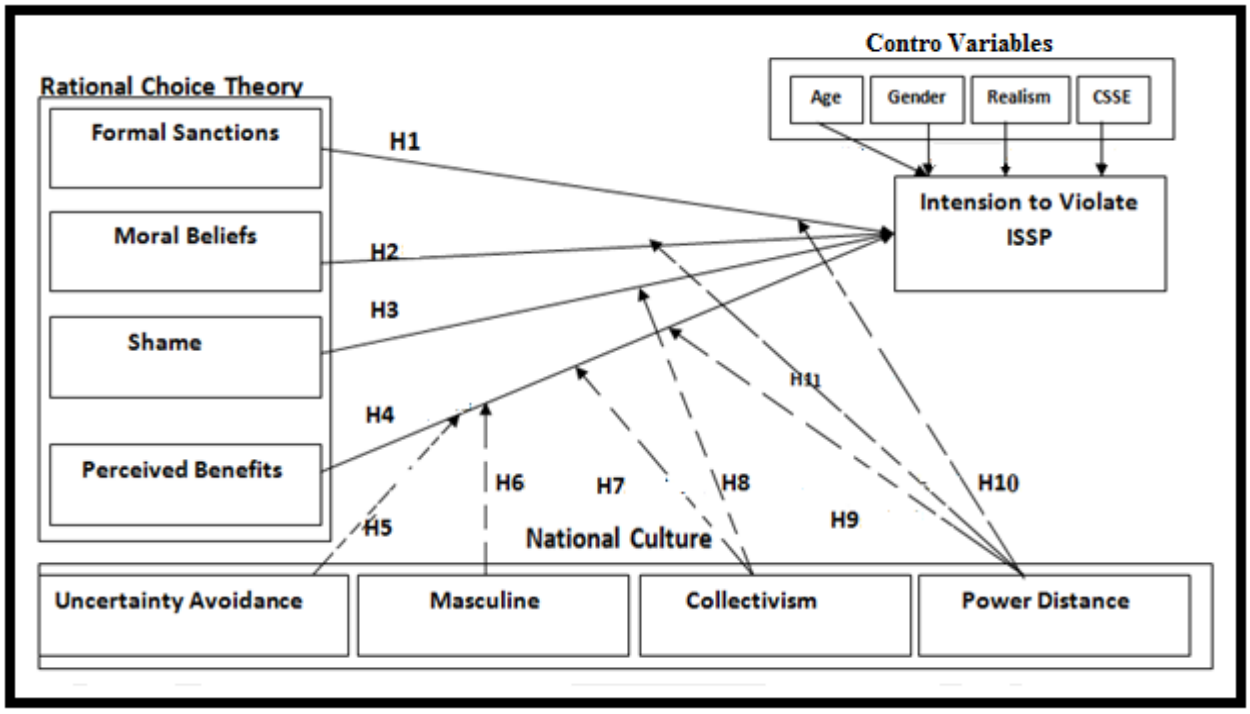


Fig. 1: The Research Model

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

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

H3: There is a negative association between shame and employees' intention to violate ISSP.

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

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

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

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

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

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' intention to violate ISSP.

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

Methods and Materials

Since researchers are expected to clearly formulate their research methodology in advance, we illustrate the research's underlying philosophies, epistemology, ontology, and method (see Fig. 2). Ontology focuses on the question of what is taken as real and how to know whether something is real (Orlikowski & Baroudi, 1991; Guba & Lincoln, 2005; Merterns, 2007). The underlying ontology used here lies in the positivist paradigm. The choice for the positivist paradigm was done because the purpose of the current research was to develop and validate an empirical model consisting of testable hypotheses to evaluate the effect of national culture and other important variables on employees' intention to violate ISSP. Orlikowski and Baroudi (1991) classified IS research as positivist when there is evidence of formal propositions, quantifiable measures of variables, hypothesis testing, and the drawing of inferences about a phenomenon from the sample to a stated population.

The epistemological assumptions are concerned with the nature of knowledge and how it can be obtained. Crotty (1998) distinguishes between three epistemological positions: objectivism, constructivism, and subjectivism. Our research epistemological view is objectivism. In the objectivism view, knowledge exists out there whether we are conscious of it or not. Researchers with the objectivism position always try to look for causes and effects and explanations. They rely upon experimental, quasi-experimental, and survey methods. When we come to the research approach, we used a quantitative method. The rationale for adopting a quantitative approach was because it has the ability to produce objective, quantifiable, and reliable data that are usually generalisable to some larger population. Whenever the purpose of a study is hypothesis testing using statistical methods and generalisation to a larger population from the sample based on numerical data, quantitative survey research is the preferred option (Creswell, 2009).

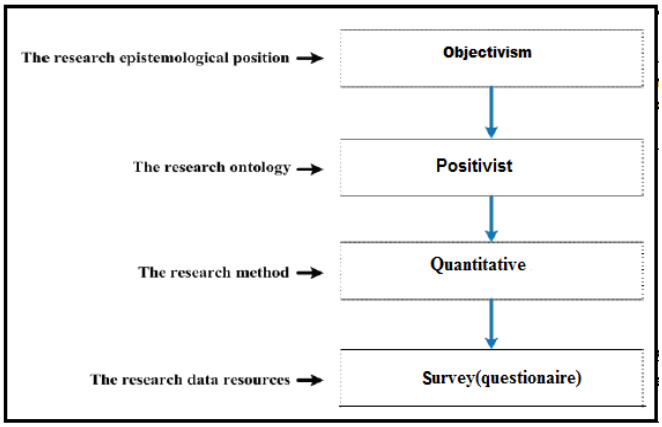


Fig. 2: The Research's Underlying Philosophies, Epistemology, Ontology, and Method

The research utilised questionnaire-based data-gathering techniques to collect the data needed to investigate and test the research hypotheses. Surveys are widely accepted and used in the IS field for empirical research; specifically, quantitative researchers frequently use data from surveys (Linda & Thomas, 2008). The sample survey methodology also leads to greater generalisability of the results, when compared to other research methods (McGrath, 1981). We used Hofstede's model of cultural dimensions because it has been rigorously validated in previous cross-cultural studies over time and in many of countries (Sondergaard, 1994). We used SEM-based statistical analysis to evaluate the relationship among the national cultural dimensions, RCT constructs, and employees' intention to violate ISSP. When we come to the population and sampling procedure, according to Singleton and Straits (2005), sampling has to be executed in two separate steps: the first step is to

select the population we were interested in so that we are in a better position to select some representatives. Most of the time, experienced researchers try to come up with a concise picture of their population before proceeding with the selection of sample, thus starting from the top at the population and working down to the sample (Bailey, 1982). In our research, the population includes organisations located in different parts of Ethiopia (i.e., Addis Ababa, Mekele, Bahir Dar, Adama, Diredaw & Hawassa), which have an established ISSP. In each company, individuals were selected randomly. We believe that there is a possibility of the threat of common method bias (CMB), which can occur, among other causes, when the dependent and independent variables are collected at the same time in the same survey instrument (Podsakoff et al., 2003).

Researchers have checked whether the sample size was likely to be sufficient prior to actually conducting the study. This is because small sample sizes can result in non-convergence and improper solutions (Anderson & Gerbing, 1984; Fornell & Larcker, 1981). Anderson and 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. Researchers used previously validated instruments wherever possible, being careful not to make significant alterations in the validated instrument without revalidating instrument content, constructs, and reliability (Boudreau et al., 2001). Thus, in our research, we used previously validated instruments. Statistical Package for the Social Sciences with Amos (SPSS Amos) software was used to run different types of statistical analysis.

