A Study of Employees' Information Security Policy Violation and Rational Choice Theory: The Case of Ethiopia

Tilahun Muluneh Arage

A Dissertation Submitted to IT Doctoral Program

Presented in Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Information Technology (Information Systems)

Addis Ababa University
Addis Ababa, Ethiopia
February 2017

ABSTRACT

A Study of Employees' Information Security Policy Violation and Rational Choice Theory: The Case of Ethiopia

Tilahun Muluneh
Addis Ababa University, 2017

Nowadays, it becomes clear that information systems security (ISS) is one of the most important issues that organizations need to focus on. Despite huge investments made by companies to keep their information systems (IS) safe, there are many ISS breaches that infiltrate companies' systems and consequently, these cost their reputation, affect customers' confidence, and bring huge financial losses. Ethiopian companies are not immune to the ISS problem and there are some signs of ISS breaches. The ISS literature suggests that almost all investments in ISS related issues are for technological solutions. However, this type of solutions alone does 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 ISS breaches are caused by employees who are the legitimate users of organizations' IS. So "how can we counter the illegal action of our own employees?" is the main agenda this research tries to address. Many researchers advocate the use of deterrence mechanisms to decrease the employees' noncompliance problem. Despite these findings, there is a lot of research output that reported the inability of the deterrent countermeasures alone to protect IS from security breaches. And more importantly, some researchers point out that different cultures require different ISS interventions. Interestingly, in the last decade, some researchers have studied how culture can influence people's intention towards ISSP (information systems security policy) compliance. However, most of the current ISS (information systems security) studies assume that deterrent countermeasures' effect is uniform across countries and culture. This situation identifies a gap that needs to be bridged, and this study address the issue by raising the question "To what extent, if any, national culture moderates the influence of formal

sanctions, perceived benefits, moral beliefs, and shame on employees' intention to violate ISSP?" We use survey method to collect data and SPSS Amos to conduct SEM (Structural Equation Modeling) based data analysis. Finally, we get results that show the moderating impact of national culture on the influence of formal sanctions, perceived benefits, moral beliefs, and shame on employees' intention to violate ISSP.

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

DEDICATION

To my father Muluneh Arage Tesema who is always eager to see my academic success. He has always been proud that his son is working toward a PhD. and now is the time to tell you that I did it. It is by and for you. In the same way, I would like to dedicate this dissertation to my beloved mother Aguagu Gebre Egziabher, even though she is not alive to see my final success, it is with pride and affection that I dedicate this dissertation to her.

ACKNOWLEDGEMENT

First and foremost, I praise the Almighty God!

This work would not come to its final shape without the incredible support of the following people. First, I would like to express my sincere gratitude to my advisor, Dr. France Belanger. She shared me her knowledge and experience without reservation throughout the process of conducting this dissertation. Beyond her professional support, she helped me to visit her university, Virginia Tech University, where I did a lot of work and expand my professional ties with established scientists in the field of IS. Professor, I will never forget you and your husband care that extends my stay in the USA interesting and successful.

I would like to express my heartfelt appreciation to my co-advisor Dr. Tibebe Beshah. Whenever I faced difficulties, he is always there to provide me his invaluable advices and supports. His friendly approach and encouragement played a great role in the successful accomplishment of my study. In addition to this, as a member of my dissertation committee Dr. Mesfin Kifle shall also take millions of thanks for taking his time reading my dissertation, attending my presentations and providing invaluable feedback for the improvement of my dissertation.

I also have a very big thanks to my girlfriend Azeb Mekonnen Bekele, she has shown me the maximum possible patience and encouragement in all aspect.

I also extend unlimited thanks to the IT PhD community and my staff members at the AAU School of commerce for the continued support and encouragement during my study.

Tilahun Muluneh Arage
February 2017

DECLARATION

I, hereby, declare that the materials contained in this dissertation have not been previously submitted for a degree in this or any other university. I further declare that this dissertation is solely based on my own research.

I also declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct.

I understand that my dissertation may be made electronically available to the general public for reference purpose.

Tilahun Muluneh

PUBLICATIONS ASSOCIATED WITH THE DISSERTATION

Arage, T., Bélanger, F., & Beshah, T. (2015). Influence of National Culture on Employees' Compliance with Information Systems Security (ISS) Policies: Towards ISS Culture in Ethiopian Companies, 'AMCIS2015', Association for Information Systems.

Arage, T. & Beshah, T. (2016). An Integrated Approach to Information Systems Security Policy Violation: The Case of Ethiopia, 'INFOS2016', ACM International Conference.

Arage, T., Bélanger, F., & Beshah, T. (2016). An Empirical Investigation of the Role of Culture on Employees' Information Systems Security Policy Compliance: Developing Economy Context, 'AMCIS2016', Association for Information Systems.

Arage, T., Bélanger, F., & Beshah, T. (2016). Investigating the Moderating Impact of National Culture in Information Systems Security Policy Violation: The Case of Italy and Ethiopia, 'MCIS2016', Association for Information Systems.

LIST OF ABBREVIATIONS

1. AGFI	Adjusted Goodness of Fit Index
2. AMOS	Analysis of Movement of Structures
3. AVE	Average variance extracted
4. CFA	Confirmatory factor analysis
5. CFI	Comparative fit index
6. CR	Construct reliability
7. CSE	Computer Self-Efficacy
8. CSSE	Computer Security Self-Efficacy
9. E-Banking	Electronic Banking
10. E-Commerce	Electronic Commerce
11. E-Payment	Electronic Payment
12. GDT	General Deterrence Theory
13. GFI	Goodness of Fit Index
14. GOF	Goodness of Fit
15. IEC	International Electro technical Commission
16. INSA	Information Network Security Agency
17. IS	Information Systems
18. ISA	Information Security Awareness
19. ISO	International Standardization Organization
20. ISS	Information Systems Security
21. ISSP	Information Systems Security Policy
22. MTMM	Multitrait-Multimethod
23. OCB	Organizational Citizenship Behavior
24. PCFI	Parsimony comparative fit index
25. PNFI	Parsimony normed fit index
26. POE	Panel of experts
27. RCT	Rational Choice Theory
28. RMSEA	Root mean square error of approximation
29. SEM	Structural Equation Modelling

30. SMC	Squared multiple correlation
31. SPSS	Statistical Software for Social Science
32. SRMR	Standardized root mean residual
33. TLI	Tucker-Lewis index

TABLE OF CONTENTS

Contents Page

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1. 1. BACKGROUND OF THE STUDY

Many organizations around the world are faced with an increasing number of information systems security (ISS) attacks on their systems. While the ISS world often focuses on analyzing and counteracting threats of external origin (Magklaras et al., 2006), most of these threats are originated from insiders (D'Arcy et al., 2009; Bulgurcu, 2010; Hedstrom et al., 2013; Lowry and Moody, 2015). According to a report by Kroll Advisory Solution (2012), 79% of all information security breaches that are happened in US hospitals concerning patients' secret medical information are caused by insiders.