The Full CFA Measurement Model

Now we proceed to the final stage of constructing the measurement model: bringing together all the individual theoretical constructs so that we can assess the validity of the full CFA measurement model. In this regard, the convergent validity of the full measurement model was evaluated based on the goodness-of-fit statistics, while the discriminant validity of the theoretical construct was assessed by comparing the AVE value of every construct with the squared inter-construct correlation of that factor (Hair et al., 2010). According to Hair et al. (2010), discriminant validity is exhibited if the AVE value is consistently higher than the squared inter-factor correlation. By using these techniques, we assessed the discriminant validity of every construct shown in the full measurement model. The full measurement model consists of eight constructs and 33 items. In addition to this, we present all the necessary goodness-of-fit statistics of the full measurement model, while Table 1 shows the result of the discriminant validity. All the CR values were within the acceptable range and all AVE values consistently higher than the squared inter-factor correlation. Hence, discriminant validity was supported.

Table 1: Construct Correlation Matrix for the Main Survey

	CR	AVE	Power Distance	Perceived Benefit	Masculinity	Formal Sanction	Shame	Moral Beliefs	Collectivism	Uncertainty Avoidance
Power Distance	0.891	0.672	0.820							
Perceived Benefit	0.928	0.765	0.360	0.875						
Masculinity	0.809	0.523	0.413	0.247	0.723					
Formal Sanction	0.878	0.547	-0.474	-0.275	-0.343	0.740				
Shame	0.931	0.772	-0.370	-0.563	-0.350	0.320	0.878			
Moral Beliefs	0.923	0.800	-0.425	-0.399	-0.397	0.217	0.340	0.895		
Collectivism	0.872	0.633	0.313	0.270	0.063	0.024	-0.300	-0.268	0.796	
Uncertainty Avoidance	0.860	0.608	-0.384	-0.203	0.036	0.312	0.326	0.419	0.084	0.779

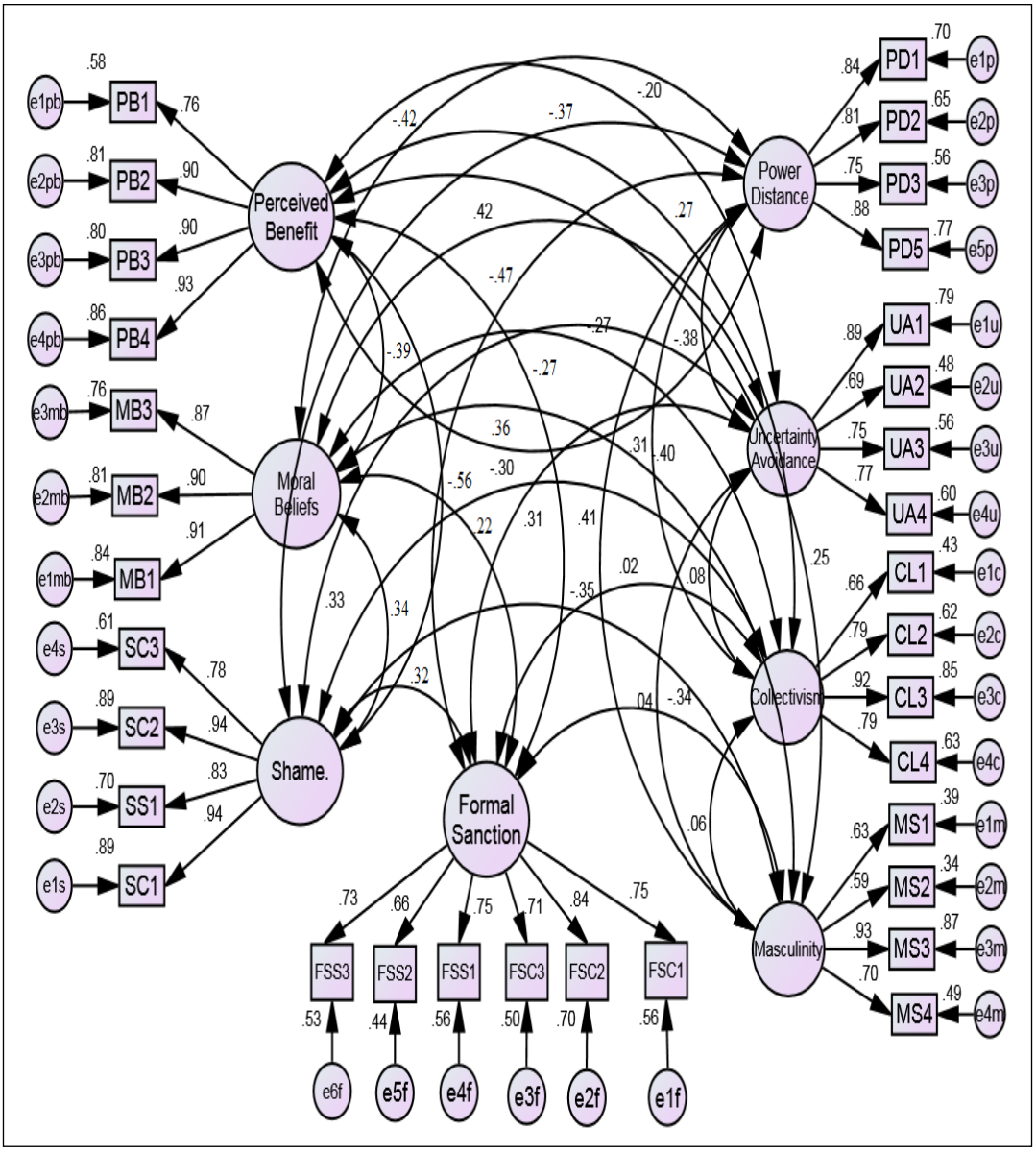


Fig. 3: The Proposed Full Measurement Model for the Main Survey

Table 2: The Goodness-of-Fit Statistics of the Full Measurement Model for the Main Survey

Absolute Fit Index		*Incremental Fit Index*		*Parsimony Fit Index*	
X2(P-value)	874.14 (.14)	CFI	.93	PCFI	.81
DF	467	IFI	.93	PNFI	.74
X2/DF	1.87	TLI	.92		
RMSEA	.065				
RMR	.025				
SRMR	.05				
GFI	.91				
AGFI	.80				

Final Reliability

In this section, we conduct an internal consistency check for each construct by using the data collected from the main survey. Before constructing the final structural model, researchers are expected to make sure that they already conducted the instrument reliability test (Straub et al., 2004). Reliability measures how consistently instrument items measure a construct of interest. In this regard, we use a type of reliability test called internal consistency. Accordingly, the Cronbach's α is used to test the construct reliability of every construct and Table 3 shows the result. According to Hair et al. (2010), a Cronbach's α of .7 or more is the most commonly accepted threshold. As can be seen from Table 3, all the values are greater than the minimum value, and hence, the internal consistency of instruments or construct reliability is satisfied.