The frequency of occurrence is not the only indicator of the impact of insiders' incidents, but also there are considerable financial costs attributed to legitimate user actions (Magklaras et al., 2006, Crossler et al., 2013). Many researchers (Magklara et al., 2002; Theoharidou et al., 2005; Warkentin et al., 2009, Hedstrom et al., 2013, Lowry and Moody, 2015) reported that insider threat remains the greatest single risk to organizations, and with this respect most ISS experts agree that more successful attacks usually come from inside the organization instead of outside, and that insider attacks are potentially more costly (Schultz, 2002; Shaw et al., 1998). In order to reduce the ever increasing number of ISS breaches, information security managers should strive to understand employees underlying reasons for complying or not complying with organizational security policies (Hedstrom et al., 2013).

The above discussion clearly shows how organizations' ISS are highly threatened by insiders, and we believe that researchers need to invest their time and energy to shed light on this problem. In this regard, our study contributes its part by investigating some of the factors that might influence employees' violation of their organization's information systems security policy (ISSP). As can be understood from the IS literature, in developing countries, there exist

very little knowledge about "how different factors like culture related to ISS and its management" (Salahuddin, 2011). Thus, we believe that it is time to give attention to ISS issues in the developing country context. In this respect, this research takes Ethiopia as one of the developing countries and examined how national culture play a role in ISSP violation. In the upcoming paragraphs, we provide a brief overview of ISS related studies in Ethiopia.
When we explore the ISS breach problems in Ethiopia, due to lack of studies in the areas of ISS, it is difficult to know the exact statistical figure with respect to the financial losses of the incidents. Interestingly, we tried to make an interview with IT security officers of different banks located in Addis Ababa, but they are not willing to state financial losses they incurred by ISS breaches. Even though there is a lack of documented and published information with respect to the ISS in Ethiopia, there are some indications which show us the existence of an ISS breaches problem in the country. For example, according to Fortune (2012), the Ethiopian Revenue and Custom Authority junior database administrator use the password, which is provided to him by his boss (because she went abroad), to deliberately delete the data related to a tax which the organization is expected to collect from its customers. In return, he received 800,000 Birr, and this single incident cost the organization 13,000,000 Birr.

In another instance of ISSP violation, the Ethiopian Airlines has terminated eleven employees working in different units because they fail to follow the ISSP of the organization (EthioNews, 2013). The suspected abuse of the systems is connected to the Sheba Miles program, whereby any customer can get a prize for travelling a specified amount of miles in a given time. The sources indicated that the alleged wrongdoing was uncovered following a request by loyal and long term customers of the Airlines. Obviously, this incident might have impact in damaging the good image of the Airlines, which in turn might bring some kind of financial loss to the company.

Even though it is difficult to get a well-documented information about the insiders attack on Ethiopian financial institutions, we summarize those few works that shed light on ISS related issues in Ethiopian banks. In this regard, a research by Devamohan (2008) found out that the Ethiopian banking industry isn't doing well with respect to securing their systems, and he

added that the new e-banking systems will not be successful until customers are satisfied with privacy and security aspects of the banks. According to Gardachew (2010), cyber security issues are the most important challenges for development of e-banking in Ethiopia, he added that in the deployment of e-banking application, attention should be drawn to the prevention of ISS crimes. According to Bultum (2012) one of the major barriers Ethiopian banking industry faces in the adoption of e-banking is a security risk. In addition to this, researchers such as: Taddesse and Kidan, (2005), Woretaw and Lessa (2012) have found out that ISS issue is one of the major challenges in the development of e-payment (electronic payment) in Africa. They added that differences in the degree of the required security and efficiency among people of different cultures and level of development aggravate the problem. This latter research indicates that culture is one of the factors that needs due consideration when we think of securing our systems from ISS breaches in the developing country context.

Even though there is a lack of well-organized and recorded studies and statistical figures, few of the research works and the figures mentioned in this section show the existence of ISS breaches problems in Ethiopia. Based on the literature review of the ISS studies in Ethiopia, we found out that almost all of them (e.g. Devamohan, 2008; Gardachew, 2010; Bultum, 2012, Woretaw and Lessa (2012)) recommend technological solutions to solve the ISS problems; however, technological solution alone couldn't bring the required level of security. Most of the researches in the area of information security has been technically oriented (Hedstrom et al., 2013). In this regards, one of the most important issues that is given very little emphasis is the behavioral issue, such as culture (Tsakumis et al., 2007; Arage et al., 2016).

Thus, our research work brings together security based RCT and national culture together to shed light on the issues of reducing the ISS problem.

1.2 . STATEMENT OF THE PROBLEM

The main research problem that initiates this research work is the lack of studies in every corner of the world in general and Africa in particular that investigates how national culture moderate the influence of formal sanctions, perceived benefits, moral beliefs and shame on employees' intention to violate ISSP. Despite signs of ISS problems in Africa and particularly in Ethiopia (Gardachew, 2010; Bultum and Ayana, 2012; Taddesse and Kidan, 2005, Woretaw and Lessa, 2012), 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 behavior is culture, and to this end, there is hardly any attempt to explore the influence of national culture on ISSP compliance (Arage et al., 2016).

In order to clearly show the ever increasing number of ISS breaches, it is important to see some statistical figures at global perspective. The ISS threat that is caused by insiders or employees noncompliance is not limited to Africa, the literature shows the existence of many ISS breaches problems all over the world. According to Garg et al. (2003), until the year 2003 companies all over the world are losing more than $2 trillion due to ISS breaches. This problem will be more frustrating when we realize that most of the breaches are caused by insiders. In this regards, between one-half and three-quarters of all ISS breaches are caused by insiders (Ernst and Young, 2003; Information Week, 2005). Because only a fraction of ISS incidents are actually discovered (Hoffer and Straub, 1989; Whitman, 2003; Crossler et al., 2013) the statistical figures from different reports and studies might be lower than the actual fact. Since insiders do have better access to the companies secured information, they can bring catastrophic consequence to their company in terms of financial as well as non-financial aspects, such as: the good image of the company, customers' confidence and many more (D'Arcy et al., 2009; Karjalainen, 2013). 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, p. 3). The cyber security watch Survey (2010) annual report indicates more than $2 billion in losses to organizations due to ISS breaches between 1997 and 2007. According to the survey, companies might continue to suffer more losses in the future

provided 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 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)

As can be understood from the above statistical figures, the ISS breach problem is increasing at alarming rate. To tackle the ever increasing ISS breaches problems, researchers in Europe and the USA try to address the noncompliance problem not only from technical only view but they also use behavioral perspective. Considering socio-organizational elements in addition to mere technical solutions is very important in protecting information systems from security breaches (D'Arcy et al., 2009, Posey et al., 2013). In this regards, we can mention the work of Dols and Silvius (2010) in Europe and the work of D'Arcy et al. (2012) in the USA that investigate the influence of national culture on employees' compliance to ISSP. But when we come to Africa, it is very difficult to get studies that 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; Lowry and Moody, 2015). For example, if we take some of the recent studies that examine the effectiveness of various ISS countermeasures, most of them (D'Arcy et al., 2012; Herath and Rao, 2009a, b; Higgins, 2005; Kankanhalli et al., 2003; Li et al., 2010; Zhang et al., 2006) use samples from the USA, while others (Lee et al., 2004; D'Arcy et al., 2012) use samples from South Korea and some (Pahnila et al., 2007; Siponen et al., 2007; Siponen and Vance, 2010; Karjalainen, 2013) use samples from Finland and also Switzerland.

This indicates that almost all studies in this area focus on the western and eastern cultures (see Appendix 1). So, how can the output from them be applied to countries with a different culture

like Ethiopia? If organizations plan to develop an effective information security culture, they should take into account the impact of both national and organizational culture (Chaula, 2006; Parsons et al., 2013). For example, the international electro-technical commission /international standardization organization (ISO/IEC) 27002, one of the most widely adopted standards for ISS management, draws heavily on general deterrence theory (GDT) in recommending policies, guidelines, and awareness programs for individuals who misuse company resources (D'Arcy and Herath, 2011; Lowry and Moody, 2015). So, can we directly implement these types of information security policy standards? We suggest the answer is no, and this creates a gap that needs to be addressed by studies. In this regards, according to Karjalainen et al. (2013) different cultures require different ISS interventions. ISO is an international standardization body that issues standards in many areas including IT and security management. These standards could either be applied by the member countries as they are or can be customized to national current development situation and requirements (Yigezu, 2011). In the area of information and ISS, ISO issued different standards, for example, ISO/IEC 27002 contains security recommendations for 12 security domains (ISO, 2005). According to ISO (2005), security compliance is one of the domains which help companies to ensure compliance with organizational standards, policies, rules and regulations, procedures and norms. Implementations of these ISSP help companies to better prepare to manage their organizations' ISS (Yigezu, 2011). Since Ethiopia is a full member of ISO, the security policies (ISO Policies) could be adopted or modified based on facts and findings from a research work.

A research conducted by D'Arcy et al. (2012) tried to examine the impact of national culture in the successful implementation of ISSP by taking some samples from the USA and South Korea. Their findings show that measures that are effective in the USA fail to be effective in South Korea and vice versa. In addition to this, other studies (actually done in western culture) found out that the interaction between IT and people is moderated by culture (Dagwell and Weber, 1983; Keil et al., 2000; Tan et al., 2003; Dinev, 2009; Parsons et al., 2013; Karjalainen, 2013).

Thus, our research contributes in identifying the moderating impact of national culture on the influence of formal sanctions, perceived benefits, moral beliefs, and shame on employees' intention to violate ISSP. This valuable output allows ISS personnel and managers to make better decisions on developing effective ISSP that best fit one's (Ethiopian) culture.

1.3. RESEARCH QUESTIONS

The major purpose of this research is to examine whether cultural difference moderate the influence of formal sanctions, perceived benefits, moral beliefs, and shame on employees' intention to violate ISSP. In addition to this, we investigated the influence of formal sanctions, perceived benefits, moral beliefs, and shame on employees' ISSP violation.

Thus, the following research questions guide this research:

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

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

1.4. RESEARCH MODEL AND HYPOTHESES

To answer the research questions, we formulated several hypotheses. Before we start the formulation of these hypotheses, we discussed some facts from the literature that can highlight how we come to construct the theoretical framework of this study, particularly how we select the theories and constructs.

To study employees ISS behavior, a number of theories have been used over the years. In this regards, theories such as: protection motivation theory (e.g. Pahnila et al., 2007; Siponen et al., 2006; Workman et al., 2008; Herath & Rao, 2009a), general deterrence theory (e.g. Kankanhalli et al., 2003; D'Arcy and Hovav, 2007; D'Arcy et al., 2009; Harrington, 1996; Straub, 1990), and agency theory (e.g. Herath and Rao, 2009b) 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 are based on GDT and /or PMT, which are mainly fear based strategies, that is fear of sanction and threat to organization ISS. According to the authors, this will gives only a partial explanation to the problem of ISSP violation.

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, rational choice theory (RCT) goes beyond this limitation and includes perceived benefits and moral beliefs as additional determinants of ISS compliance. The theory clearly states that individuals will always go through a utilitarian calculation of perceived benefits, moral beliefs, shame, formal and informal sanctions when they make decision toward obeying or violate rules (Vance & Siponen, 2012).

Because of its parsimonious and elegant explanation, the RCT has been widely applied to the study of individual, social, and economic behaviors in many contexts (McCarthy, 2002). In this regards, RCT is well suited to explain white collar crime than a street level crime (Cao, 2004) and thus, it will be valuable to use this theory to better explain employees' ISSP compliance behavior. 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, we can mention some works (e.g. Bulgurcu et al., 2010; Li et al., 2010; Siponen & Vance, 2012) that go beyond the norm and analyze the ISS issues by using RCT into their empirical researches. When we critically analyze their contribution to the ISS world, mainly they introducing the RCT theory to the IS discipline (Vance & Siponen, 2012), and that is outstanding contribution. On the other hand, we believe that these studies do have their own limitations, for example, all of them use sample from western culture (Europe & USA) and hence the result of their research may not be valid for other cultures, particularly for countries in the developing economy like Ethiopia. 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 culture 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 with compliance, and they advise the inclusion of national culture when designing ISSP practice and technology. Even though culture can be studied at different level (e.g. organizational, national), it is identified on the literature that national culture has been shown to impact information security more than organizational culture (Phlep, 2005). Due to this fact, we incline to focus on national culture. Hence, we believe that the choice of national culture as one of the theoretical lenses is appropriate.

with respect to the choice of constructs from the two theories (RCT and National culture), mainly we focused on variables that have been given less emphasis but predicted as having considerable impact on employees' compliance behavior. In addition to this, we includes variables that have been reported to have inconsistent impact on employees' compliance behavior so that our study shed light on factor that might contribute to the inconsistent finding. With respect to national culture, even though it has five dimensions (Hofstede, 1980, 1984, and 2001), the cultural hypotheses of this study addressed only four of them, namely: power distance, uncertainty avoidance, collectivism/ individualism, and masculine/feminine. The decision to exclude long term orientation dimension of national culture is 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 of the RCT constructs, namely: formal sanctions, perceived benefits, moral beliefs, and shame while we exclude informal sanction. The reason to exclude informal sanction is because it is relatively addressed in a detail manner by previous studies (Siponen et al., 2007; Harrington, 1996; Siponen and Vance, 2010; Pahnila et al., 2007) and we believe that the remaining constructs need a more close eyes by researchers.

As can be seen from the research model (Figure 1.1) there are 11 hypotheses.