Table 3: Instrument Reliability

Constructs	*No. of Items*	*Cronbach's α Value*
Power Distance	4	.90
Uncertainty Avoidance	4	.83
Collectivism	4	.87
Masculinity	4	.84
Perceived Benefits	4	.87
Moral Beliefs	3	.91
Shame	4	.91
Formal Sanction	6	.89

Results and Discussion

Once the validity and reliability of the measurement model are checked, the next step is to test the structural model. Hence, in this section, we focus on assessing the structural model, which is testing the relationship between the theoretical constructs shown in the research model. We use the structural equation modelling (SEM) methodology for representing, estimating, and testing the network of relationships between the theoretical constructs. In addition, we present and discuss the main findings of the research against the research questions shown in the second chapter. The main research question (from the second chapter) this study raised is "to what extent, if any, does cultural difference moderate the influence of security countermeasures (formal sanction), perceived benefit, moral beliefs, and shame on employees' intention to violate ISSP?" Thus, in the upcoming sections we discuss the following topics in detail: in section 1.9.4 we present the final result of the structural model validity, hypothesis testing and we discuss the findings of the research.

Assessment of the Structural Model Validity and Hypothesis Testing

Unlike the traditional statistical methods, which are mainly dependent on a single statistical test, SEM relies on many statistical tests to investigate how well a proposed theoretical model fits the reality or the collected data (Suhr, 2006). Thus, to evaluate the validity of the structural model, we use different types of statistical tests available in SEM. As clearly shown in the process of constructing the full measurement model, we depict how well each of the theoretical constructs relate or correlate with each other. However, the correlation shown in the full measurement model is a simple correlation and it does not provide other important statistical information about the nature of the relationship between the theoretical constructs. In this regard, a measurement model could only be taken as a first step towards constructing the structural model (Hair et al., 2006). Since we have already finalised the construction and testing of the measurement model, our next job is to construct and test the structural model. According to Byrne (2001), the structural model depicts which construct directly or indirectly influences the value of the other constructs in the research model.

To test the structural model validity, reliability, and acceptability, researchers usually go through the following activities (Kassahun, 2012): (1) analysing the goodness-of-fit statistics (see previous chapter Table 2); (2) evaluating the R-squared coefficient of determination and according to Chin (1998), a value of .5 or above is considered very good; (3) evaluating the magnitude level, significance (based on the P-value), and direction of the estimated structural values – Hair et al. (2006) state that the significance level of a parameter estimate should be less than .05. Fig. 4 shows the theoretical structural model of the research.

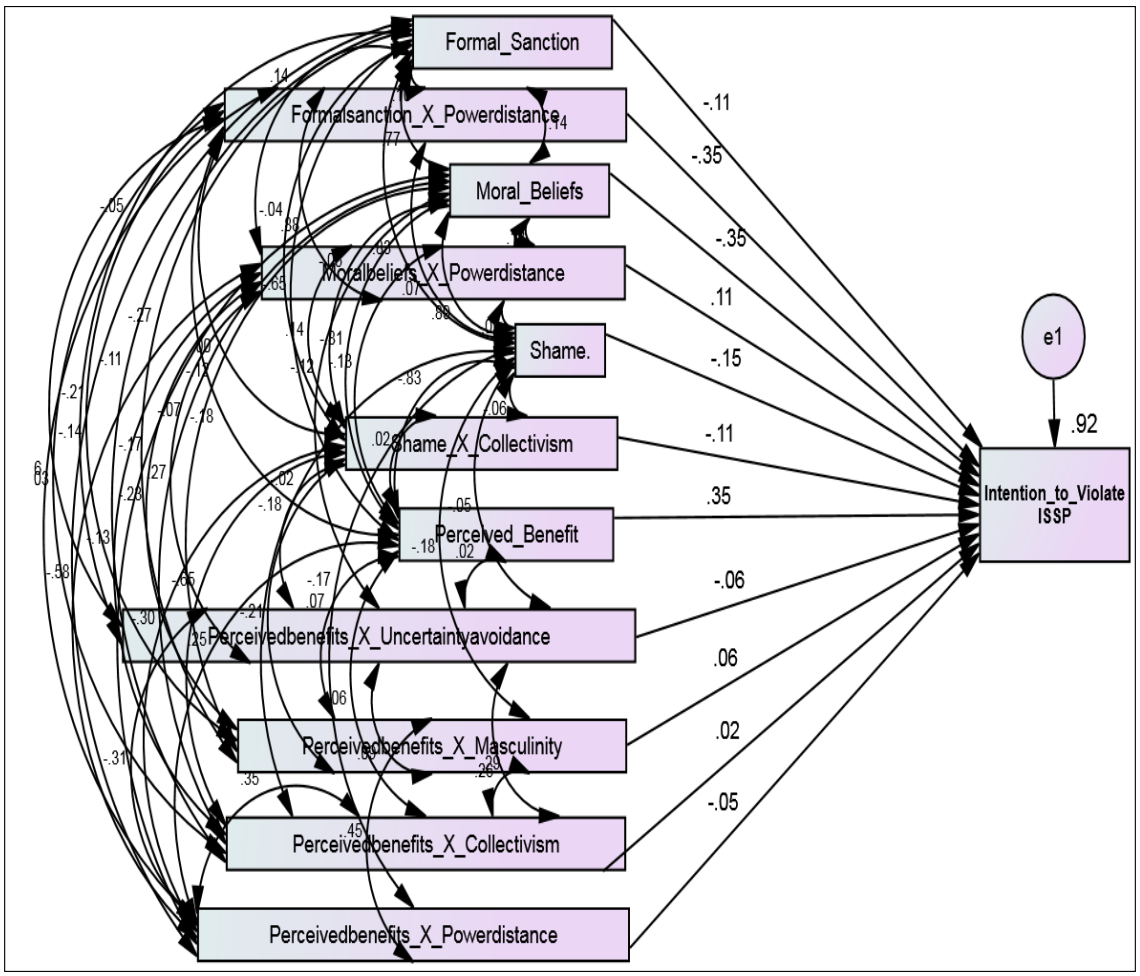


Fig. 4: The Full Structural Model

We evaluate the structural model against those three criteria. Table 4 shows the goodness-of-fit for the whole structural model.

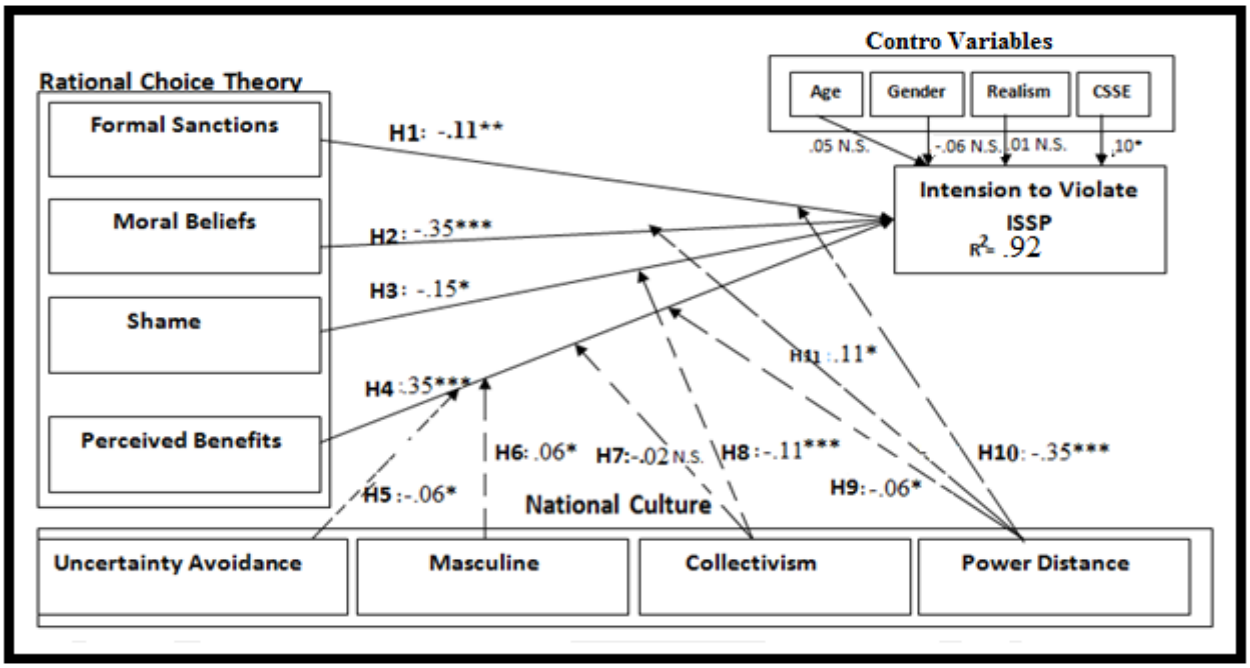
Table 4: The Goodness-of-Fit Statistics for the Structural Model