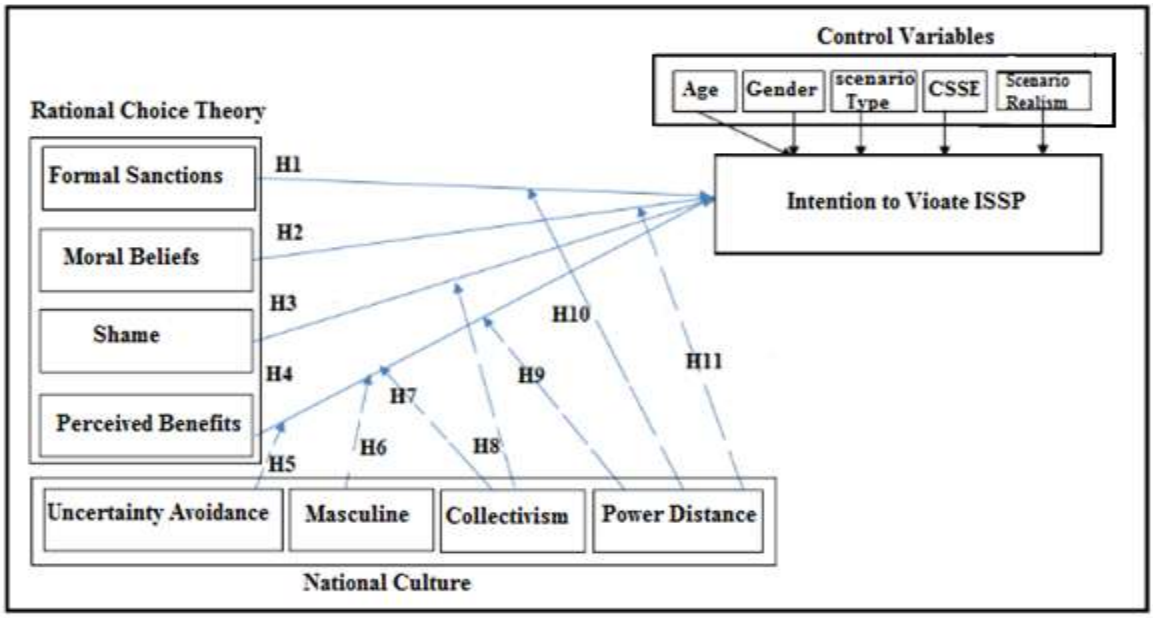

Figure 1.1: The Research Model

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 is on employees' intention to violate ISSP

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

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

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

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

H10: The higher the degree of power distance, the weaker the impact of formal sanctions is on employees' intention to violate ISSP

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

1.5. OBJECTIVES OF THE RESEARCH

The general objective of this study is to build and test an empirical model that shows the moderating influence of national culture on the influence of formal sanctions, perceived benefits, moral beliefs, and shame on employees' intention to violate ISSP. In addition to this, we set out an objective to investigate the direct influence of formal sanctions, perceived benefits, moral beliefs, and shame on employees' intention to violate ISSP.

To address the general objective of the research, we accomplished the following specific objectives:

- Identify, present and discuss the different dimensions of Hofstede (1980, 1984, and 2001) national cultural model.
- Identify, present and discuss the different dimensions of the RCT.
- Test the moderating effect of the dimensions of the national culture in a survey study among employees who work in organizations located in Ethiopia.
- Identify and discuss the important cultural factors to take into account in the process of developing and implementing organizational ISSP and practices.
- Identify and discuss the important RCT factors to take into account in the process of developing and implementing organizational ISSP and practices
- Construct an empirical model in which the moderating effect of national culture dimensions is tested between RCT constructs and employees' intention to violate ISSP.

1.6. RESEARCH METHODOLOGY

Since researchers are expected to clearly formulate their research methodology in advance, we illustrate the research's underlying philosophies: ontology, epistemology, and method. Ontology focuses on the question of what is taken as real and how to know whether something is real (Orlikowski and Baroudi, 1991; Guba and Lincoln, 2005; Merterns, 2007). The underlying ontology used here is close to positivist paradigm, particularly reality as a contextual field of information (Morgan and Smircich, 1980). The choice for this position is done because we are expected to conduct a detailed qualitative analysis of literature to select important theories and constructs for the study. In addition to this, the purpose of the current research is to develop and validate an empirical model consisting of testable hypotheses.

The epistemological assumptions are concerned with the nature of knowledge and how we can get it. Crotty (1998) discusses three epistemological positions: objectivism, constructivism, and subjectivism. Our research epistemological view is objectivism. In 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 (Crotty, 1998).

When we come to the research method, we used a quantitative method. The rationale for adopting a quantitative method is because it provides the ability to produce objective, reliable, and quantifiable information that can easily be generalized to some larger population. Whenever the purpose of a study is hypothesis testing using statistical methods, quantitative survey approach is the best choice (Creswell, 2009). The research utilized questionnaire-based data-gathering technique 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 and Thomas, 2008). The survey methodology also leads to greater generalizability of the results when compared to other research methods (McGrath, 1981). We used Hofstede's (1980, 1984, and

2001) model of cultural dimensions because it has been rigorously validated in previous cross-cultural studies over time and in many countries (Sondergaard, 1994).

With respect to data analysis, we used SEM (Structural Equation Modeling) based statistical analysis to evaluate the relationship between 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 are interested in so that we will be 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 the sample, starting from the top at the population and working down to the sample (Bailey, 1982). In our research, the populations include employees who are working in different organizations located at various part of Ethiopia l (i.e. Addis Ababa, Mekele, Bahir Dar, Dire Dawa, and Hawassa). In each organization individuals are selected randomly.

Researchers should check whether the sample size is enough before conducting their study, this is because small sample sizes can result in non-convergence and improper solutions (Anderson and Gerbing, 1984; Fornell and Larcker, 1981). Anderson and Gerbing (1984) stated that researchers need to have 150 or more usable responses to conduct a quantitative analysis. After dispatching our questionnaires, we managed to get 210 usable responses, which is above the minimum threshold. In this study, we used previously validated instruments while Statistical Package for the Social Sciences with Analysis of Movement of Structures (SPSS Amos) software is used to run different types of statistical analyses.

1.7. OVERVIEW OF INFORMATION SYSTEMS SECURITY

The security of IS in an organization is a critical activity for information intensive organizations (Herath and Rao, 2009b). Nowadays, organizations are expected to keep their systems secure because of the growing dependency of companies on e-commerce (Barsanti, 1995), growing need for IS to provides the backbone of organizational structure (Kankanhalli

et al., 2003), and increasing requirement for regulatory compliance in the wake of financial scandal (Abu-Mussa, 2004).

According to the ISS literature, there are two approaches that are used by information security managers to protect their system from security threat. The first and the most commonly used approach is the technical approach while the second one is the socio-organizational approach (Dhillon and Backhouse, 2001), which focuses on the use of social theory as their basic theoretical foundation to investigate ISS issues. Many organizations are trying to provide a technological solution for almost all security problems, but nowadays it becomes clear that using only technological solution is not enough to keep companies security (Slay, 2003). These days, it become clear that ISS cannot be achieved through only technological tools and effective organizational ISS depends on all three components: people, processes, and technology (Hamill et al., 2005). Even though the area of end user security behavior is gaining increasing attention, the human element remains to pose serious security threat. Since this is a new area, the knowledge of end user security behavior and factors affecting this behavior is at its early stage (Herath and Rao, 2009b). Many researchers advocate the use of deterrence mechanisms (see Figure 1.2) to lighten the noncompliance problem (D'Arcy et al., 2009; Kankanhalli et al., 2003; Straub, 1990).