Absolute Fit Index		*Incremental Fit Index*		*Parsimony Fit Index*	
X2(P-value)	292.2	CFI	.93	PCFI	.67
DF	(.23)	IFI	.94	PNFI	.66
X2/DF	75	TLI	.92		
RMSEA	3.9				
RMR	.08				
SRMR	.04				
GFI	.06				
AGFI	.91				
	.82				

As can be seen from the goodness-of-fit statistics in Table 4, all the values satisfy the criteria for a good model. The chi-square value of 292.2 (at P > .05), with 72 degrees of freedom indicates a good fit. With respect to the absolute fit index, all the statistics meet the minimum requirements (GFI > .90, AGFI > .80, RMR & SRMR < .09, and RMSEA < .08/.1), and the incremental fit index statistics (IFI, TLI, and CFI) have values greater than or equal to .92, while the parsimonious fit indices (PCFI and PNFI) score above .05. Thus, all the selected statistics indicate the existence of best fit between the structural model and the collected data.

Following the goodness-of-fit test, we proceed with the next statistical test, which is the assessment of the coefficient of multiple determination (R-squared). Thus, we assessed the proportion of variance in the dependent variable, which is employees' intention to violate ISSP, accounted for by the model. Fig. 4 shows that 92% of

the variance in employees' intention to violate ISSP is explained by the model, and according to Chin (1998), R-squared value of .5 or above is considered to be very good. The last statistical test conducted to further strengthen the validity of the structural model is to evaluate the standardised factor loadings, the direction of the relationships, and the level of significance. To this end, Fig. 5 and Table 5 show these statistics.



Notes: N.S. = non-significant; ***p-value < 0.001; **p-value < 0.01; *p-value < 0.05.

Fig. 5: The Final Path Diagram for the Research Model

Table 5: The Result from the Final Structural Diagram

Path	*Hypothesis*	*Standardised Estimate*	*S.E.*	*C.R.*	*P*
Intention_to_Violate_ISSP ← Formal_Sanction	H1	−0.107	0.065	−2.808	0.005
Intention_to_Violate_ISSP ← Moral Beliefs	H2	−0.352	0.054	−7.513	***
Intention_to_Violate_ISSP ← Shame	H3	−0.149	0.054	−2.529	0.011
Intention_to_Violate_ISSP ← Perceived Benefit	H4	0.349	0.063	8.789	***
Intention_to_Violate_ISSP ← Perceivedbenefits_X_UncertaintyAvoidance	H5	−0.061	0.023	−2.501	0.012
Intention_to_Violate_ISSP ← Perceivedbenefits_X_Masculinity	H6	0.063	0.021	2.573	0.01
Intention_to_Violate_ISSP ← Perceivedbenefits_X_Collectivism	H7	−0.016	0.026	0.553	0.58
Intention_to_Violate_ISSP ← Shame_X_Collectivism	H8	−0.112	0.027	−4.176	***
Intention_to_Violate_ISSP ← Perceivedbenefits_X_Powerdistance	H9	−0.055	0.028	−1.986	0.049
Intention_to_Violate_ISSP ← Formalsanction_X_Power distance	H10	−0.354	0.036	−7.303	***
Intention_to_Violate_ISSP ← Moral beliefs_X_Power distance	H11	0.106	0.035	2.265	0.024

The entire stated hypotheses, except three, are found to be significant at least at 95% confidence interval, and hence, they are accepted. More specifically, hypothesis 7 failed to be significant, while hypotheses 9 and 10 were found to be significant, but in the opposite direction to what was stated in the research.

Discussion

In this section, we discuss the result of each hypothesis. As indicated in the first chapter, the main purpose of this study is to examine the moderating influence of national culture on the impact of security countermeasures (formal sanctions), perceived benefits, moral beliefs, and shame on employees' intention to violate ISSP. By using a sample of data collected from medium- and large-sized organisations in Ethiopia, we found strong evidence on the considerable influence of national culture dimensions in strengthening or weakening the relationship between ISS countermeasures and other important variables, as depicted by RCT, and employees' intention to violate ISSP. Thus, in the following paragraphs, we highlight the main findings of the study.

As can be understood from the result of the first hypothesis, formal sanction is found to have a negative influence on employees' intention to violate ISSP. This means when organisations use deterrence mechanisms, in the form of formal rules and policies, it is more likely to be associated with reduced employees' intention of violating their organisation's ISSP. As indicated in the IS literature, there exists inconsistent findings concerning the impact of formal sanctions on reducing computer abuse or IS misuse (D'Arcy & Herath, 2011). The results of our study are consistent with many research outputs in the area of criminology (e.g. Paternoster & Simpson, 1996; Pratt et al., 2006) and, more importantly, in the ISS area. For example, previous studies report the ability of formal sanctions to reduce IS misuse intention (D'Arcy et al., 2007), unauthorised access intention (D'Arcy & Hovav, 2009), ISSP non-compliance (Siponen et al., 2007), and computer abuse incidents (Straub, 1990; Kankanhalli, 2003). In our review of the IS literature, we could not find any empirical studies that explore this relationship in the context of developing economies.

Second, moral belief is found to have a strong negative impact on employees' intention to violate their organisation's ISSP. This means as employees have strong moral beliefs or commitment, they will intend not to violate their organisation's ISSP. This finding is not only consistent with the basic principle of rational choice theory (Becker, 1968), but also with criminology studies, which report that people with low moral beliefs or personal norms are more inclined to engage in deviant behaviour like corporate crime (Paternoster & Simpson, 1996) and tax evasion (Wenzel, 2004). Further, research outputs in psychology (e.g. Blasi, 1980; King & Mayhew, 2002; Rest, 1986 as cited in Myyry et al., 2009) also report that good moral reasoning helps people develop desirable behaviour. More importantly, in the area of ISS, personal norms (Li et al., 2010) and moral beliefs (Siponen & Vance, 2012) are reported as having a positive impact on employees' compliance intention to Internet use policy and a negative impact on intentional violation of ISSP, respectively.

Third, shame is found to have a strong negative effect on employees' intention to violate their organisation's ISSP. This result indicates that as employees feel that violating ISSP is a shameful activity, they will distance themselves from such acts. When we compare our findings against previous studies, it is consistent with studies in the criminology literature (e.g. Grasmick & Bursik, 1990; Nagin & Paternoster, 1993; Tibbetts, 1997). However, when we come to ISS literature, we can only find a single empirical study by Siponen and Vance (2010) that investigates the impact of shame as a deterrent construct, and in that same study, they report the inability of shame to reduce employees' non-compliance to their organisation's ISSP. A plausible reason for the contradiction of our findings with Siponen & Vance (2010) may be due to the difference in the cultural makeup of the sample respondent in the two studies. In this respect, our sample is taken from a more collective society where violating norms leads to a feeling of shame, while the sample for the study conducted by Siponen and Vance (2010) were taken from an individualistic society (Finland) where breaking norms resulted in feelings of guilt, not shame (Hofstede, 1980).

Fourth, perceived benefit is found to be an excellent predictor of employees' violation of ISSP. This means when employees perceive that violating their organisation's ISSP helps them achieve some sort of benefits, they will most probably engage in violating those rules. This finding is similar to what the RCT states: when people make choices, they analyse the outcome of each of the alternatives and choose the one that is perceived to bring more satisfaction/perceived benefits (McCarthy, 2002). Moreover, the finding is consistent with empirical studies in ISS literature: Vance and Siponen (2012) report the significant positive impact of perceived benefits on employees' intention to violate ISSP, while Li et al.

(2010) report a significant negative influence of perceived benefits on employees' compliance intention to Internet use policy.

Hypothesis 5 proposes that the higher the degree of uncertainty avoidance, the weaker the impact of perceived benefits on employees' intention to violate ISSP; as can be seen from Fig. 5, this hypothesis is supported. This means that, even though the perceived benefits of non-compliance initiate employees to violate their organisation's ISSP, the strength of this relationship is weaker for high uncertainty avoidance employees than their low uncertainty avoidance counterparts. In this regard, researches in the area of sociology (e.g. Hofstede, 2003, 2011) found that people who score high in uncertainty avoidance give primary emphasis for the enforcement of rules and regulations, than their low uncertainty avoidance counterparts. If we bring this same scenario to ISS, we may be inclined to say that low uncertainty avoidance employees may violate their organisation's ISSP more often than their high uncertainty avoidance counterparts, as long as there are perceived benefits of violating the policies. In the ISS literature, this result is consistent with those of Timo (2009), who reported that low degree of uncertainty avoidance might lead to ISS problems. To the best of our knowledge, our study is the first empirical study to research the moderating influence of uncertainty avoidance in the relationship between perceived benefits and employees' intention to violate ISSP.

When we come to the sixth hypothesis, it proposes that the higher the degree of masculinity, the stronger the impact of perceived benefits on employees' intention to violate ISSP; this is supported. The finding of this research is consistent with conceptual cultural studies in the field of sociology. Hofstede (2001) states that for people in highly masculine society, the world is "unjust", and if any activity helps them achieve wealth then they will struggle to get it done in any way they can. On the other hand, a financial reporting study by Doupnik and Tsakumis (2004) has found that as masculinity increases people show a tendency to disclose their organisation's secret financial information to outsiders in response to some benefits. Our finding is also consistent with findings in the area of ISS. For example, Timo (2009) found that higher masculinity is most often associated with ISS problems. While the role of masculinity has been studied in different disciplines, to the best of our knowledge, there is no single study in the area of ISS that investigates the moderating influence of masculinity in the relationship between perceived benefits and employees' intention to violate their organisation's ISSP.

The seventh hypothesis claims that the higher the degree of collectivism, the stronger the impact of perceived benefits on employees' intention to violate ISSP. Unfortunately, this hypothesis is not supported. Even though this result is consistent with the findings of some studies that are conducted in various disciplines, the literature indicates that many of the findings related to collectivism have got mixed support. In this regard, Husted (2000) found that the rate at which individualistic societies engage in software piracy is higher than for the less individualistic societies. Contrary to this, Timo (2009), in the area of ISS, Tan et al. (2003), in the area of IS development projects, and Leidner and Kayworth (2006), in the aviation industry, reported that for the perceived benefit of being in harmony with friends and colleagues, peoples in collective society tend not to report their group's wrongdoings. From this we may infer that, for the perceived benefit of being in harmony with friends and colleagues, employees in a collective society may not expose their friends for violating rules, and this may initiate employees to engage in violating their organisation's policies themselves. However, in our study, the perceived benefits of violating organisation's ISSP are measured in terms of saving employees personal and work time, and it has very little, if any, relationship with the perceived benefit of being in harmony with friends. And hence, in such a scenario, as the perceived benefit of saving time increases, employees in a more collective society may not violate their organisation's ISSP more often than employees in less collective societies do. This is because people in an individualistic society are more inclined to show a self-centred character (Hofstede, 2011). This fact might initiate them to override their organisation's rules in exchange for the perceived benefit of saving time.

The eighth hypothesis proposes that the higher the degree of collectivism, the stronger the impact of shame on employees' intention to violate ISSP; this is supported by the collected data. In part, this finding is substantiated by Hofstede's (2011) cultural theory, which states that if people bypass rules in collective societies, then they feel ashamed, while the same action leads to a feeling of guilt in an individualistic society. If we bring this same reality

into ISS, we are inclined to say that shame decreases employees' intention to violate their organisation's ISSP and the strength of this relationship will get stronger and stronger for more collective societies than less collective societies.

In the ninth hypothesis, we propose that the higher the degree of power distance, the stronger the impact of perceived benefits on employees' intention to violate ISSP. This hypothesis is found to be significant, but in the opposite direction to what is being hypothesised, and hence, it is not supported by the collected data. Previous researches in the area of corruption (Husted, 1999) and tax evasion (Tsakumis, 2007) highlighted that as people in high power distance societies perceive that there exists financial benefits for violating rules, they will engage in such activities more often than low power distance societies. Unlike the above two researches, in our study the perceived benefit of violating ISSP is not monetary value, but time, and this may in part influence the finding of our study, because saving time is different from getting money and the two societies may give different levels of importance for these perceived benefits. The result of this research implies that as perceived benefits of saving time increase, employees' intention of violating their organisation's ISSP also increases, and this relationship is stronger for low power distance than high power distance employees. To the best of our knowledge, this is the first study to empirically investigate the moderating impact of power distance between perceived benefits and employees' intention to violate their organisation's ISSP.

In the tenth hypothesis, we propose that the higher the degree of power distance, the weaker the impact of formal sanctions on employees' intention to violate ISSP. The result is found to be significant in the opposite direction from what has been proposed. Even though this result is consistent with some studies, the outputs from different researches show mixed support. In this regard, Husted (1999), in the area of corruption, Tsakumis (2007), in the area of tax evasion, and D'Arcy et al. (2007), in the area of ISS, found that in high power distance societies, people break formal rules and procedures more often than people in low power distance societies. On the other hand, in an empirical work by Dols and Silvius (2010), it is reported that employees in high power distance society are found to be more obedient than low power distance people, to their organisation's rules, given that they are ordered by their boss. In another study by Ifinedo (2009), in the area of IT security management, it is reported that a government-driven security regulation is more successful in high power distance society than in low power distance. Moreover, according to Hofstede (2001), the way bosses behave or act can play a critical role in creating compliance to rules in high power distance society. In this regard, what may be implicit in the mind of our sample respondents is that they feel they are expected/ordered by their boss to comply with their organisation's ISSP.