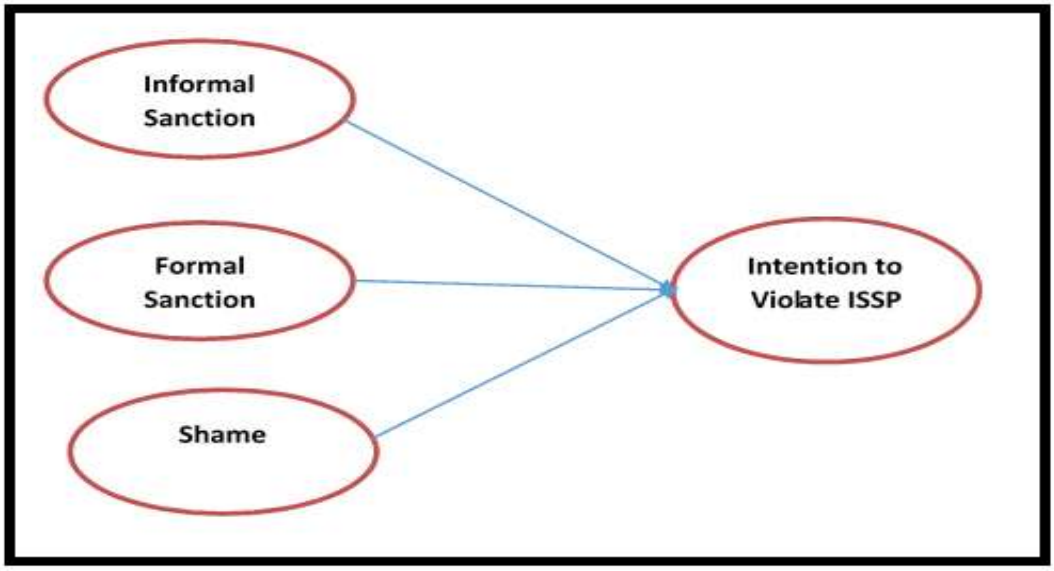

Figure 1.2: The General Deterrence Theory

(Source: Adapted from Siponen and Vance 2010, p. 489)

In the last few decades, research on GDT has undergone a number of extensions (Grasmick and Bursik, 1990; Piquero and Tibbetts, 1996). The main extension is made by the RCT (see Figure 1.3), a modern extension of classical GDT which introduces constructs, such as: perceived benefits, moral beliefs and also "non-legal costs", which are informal sanctions and shame. Informal sanctions refer to the disapproval of friends or peers for a given action (Paternoster and Simpson, 1996), while shame refers to a feeling of guilt or embarrassment if others knew one's socially undesirable actions (Eliason and Dodder 1999, as cited in Siponen and Vance, 2010).

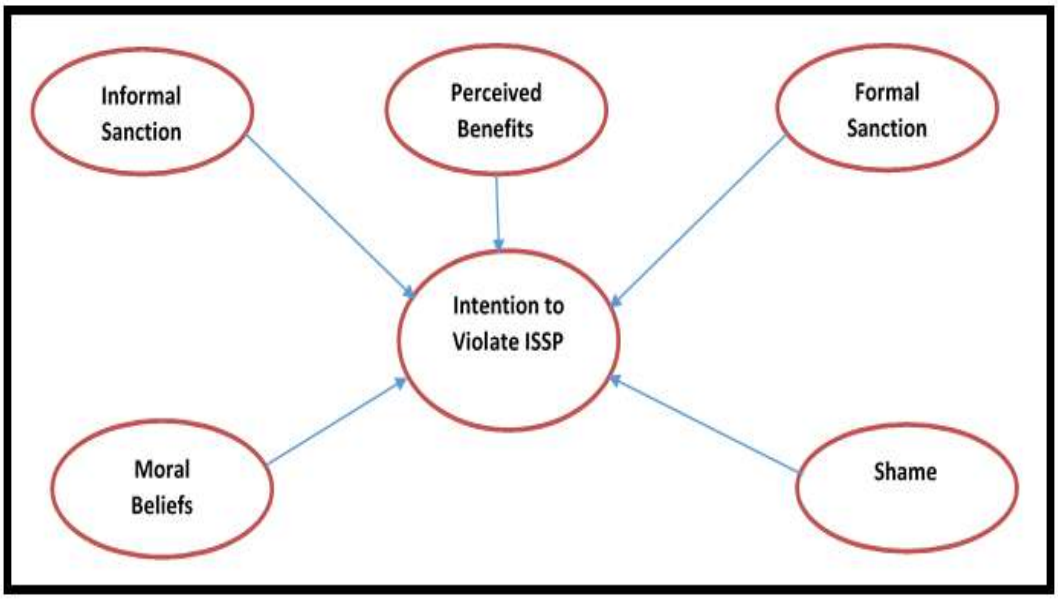

Figure 1.3: The Rational Choice Theory

(Source: Adapted from Siponen and Vance 2010, p. 80)

The GDT, which is rooted in classic criminology (Beccaria, 1963) assumes that human beings make decisions toward perpetrating or retreating from bad act or crime based on the maximization of their benefits and the minimization of costs. Classic GDT mainly focuses on formal sanctions and explains that the more people perceived certainty, severity, and celerity of sanctions for an inappropriate act, the more they are deterred from that activity (Gibbs, 1975). In this regards, Straub and Welke (1998) also highlight the contribution of deterrent countermeasures to reduce future computer abuse. But, when we look at various empirical studies that are conducted on the application of GDT, it is clear that their outputs are

inconclusive. Different researchers explain the cause of this inconsistency at different times in different ways. Some add variables that could better explain under what condition the countermeasures might work well (e.g. D'Arcy and Herath, 2011; Siponen et al., 2010; Harrington, 1996), such as computer self-efficacy (CSE). According to IS literature, CSE can take two forms: general and task-specific. The general CSE refers to an individual's overall confidence to make use of IT tools, and task-specific CSE refers to an individual's confidence with respect to specific IT related applications, such as using MS Excel or MS Word (Marakas et al., 2007).

A number of researchers have come to emphasize the importance of CSE as a factor to explain the behavior of IS users (Compeau and Higgins, 1995; Marakas et al., 2007). Even though there is an increasing criticism on the uses of the general level CSE, there are researchers (e.g. D'Arcy et al., 2011) who use this same concept in their studies. For example, Compeau and Higgins (1995) stated the importance of creating a specific association of CSE with specific domain of interest relating to computers. D'Arcy and Herath (2011) recommend measuring CSE and testing for its moderating influence in IS deterrence studies. They emphasize that domain-specific measures (e.g., self-efficacy toward ISS-related behaviors) are recommended over a general CSE. In this regards, a research by Phelps (2005) proposes a model for measuring information system security self-efficacy.

1.8. LIMITATION OF THE STUDY

The major limitations of this study are summarized as follows: The first limitation of this study is we don't use all the dimensions of Hofstede's (1980, 1984, and 2001) national culture, rather we only took four of them. Second, the respondents of our study are confined to organizations that do have established ISSP. Third, we don't measure the actual behavior of employees, rather we use intention as a proxy to actual behavior. The fourth limitation of this study arises due to the sensitive nature of the research topic, in this respect, respondents might not give their real feeling for questions that involves ethical issues. The last limitation of this study is the lack of generalizability of this study findings to countries outside Ethiopia due to the impact of national culture.