In the last hypothesis, we proposed that the higher the degree of power distance, the weaker the impact of moral beliefs on employees' intention to violate ISSP. This hypothesis is supported. This finding is consistent with conceptual works in different disciplines. In this regard, in low power distance societies, there exists a participatory management style (Moore, 2003) and it is a good predictor of organisational citizenship behaviour (OCB), which interns associated with a higher degree of compliance with rules, by creating an environment where every individual feels a sense of belonging and is morally more tied up to the wellbeing of their company (Organ & Konovsky, 1998). This means as employees' moral beliefs increase, their intention to violate their organisation's ISSP decreases, and this relationship is stronger for lower power distance employees than their higher power distance counterparts. This idea is partly strengthened by Peterson et al. (2001), who state that, even though the degree of influence varies, both individual's supervisors and people at home do have an influence on an individual's decisions concerning ethical dilemmas like non-compliance with organisation's rules (Peterson et al., 2001).

Finally, the effect of the four control variables (age, gender, CSSE, and realism) on employees' intention to violate their organisation's ISSP was also examined and one of them is found to be significant. The reason to include these variables as a control variable is because the data was collected from different organisations that are located in different parts of Ethiopia. More specifically, CSSE is included as a control variable because the respondents might have a different level of CSSE, while realism is included because each respondent is given a randomly selected scenario (from three scenarios), and we need to investigate if the response of the employees significantly vary based on their assumption of how realistic the given scenario is. In this regard, we found that employees' CSSE

has a considerable positive influence on their intention to violate their organisation's ISSP, while the remaining variables (age, gender, and realism) are found to have an insignificant influence.

Conclusion

As clearly discussed in this paper, even though there exist a number of ISS standards around the world, protecting the ISS becomes a moving target for most organisations. To shed light on this problem (i.e., non-compliance), researchers in the area of ISS have been conducting a number of studies by using different theoretical lenses (e.g. GDT, PMT, RCT); based on their findings, they reported on factors that might have a significant influence on improving employees' information security behaviour. Almost all of these attempts are focused in the western context and what is implicit in most of these studies is that factors that work in one country will also work in another country. Contrary to this, there exist few studies that indicate how country-dependent factors like national culture affect the findings of such studies. Hence, there is an increasing call for researchers around the world to embark on exploring the impact of national culture on employees' information security behaviour. Thus, our study could be taken as an attempt to respond to this timely and critical call for research. In this respect, this study empirically investigated how constructs of rational choice theory (formal sanction, shame, perceived benefits, and moral beliefs) influence employees' intention to violate their organisation's ISSP. In addition to this, the study has also empirically tested the direct moderating influence of national culture dimensions (power distance, uncertainty avoidance, masculine/feminine, and collectivism/individualism) between rational choice theory constructs and employees' intention to violate their organisation's ISSP. Our proposed empirical model is sufficiently supported by the collected data. In this regard, we got a very important empirical evidence on factors that inhibit and also initiate employees to violate their organisation's ISSP. Moreover, the findings show strong evidence on the influence of contextual factors and national culture on employees' information security behaviour, and consequently, highlights the importance of taking some level of precaution when organisations introduce new policies or standards that are copied from abroad. Policy makers and ISS managers in Ethiopia, particularly at INSA, can learn how important it will be to modify or adapt their ISSP, which was copied from ISO 27002, based on the findings of this study.

In addition to the practical implications of our findings, we also highlighted the contribution of our study to research and theory. Based on the limitations of the study, we recommend suggestions for future researchers in the area of ISS, to further enrich the existing knowledge around factors affecting employees' information security behaviour.

Limitations of the study

Just like most empirical researches, this study has got its own limitations. These limitations are discussed below.

The first limitation of this study is the use of only four of the national culture dimensions, namely power distance, uncertainty avoidance, collectivism, and masculinity. The main reason to exclude long-term orientation is due to the fact that Ethiopia does not have a score for this dimension of Hofstede's (1980, 2001) work. Since our research includes a majority of the national culture dimensions, we believe that the absence of one dimension does not have a considerable influence on the research findings.

The second limitation of this study is the use of companies that only have established ISSP. Particularly, each organisation was included in the sample after the ISS officers of the organisations were asked if they have a well-documented and communicated ISSP; we left out organisations that do not have ISSP. This might raise a question on the representativeness of the selected organisations. However, this study could not be realised by including employees who do not work under any ISSP. Moreover, previous studies in the area of ISS also use the same procedures (e.g. Li et al., 2010; Vance & Siponen, 2012).

The third limitation of this study might be the lack of a measure of the actual behaviour of employees, and hence, the use of intention as the dependent variable might raise the question "Whether intention indicates the actual behaviour of employees?" Many researchers argue in favour of using intention as the valuable approximation that provides a good explanation for behaviour. The psychological theory of planned behaviour suggests that

people frequently behave as they predict (Ajzen, 1991). In this respect, researchers such as Paternoster & Simpson (1996), Wenzel (2004), Pahnila et al. (2007), and Siponen and Vance (2010) use intention as a proxy to actual behaviour in their study to predict employees' behaviour in the workplace.

Fourth, due to the sensitive nature of the topic, respondents might intend to provide socially desirable responses to the questions instead of what is prevailing. This may result in relationships between variables in the research model which are against the literature. To reduce this limitation, we use a scenario method. According to Harrington (1996), since the scenario describes others' behaviour in hypothetical cases, respondents will not be intimidated to report their real intentions to agree or disagree with what the scenario illustrates.

Fifth, in addition to the above limitations, since national culture is found to have a significant influence in IS studies (Leidner & Kayworth, 2006), it is important to note that the result of this study may not be applicable to countries outside Ethiopia.

In spite of these limitations, the study has managed to provide very important and timely insight into the problem of employees' violation of their organisational ISSP and how national culture influences employees' compliance behaviour towards ISSP. In this regard, we do believe that this study adds to the growing body of knowledge in the area of ISS and it has met its objective.

Recommendation for Future Studies

In this research, the survey method was used to investigate the moderating influence of national culture between rational choice theory constructs and employees' intentions to violate their organisational ISSP. Although this study answers the research questions stated in the first chapter, there are other issues that need further investigation by future researchers in the field of ISS.

First, this study used a quantitative research method, and we encourage future researchers to complement the survey method with interviews so that the results can be further explained and triangulated.

Second, researchers can repeat this same study in different countries, so that they can test the generalisability of the findings of this study across different countries with a similar national culture profile. As can be understood from the literature, researches in the area of ISS use Hofstede's (1980) cultural values without measuring culture at the individual level, and their output shows inconclusive findings concerning the impact of national culture dimensions across different countries with a similar cultural makeup. Thus, we advise future researchers to conduct similar studies in the context of a developing country (a country with similar cultural makeup as Ethiopia) and see if the findings are generalisable in the context of developing countries with a similar cultural profile. Moreover, since ISSP is a new and sensitive area of research in developing countries, repeating this same study will help secure matured knowledge of ISSP and national culture in the context of a developing country.

Third, further studies are needed to investigate the moderating influence of the collectivism cultural dimension between perceived benefits and intention to violate organisational ISSP. Contrary to our expectations, collectivism is found to dampen the positive relationship between the perceived benefits and intention to violate organisational ISSP. Different research outputs in IS reported that for the perceived benefit of being in harmony with friends, employees in a collective society may not expose their friends for violating the organisation rules, and this may initiate employees to engage in violating organisational policies on their own. In this regard, we do believe that the instrument used to measure perceived benefits needs further research. In our study, the instruments that are used to measure the perceived benefit of non-compliance are mainly confined to saving personal and work time. Thus, we encourage researchers to use a new instrument to find out if the sense of being in harmony with friends overrides employees' intention to follow their organisational ISSP.