1.9. SCOPE OF THE STUDY

With respect to the cultural dimensions, the research focus on four of the Hofstede's (1980, 1984, and 2001) cultural dimensions, namely: power distance, uncertainty avoidance, collectivism/individualism and, masculine/feminine. From the RCT, we focus on formal sanctions, shame, perceived benefits, and moral beliefs.

According to Leidner and Kayworth (2006), we can study culture at different levels, including at the national, organizational, or subunit level. But, this research limits itself to the national level of culture. The choice of the national culture for this study is not random; rather, it is based on its considerable power in influencing employees' behavior. Robbins (2005) argues that national culture and organizational culture are highly related to employees' behavior and, more importantly, culture at the national level exerts considerably higher impact on employees' ISS behavior. Therefore, specific information about national culture of individuals plays a great role in predicting employees' ISS behavior in organizations.

1.10. ETHICAL CONSIDERATION

Appropriate acknowledgment and citation are made for any concepts or ideas taken from the literature. An attempt has also been made not to apply pressure or inducement of any kind to encourage an individual to become a subject of research. In addition, the identity of individuals from whom information is obtained in the course of the research project are kept strictly confidential. No information revealing the identity of any individual are included in this final report or in any other communication prepared in the course of the research project, unless the individual concerned has consented in writing to its inclusion beforehand.

CHAPTER 2

LITERATURE REVIEW

2.1. INTRODUCTION

In this study, we conducted a quantitative analysis to understand some of the determinant factors for employees ISSP violation. More specifically, we investigated the relationship between RCT constructs and employees' intention to violate ISSP and also the moderating influence of national culture in this relationship. Even though ISS has always been one of the important concerns for top level managers, the attention given to it shows a considerable difference over the years. For example, in 1981 it was ranked 14th, in 1985 it becomes 5th, while in 1989 it dropped to 19th (Loch et al., 1992). If we see a more recent figures, in 2003, it becomes 17th (Pimchangthong et al., 2003) and in 2013, 2014 and 2015 both large and small organization ranked concern about ensuring ISS protection as a top 5th, 2nd , and 5th risk issue respectively (Scott, 2015). The recent releases might be an indication of how ISS is getting increasing emphasis in both small and large organizations. In parallel to this, there is also an increasing attempt in the behavioral IS studies to investigate factors which contribute to ISSP compliance. Unfortunately, what we should remember here is that many researchers reported inconsistent and even sometimes contradictory results, concerning the impact of various factors on ISSP compliance (Sommestad, 2014). We believe that it is the job of IS researchers to find out the causes of these inconclusive outputs. In this regards, we contribute our own by investigating one of the decisive factors that is believed to contribute to the inconsistent findings.

In this chapter, we have conducted a detailed literature review of the following topics: ISS and insiders, ISSP compliance, studies in ISS compliance behavior, overview of antecedents/determinants of security compliance, RCT, national culture, national culture and ISS, research model and hypotheses.

2.2. INFORMATION SYSTEMS SECURITY AND INSIDERS

As discussed in the first chapter, our research mainly focuses on insiders and factors that play a role in their violation/compliance of ISSP. Hence, it is necessary to precisely define what insiders are and also what we mean by ISS violation. ISS violation is defined as any act by individuals using computer that is against the rule and policies of an organization (Hu et al., 2012). According to the author, by this definition, ISS violation includes but not limited to: unauthorized access to data and IS, unauthorized copying or transferring of secret data, selling confidential data for third party whether because of opportunism, greed, a desire for revenge, or a combination of these. Insider is defined as the organizational member who is a 'trusted agent' inside the firewall (Im and Baskerville, 2005; Stantton et al., 2005, as cited in Warkentin and Willison, 2009)

Even though the security of information intensive companies is of paramount importance (Herath and Rao, 2009b), these days, every company needs to give a great emphasis for ISS. Up to 90% of organizations face at least one ISS breach every year (Bagchi and Udo, 2003), and security breaches caused by employee noncompliance costs organizations millions of dollars (Herath and Rao, 2009b). While ISS researchers and practitioners mainly concentrate on fighting security breaches caused by external agents (Magklaras et al., 2006), most of the threats are originated from insiders (D'Arcy et al., 2007). Specifically, according to Warkentin and Willison (2009), while the media headlines mainly focus on magnificent threat caused by external hackers; insiders pose silent but more dangerous threat than outsiders. If we precisely look at the percentage of insider attack, between one-half and three-quarters of ISS breaches are caused by the legitimate users of organizational IS (Ernst and Young, 2003; Information Week, 2005). Another study also shows that half of intrusion and security violation occur from within the organization (Baker et al., 2010; Richardson, 2008). Not only the frequency of occurrence, but also there a lot of financial losses associated with the legitimate user actions (Magklaras et al., 2006). Since insiders do have better access to the companies secured information, they can bring catastrophic consequence to their company in terms of financial as well as non-financial aspects, such as: the reputation of the company, customers' confidence and many more (D'Arcy et al., 2007).

More recently, the cyber security watch survey (2012) annual report indicated that insider attacks increased from 41% in 2004 to 53% in 2011, while the 2014 report showed that in 2012 it remains at 53%, and in 2013 it showed some reduction (37%). In addition, according to a report by Verizon (2012), the security breaches caused by insiders increased on average from 33% (2004 -2007) to 48% (2009).

As can be understood from the IS literature (e.g. Magklaras et al., 2002; Theoharidou et al., 2005; Warkentin et al., 2009), the insider threat remains the greatest single risk to organizations, and with this respect, most security experts agree that more successful attacks come from inside the organization than from outside, and that insider attacks are potentially more costly (Schultz, 2002; Shaw et al., 1998). In the behavioral ISS literature and industry survey of IT managers, it becomes clear that the insiders are the main cause of security breaches in companies (Hu et al., 2012; Warkentin and Willison, 2009). The authors added that despite the existence of ample modern protective technologies, security procedures and ISSP, insiders still remain the greatest threat to organizational IS.

Another important point we need to take into account is the reported figures about the insider attacks. Because only a fraction of security incidents is actually discovered (Hoffer and Straub, 1989; Whitman, 2003), the figures from different reports and studies might be lower than the actual fact. For example, according to the Cyber Security Watch Survey (2014): "The public might not be aware of the number of insiders events or the level of the damage caused by them, because 70% of insider incidents are handled internally without legal action". According to a recent release of this same report in 2014, still the percentage is high (75%) in 2014 (Cyber Security Watch Survey, 2014). From our understanding of the extant literature, it is time to embark on behavioral ISS studies to combat the ever increasing security breaches caused by the insiders; otherwise more catastrophic events might come in the future. The internal incidents are here to stay and their mitigation should be a priority issue for IT professionals (Magklaras et al., 2006).