Fourth, it could be a very good research avenue if future researchers investigate the impact of constructs that are not included in this study (e.g. informal sanctions and long-term orientation) on employees' ISSP violation intention. This will help enrich the knowledge around factors that contribute to the successfulness of organisational ISSP.

Fifth and finally, even though the theory of reasoned action states that behavioural intention predicts actual behaviour (Ajzen, 1975), future studies could be conducted by

using the actual compliance behaviour as the dependent variable. In this regard, the result obtained from reported compliance can be compared against the result obtained from monitoring employees in their workplace. Even though it is very difficult to objectively measure the actual compliance behaviour of employees, there exists some mechanism, like examining the activity log of employees on their computer or monitoring employees' computer at the end of their work hour, to confirm if they obey some of the organisational security policies (e.g. lock their computer).

References

Abu-Musa, A. A. (2004). Investigating the security controls of CAIS in an emerging economy: An empirical study on the Egyptian banking industry. *Managerial Auditing Journal, 19*(2), 272-302.

Afroprofile. (2013). Africa's top 50 banks. Retrieved from http://www.afroprofile.com/index.php/jobs-in-nigeria/africa-s-top-100-banks.html

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

Al-Awadi, M., & Renaud, K. (2007, July). *Success factors in information security implementation in organizations.* In IADIS International Conference e-Society.

Alexander, C. S., & Becker, H. J. (1978). The use of vignettes in survey research. *Public Opinion Quarterly, 42*(1), 93-104.

Alfawaz, S., Nelson, K., & Mohannak, K. (2010, January). Information security culture: A behaviour compliance conceptual framework. In *Proceedings of the Eighth Australasian Conference on Information Security* (vol. 105, pp. 47-55). Australian Computer Society, Inc.

Alghazzawi, D. M., Hasan, S. H., & Trigui, M. S. (2014). Information systems threats and vulnerabilities. *International Journal of Computer Applications, 89*(3), 25-29.

All Africa Global Media Publisher. (2007). Dashen to resume issuing visa cards. Retrieved June 13, 2013, from http://www.allafrica.com/stories/200708271429.html

Alreck, P. L., & Settle, R. B. (2004). *The survey research handbook* (3rd ed.). Boston, MA: McGraw-Hill.

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*(2), 155-173.

Armstrong, J. S., & Overton, T. S. (1977). Estimating nonresponse bias in mail surveys. *Journal of Marketing Research,* 396-402.

Birch, D. G., & McEvoy, N. A. (1995). Structured risk analysis for information systems. *Hard Money-Soft Outcomes,* 29-51.

Choe, J. M. (2004). The consideration of cultural differences in the design of information systems. *Information & Management, 41*(5), 669-684.

Chow, C. W., Deng, F. J., & Ho, J. L. (2000). The openness of knowledge sharing within organizations: A comparative study of the United States and the People's Republic of China. *Journal of Management Accounting Research, 12*(1), 65-95.

Chua, W. (1986) Radical developments in accounting thought. *Accounting Review, 61,* 601-632.

Clarke, M. (2011). The role of self-efficacy in computer security behavior: Developing the construct of computer security self-efficacy (CSSE). ProQuest LLC.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, 189-211.

Converse, J. M., & Presser, S. (1986). *Survey questions: Handcrafting the standardised questionnaire.* SAGE Publications.

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM, 50*(10), 113-117.

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), 79-98.

D'Arcy, J., & 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), 643-658.

De Mooij, M., & Hofstede, G. (2010). The Hofstede model: Applications to global branding and advertising strategy and research. *International Journal of Advertising, 29*(1), 85-110.

De Vreede, G. J., Jones, N., & Mgaya, R. J. (1998). Exploring the application and acceptance of group support systems in Africa. *Journal of Management Information Systems*, 197-234.

Devamohan, A. (2008). E-banking problems and prospects in Ethiopia. Retrieved from http://wA.Devamohan%20-%20E-banking.htm.

Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security, 7*(4), 171-175.

Dhillon, G., & Moores, S. (2001). Computer crimes: Theorizing about the enemy within. *Computers & Security, 20*(8), 715-723.

Ethiopian Radio and Television Agency. (2012). The Ethiopian radio and television agency. Retrieved from http://www.ertagov.com/news/

Ferketich, S., Phillips, L., & Verran, J. (1993). Development and administration of a survey instrument for cross-cultural research. *Research in Nursing & Health, 16*(3), 227-230.

Field, A. (2009). *Discovering statistics using SPSS.* Sage Publication.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2010). *Multivariate data analysis* (6th ed.). NY: Pearson.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2010). *Multivariate data analysis* (7th ed.). NY: Pearson.

Hamill, J. T., Deckro, R. F., & Kloeber, J. M. (2005). Evaluating information assurance strategies. *Decision Support Systems, 39*(3), 463-484.

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20*(3), 257-278.

Hasan, H., & Ditsa, G. (1999). The impact of culture on the adoption of IT: An interpretive study. *Journal of Global Information Management (JGIM), 7*(1), 5-15.

Hechter, M., & Kanazawa, S. (1997). Sociological rational choice theory. Annual review of 9 to 5 underground: Are you policing computer crimes? *MIT Sloan Management Review, 30*(4), 35.

Hofstede, G. (1980). *Culture's consequences: International differences in work-related values.* Beverly Hills, CA: Sage Publications.

Hofstede, G. (1983). Dimensions of national cultures in fifty countries and three regions. In *Expiscations in Cross-Cultural Psychology*. Lisse, Netherlands: Swets & Zeitlinger.

Hofstede, G., (1991). *Cultures and organizations: Software of the mind: Intercultural cooperation and its importance for survival*. London: McGraw-Hill.

Hofstede, G. (2000). The information age across cultures. *Proceedings of 5th AIM Conference: Information Systems and Organizational Change.*

Johns, S. K., Smith, M., & Norman, C. S. (2002). How culture affects the use of information technology. In *Accounting Forum* (vol. 27, no. 1, pp. 84-109).

Jones, M. L. (2007). Hofstede-culturally questionable?

Kohlberg, L. (1984). *Essays on moral development: The psychology of moral development* (vol. 2). New\Brk: Harper & Row.

Krueger, N., & Dickson, P. R. (1994). How believing in ourselves increases risk taking: Perceived self-efficacy and opportunity recognition. *Decision Sciences, 25*(3), 385-400.

Lafree, G., Ducan, L., & Piquero, A. R. (2005). Testing a rational choice model of airline hijackings. *Criminology, 43*(4), 340-361.

Morgan, G. A., & Griego, O. V. (1998). *Easy use and interpretation of SPSS for Windows: Answering research questions with statistics*. Psychology Press.

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

Singleton, J., & Straits, B. C. (2005). *Approaches to social research.* New York, NY: Oxford University Press.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Siponen, M. T. (2001). Five dimensions of information security awareness. *Computers and Society, 31*(2), 24-29.

Siponen, M. T. (2005). An analysis of the traditional IS security approaches: Implications for research and practice. *European Journal of Information Systems, 14*(3), 303-315.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information

systems security policy violations. *MIS Quarterly, 34*(3), 487.

Siponen, M., Pahnila, S., & Mahmood, A. (2006). Factors influencing protection motivation and IS security policy compliance. In *Innovations in Information Technology* (pp. 1-5). IEEE.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: An empirical study. In *New Approaches for Security, Privacy and Trust in Complex Environments* (pp. 133-144). US: Springer.

Slay, J. (2003). IS security, trust and culture: A theoretical framework for managing IS security in multicultural settings. *The Emerald Research Register, 20*(3), 98-104.

Soares, A. M., Farhangmehr, M., & Shoham, A. (2007). Hofstede's dimensions of culture in international marketing studies. *Journal of Business Research, 60*(3), 277-284.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security, 22*(1), 42-75.

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48*(7), 296-302.

Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly,* 45-60.

Straub, D. W. (1994). The effect of culture on IT diffusion: E-Mail and FAX in Japan and the US. *Information Systems Research, 5*(1), 23-47.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly,* 441-469.

Straub, D. W., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *The Communications of the Association for Information Systems, 13*(1), 63.

Zhang, Z., Wong, D. S., Xu, J., & Feng, D. (2006, June). *Certificateless public-key signature: Security model and efficient construction*. In International Conference on Applied Cryptography and Network Security (pp. 293-308). Springer Berlin Heidelberg.

APPENDICES

Appendix 1: Scenario and Instrumentation

Information Systems Security Survey

	Section One **Please provide your level of agreement or disagreement** *with the following statements. (Please mark only one 'X' for each line in the labelled column.)* **Strongly Disagree = 1; Disagree = 2; Neutral = 3; Agree = 4; Strongly Agree = 5**	**1**	**2**	**3**	**4**	**5**
1	I would feel comfortable following most of my organisation's information systems security policies on my own.					
2	If I wanted to, I could easily follow my organisation's information systems security policies on my own.					
3	I would be able to follow most of my organisation's information systems security policies even if there was no one around to help me.					
4	People in higher organisational positions should make most decisions without consulting people in lower positions.					
5	People in higher organisational positions should not ask the opinions of people in lower positions too frequently.					
6	People in higher organisational positions should avoid social interaction with people in lower positions.					
7	People in lower organisation positions should not disagree with decisions by people in higher positions.					
8	People in higher organisational positions should not delegate important tasks to people in lower positions.					
9	People should avoid making changes because things could get worse.					
10	Change should be avoided when its outcomes are uncertain.					

11	It is better to work in an organisation with specific rules and regulations as opposed to a more flexible organisation.					
12	I would prefer a bad situation that I know about to an uncertain situation which might be better.					
13	Providing opportunities to be innovative is more important than requiring standardised work procedures.					
14	It is important that people take initiative in their work rather than always following step-by-step instructions.					
15	Individuals should sacrifice self-interest for the group.					
16	Individuals should stick with the group even through difficulties.					
17	Group welfare is more important than individual rewards.					
18	Group success is more important than individual success.					
19	Individuals should only pursue their goals after considering the welfare of the group.					
20	Group loyalty should be encouraged even if individual goals suffer.					
21	It is more important for men to have a professional career than it is for women.					
22	Men usually solve problems with logical analysis; women usually solve problems with intuition.					
23	Solving difficult problems usually requires an active, forcible approach, which is typical of men.					
24	There are some jobs that a man can always do better than a woman.					
25	Non-compliance with an organisation's information systems security policies saves work time.					
26	Non-compliance with an organisation's information systems security policies saves employees' time.					

Section Two *Please Read the Following Scenario*						
Jack is working in a position that requires access to customers' personal information. However, his company's information security policy prohibits him from giving customers' personal information to anyone, except the main office. Jack is expected to send some of the customers' personal information to the main office but the Internet connection in his office is too slow to send the data. So Jack believes that asking his friend to send the customer information from his office with a convenient Internet connection could save a lot time and money for the company. He also knows that an employee was recently reprimanded (criticised) for sending data through an unauthorised person. Jack gives the data to his friend to send to the main office.						
Please provide your level of agreement or disagreement with the following statements. (Please mark only one 'X' for each line in the labelled column.) *Strongly Disagree = 1; Disagree = 2; Neutral = 3; Agree = 4; Strongly Agree = 5*		*1*	*2*	*3*	*4*	*5*
27	I would do what Jack did in the scenario.					
28	I feel that Jack acted wrongly by violating the company's information systems security policy.					
29	It is morally wrong to do what Jack did in the scenario.					
30	It is morally wrong to violate company information systems security policies.					
31	If I did what Jack did, I would save personal time.					
32	If I did what Jack did, I would save work time.					
Based on the above scenario, please rate how problematic the following statements are. *(Please mark only one 'X' in the column.)* *Not problematic = 1, Somewhat problematic = 2, Neutral = 3, Problematic = 4, Very problematic = 5*						
33	How much of a problem would it create in your life if you were sanctioned (punished) for doing what Jack did?					
34	How much of a problem would it create in your life if you were formally reprimanded (**criticised**) for doing what Jack did?					

	Section Three					
	Please rate the likelihood *of the following statements. (Please mark only one 'X' in the column.)* **Highly Unlikely = 1; Unlikely = 2; Neutral = 3; Likely = 4; Highly Likely = 5**	*1*	*2*	*3*	*4*	*5*
35	How likely is it that you would be ashamed if co-workers knew that you had violated company information security policy?					
36	What is the likelihood that you would be formally reprimanded (criticised) if management learned you had violated the company's information security policy?					
37	What is the likelihood that you would be formally sanctioned if management learned you had violated the company's information security policy?					
38	What is the likelihood that you would receive sanctions if you violated the company's information security policy?					
	Please rate how problematic the following statements are. *(Please mark only one 'X' in the column.)* **Not problematic = 1, Somewhat problematic = 2, Neutral = 3, Problematic = 4, Very problematic = 5**	*1*	*2*	*3*	*4*	*5*
39	How problematic would it be if you felt ashamed that co-workers knew you had violated the company information security policy?					
40	How much of a problem would it be if you received severe sanctions if you violated the company information security policy?					

	Please rate the likelihood of the following statement. (Please mark only one 'X' in the column.) Highly Unlikely = 1; Unlikely = 2; Neutral = 3; Likely = 4; Highly Likely = 5	*1*	*2*	*3*	*4*	*5*
41	How likely is it that you would be ashamed if others knew that you had violated the company information security policy?					
	Please rate how problematic the following statement is. *(Please mark only one 'X' in the column)* **Not problematic = 1, Somewhat problematic = 2, Neutral = 3, Problematic = 4, Very problematic = 5**	*1*	*2*	*3*	*4*	*5*
42	How problematic would it be if you felt ashamed that others knew you had violated the company information security policy?					
	Please rate the likelihood of the following statement. (Please mark only one 'X' in the column.) Highly Unlikely = 1; Unlikely = 2; Neutral = 3; Likely = 4; Highly Likely = 5	*1*	*2*	*3*	*4*	*5*
43	How likely is it that you would be ashamed if managers knew that you had violated the company information security policy?					
	Please rate how problematic the following statement is. (Please mark only one 'X' in the column.) Not problematic = 1, Somewhat problematic = 2, Neutral = 3, Problematic = 4, Very problematic = 5	*1*	*2*	*3*	*4*	*5*
44	How problematic would it be if you felt ashamed that managers knew you had violated the company information security policy?					

Section Four

General Questions (for classification purposes only)

Please indicate your gender ___ Female ___ Male

How realistic is the given scenario?

___Non-realistic _____Somewhat realistic ____Realistic

What is your highest completed education certification?

___ High school certificate/diploma

___ Bachelor's degree

___ Master's degree

___ Doctoral degree

___ Others, please specify _____

What is your age? _____ years

Years of computer usage:

___ ≥ 10years ___ ≥ 5 years ___ ≥ 2 years ___< 2 year

What is your current employment status?

_____ Student ____ Employee _____ Retired _____ Others