When we come to a recent international ISS issue, we can mention the whistle blower Edward Snowden. His action could be mentioned as a recent example of how much threat insiders might pose to their organization, and even to their country and the world as a whole. According to CISCO (2013), one of the hottest security related issues in 2013 is Snowden's disclosure of confidential information. According to the report, the former U.S. government contractor leaked secret information to a U.K. based newspaper. He obtained the information while he was working on assignment for the U.S. National Security Agency (NSA). These and other disclosure by Snowden about government surveillance practices raise a critical security concern at different levels, such as: between private citizens and organizations in the public and private sector (CISCO, 2013).

When we come to the Ethiopian case, due to lack of studies in the areas of ISS breaches, it is difficult to know the actual figure with respect to the financial losses of the incidents. But, in the first chapter, we reviewed some important examples that can somewhat show how the ISS environment looks in Ethiopia.

In response to the security breach problem, a number of studies are done in different disciplines. When we analyze these studies, we can note the difference in the way how they are prepared to tackle the ISS problem. Some disciplines focus on technical solutions while others focus on socio-organizational issues. If we take studies that are conducted in the area of engineering and computer science, most of them focus on the question "how to protect the IS from external threat?" and in response to this question, they develop many techniques like intrusion detection systems, firewall, anti-malware software, and many more (Warkentin and Willison, 2009). But when we come to the MIS researchers, unlike the computer scientist, their targets are insiders and their main focus is to give solutions that are related to behavioral issues. Researchers like Warkentin and Willison (2009) indicated the existence of a significant effort in the MIS discipline to investigate the human element that is within the company, as a critical perpetrator of companies IS.

Even though the literature shows us the increasing numbers of behavioral ISS studies, still much more effort is expected from researchers to know more about insiders' ISS behavior. Since this is a new area, the knowledge of end users' security behavior and factors affecting this behavior is at its embryonic stage (Herath and Rao, 2009b). Still another research by Zafar and Clark (2009) stated that even though the impact of security related problems are well understood by organizations, IS research in this area is still in its infant stage. Thus, our research contribute its part in alleviating the insider compliance problem by considering one of the very important factors that is believed to shape human behavior: national culture.

2.3. INFORMATION SYSTEMS SECURITY POLICY COMPLIANCE

Nowadays, organizations are highly dependent on IS to get their job done, and hence they are expected to manage the risk associated with their day to day use of systems. Unless they properly manage the risks, they will find themselves in a very frustrating situations like corporate liability, loss of image in the eyes of its customers, and financial losses (Cavusoglu et al., 2004). Due to this fact, many organizations give considerable emphasis for protecting their systems from security breaches and, more importantly, it became one of their main agendas (Ransbotham and Mitra, 2009).

Despite the attention given for security related problems, many organizations around the world are increasingly suffering the consequence of ISS breaches (Alghazzawi et al., 2014). Different studies (e.g. Lee and Lee, 2002; Willison, 2006) indicated that more than 90% of organizations face at least one serious ISS breach every year. More than half of the total ISS breaches are caused by insiders (Warkentin and Willison, 2009; Whitman and Mattord, 2008). More specifically, between one-half and three-quarters of all security incidents originate from within the organization (Ernst and Young, 2003; Information Week, 2005). Because only a fraction of security incidents is actually discovered (Hoffer and Straub, 1989; Whitman, 2003), the figures from different reports and studies might be lower than the actual fact.

To better manage the security noncompliance problem, organizations around the world develop and communicate different types of ISSP (Sommestad et al., 2014). These security

policies are constituted from different types of principles, rules, intentions, and guidelines which the organization expects the employee to obey (Sommestad et al, 2014). Even though organizations are investing huge amount of money to bring and implement these ISSP, the ISS breaches caused by insiders are on the rise (Foster, 2006, as cited in Li et al., 2010) and consequently, Young and Case (2004) reported that the majority of organizations comes to conclude that their company ISSP are ineffective. In this respect, some studies (Ernst and Young, 2008; Puhakainen, 2006) point out that no matter how the ISS practice or technique is best, it can only be successful if properly implemented by users.

The ISS literature indicates that noncompliance is a major challenge and we do believe that coming up with the mitigation mechanism should be the priority agendas of ISS researchers. From our analysis of the ISS compliance literature, we understand that there exist diverse types of research works that attempts to tackle this problem. Below, we summarized these prior studies in an effort to understand how researchers tried to address the computer abuse/noncompliance issue and also what are some of the limitations of these studies.

2.4. STUDIES IN INFORMATION SYSTEMS SECURITY COMPLIANCE BEHAVIOR

Prior studies in the area of ISS behavior has focused mainly on two outcomes or dependent variables, namely: (1) Computer abuse, (2) ISSP violations. Below is the detailed discussion of these variables.

2.4.1. Computer Abuse

The term computer abuse is first used by Parker (1976) in his research "Crime by Computer", since then many researchers all over the world start using the term. Computer abuse, according to Harrington (1996) is defined as activities like cracking/hacking, computer fraud, virus, and corporate crime using a computer. Starting from early 1990's, various theories have been used to examine and explain computer abuse by individuals, for example GDT (Straub, 1990), Protection Motivation Theory (PMT) (Siponen et al., 2006), and Agency Theory (Herath and

Rao, 2009b) are among the most commonly used theories. But from the above mentioned theories, GDT is considered by most as widely used theory (D'Arcy and Herath, 2011). The classical GDT focuses only on formal sanctions and it states that as sanctions become severe, certain and swift individuals will be deterred from engaging in a rule breaking activity (Gibs, 1975). Later, the theory inculcates informal sanction (social-disapproval), shame (self-disapproval), and moral inhabitation (Piquero and Tibbetts, 1996).

Despite its strong theoretical foundation, the GDT receives a mixed support in the ISS sytudies. According to D'Arcy and Herath (2011) there exist uneven and often contradictory findings on the impact of sanctions on reducing ISS violation. When we review deterrence based studies, the work of Straub (1990) is at the forefront of the literature, and in his study deterrence countermeasures are found to have a high impact on reducing IS abuse level. In addition to this, many researchers (Tudor, 2000; Kankanhalli, 2003; Herath and Rao, 2009a) reported that deterrent measures improve the security level and reduce computer abuse. But this is not the whole story, because a considerable number of studies (Li et al., 2010; Siponen and Vance, 2010; Pahnila et al., 2007; Siponen et al., 2007; Lee et al., 2004) reported the inability of, at least, some of the constructs of GDT to reduce IS abuse. The above studies could be used as a witness to the existence of inconclusive output around GDT, and we do believe that researchers in the ISS field should work hard to quite or at least reduce this noise.

According to Boudreau and Robey (1996), if there exist contradictory findings over a single issue in a discipline, researchers might follow three strategies to deal with it. According to the authors, the first strategy is identifying contingent variables, while the second one is analyzing methodological concerns, and the last but not least is making an appropriate review of substantive research questions. Following this same strategy D'Arcy and Herath (2011), collected and analyzed almost all IS deterrence studies for the period 1990-2011 and come up with very important recommendations that future researchers in the discipline should focus on. According to the authors, one of the main shortcomings of prior studies is a methodological issue, different researchers use sample from different countries/culture, and hence the difference in the result of their research might be explained by the difference in the people's culture. While the other important point they raised is the impact of contingency

variables, one of which is CSE and it is discussed in the upcoming section. Table 2.1 shows theory based empirical researches in the area of ISS compliance and the main gap left by these studies.

Table 2.1: Theory-based empirical studies in individual security policy compliance and the gap identified

No table of figures entries found.	Theories used	Research focus	Potential research gap or opportunities
Chan et al. (2005)	Organizational climate	Impact of organizational information security climate on employee's compliance behavior	Limited theory-based empirical studies; inconsistent results regarding the impact of sanctions or countermeasures; Some of the fundamental set of constructs (such as perceived benefits of deviant behaviors, shame, and moral beliefs) have been overlooked by majority of the theories; None of the studies consider the impact of national culture on individuals' security behavior (methodological issue).
D'Arcy and Hovav (2012), Herath and Rao (2009b)	General deterrence theory, Agency theory	Impact of intrinsic and extrinsic motivations on employee's policy compliance intention; penalty/sanction is considered an extrinsic motivation; sanction supported	
Herath and Rao (2009a)	General deterrence theory, Protection motivation theory	The impact of protection motivation, deterrence, and organization commitment on employee's policy compliance intention	
Pahnila et al. (2007)	General deterrence theory, Protection motivation theory	The impact of positive enforcement and negative enforcement on employee's compliance intention and behavior; sanction, coping appraisal, and threat appraisal are considered negative enforcement; sanction not supported	
Siponen et al. (2006)	Protection motivation theory	The impact of coping appraisal and threat appraisal on employee's compliance intention and behavior	
Bulgurcu et al. (2010)	Theory of Planned Behavior, Rational choice theory	Identifies the antecedents of employee compliance with the information security policy (ISP) of an organization	
Li et al. (2010) Vance, and Siponen (2012)	Rational choice theory	Apply rational choice theory to Internet abuses in the workplace and employees intentional violation of organizational information security policies	
Lowry and Moody (2015)	control-reactance compliance model (CRCM)	Understanding of both motivations to comply with new ISPs and motivations to react negatively against them	

2.4.2. Information Systems Security Policy Violation

The other main stream of ISS studies is ISSP violation. Since ISS is a very big concern for today's organizations, many companies invest huge amount of money to come up with a suitable and effective mechanism that is believed to be the safeguard of their IS. In this respect, one of the commonly known security mechanism is to implement ISSP which contains rules, regulation, guidelines, intentions, and principles (Sommestad et al., 2013). In this regards, ISSP clearly states, what are the measures to be taken against different kinds of violations, and also what is acceptable use of IS resources (ISO/IEC, 2009).

Despite the existence of the security policies, protecting the IS become a moving target for most organizations around the world (Sommestad et al., 2013). To tackle the noncompliance problem, various studies have been conducted, for example: Siponen et al. (2006), Pahnila et al. (2007), Herath and Rao (2009a, 2009b), Chan et al. (2005), Bulgurcu et al. (2010), Young (2010), and Siponen and Vance (2010). The majority of the studies uses PMT and/or GDT, while some uses other theories like agency theory and GDT together (Herath and Rao, 2009b), organizational theory (Chan et al., 2005), health belief model (Kumar et al., 2009).

In general, many of these studies with the exception of few (Vance and Siponen, 2012; Li et al., 2010; Bulgrucu et al., 2010 (only on costs/benefits of compliance and costs of noncompliance, but not benefit of noncompliance)) focus on fear based mechanisms, such as cost of sanction, while they ignore the impact of perceived benefits of noncompliance and moral beliefs. Even in those studies that includes perceived benefits (e.g. Li et al., 2010), their output could not be generalized to a broad level of ISSP compliance, because it only covers a special form of security policy, internet use policy only. In this regards, Vance and Siponen (2012) point out the need for the inclusion of various types of security policy violations so that the output can be generalizable across various IS policy violation. The other study that uses perceive benefits is the work of Vance and Siponen (2012), and they recommend future studies on perceived benefits and moral beliefs in various cultural setup.

Most importantly, none of the current studies in the ISS literature investigate the impact of culture on perceived benefits and moral beliefs. Thus, our research work is the first to shed light on these issues.

2.5. OVERVIEW OF ANTECEDENTS/DETERMINANTS OF SECURITY COMPLIANCE

In the area of ISS, the literature indicates the ever increasing number of behavioral ISS studies on various areas, such as: how to protect IS from insiders attack or abuse (Siponen and Willison, 2009; Willison, 2006; Willison and Backhouse, 2006). As discussed in the above sections, to combat the ISS problems, different researchers use different perspective and theories in their study. Some uses GDT to investigate the impact of individual's behavior on computer abuse and crime (e.g. Straub and Nance, 1990; Straub and Welke, 1998; Straub, 1990). On the other hand, others use PMT to find out the relationship between individuals and ISS related issues, in this respect, Johnston and Warkentin (2010) conducted a research on the use of anti-malware software, while Herath and Rao (2009b), and Ifinedo (2009) focused on users' compliance with ISSP. Moreover, a study by Lee (2011) focuses on adoption of anti-plagiarism software.

In addition to these theories, researchers examine the relationship between different variables that are believed to have impact in ISSP compliance. Thus, some researchers use variables like computer security self-efficacy, users' security awareness, and more importantly, culture to investigate the contribution of these factors in individual ISSP compliance. In the following sections, we conducted a detailed review of some of the determinants of security policy compliance, namely: computer security self-efficacy, users' security awareness, and culture respectively

2.5.1 Computer Security Self-Efficacy

Computer security self-efficacy (CSSE), is defined as individuals' judgment of their own skills, knowledge, or competency to efficiently follow ISSP (Phelps, 2005). As indicated in

earlier sections, according to the extensive literature review made by D'Arcy and Herath (2011), one of the contingent variables which might contribute to the inconsistent findings around the impact of countermeasures is CSE.

According to the IS literature, CSE can take two forms: general and task-specific. The general CSE refers to an individuals' confidence in their ability to use IT tools, while task-specific CSE refers to individuals' confidence in using specific IS applications, such as using MS Excel (Marakas et al., 2007)

Many researchers have come to emphasize the importance of CSE as a significant factor to explain the behavior of IS users (Compeau and Higgins, 1995; Marakas et al., 2007). Even though there is an increasing criticism on the uses of the general level CSE, there are many researchers (e.g. D'Arcy and Hovav, 2009; D'Arcy et al., 2011; Son, 2011) who use this same concept in their studies. Even vigorously validated measures of CSE, when applied to unrelated studies, will have limited generalizability (Marakas et al., 2007). In this respect, Compeau and Higgins (1995) discussed the importance of creating a specific association of CSE with specific domain of interest relating to computers. Even though there are emerging attempts to examine the CSE in different domains (e.g. Database CSE, internet CSE, Word processing CSE and ethical CSE), little attention have been given for security related CSE measures (Clarke, 2011). In addition to this, D'Arcy and Herath (2011) recommend measuring CSE, and testing for its moderating influence in IS deterrence studies. They emphasize that, domain-specific measures (e.g., self-efficacy toward IS security-related behaviors) are recommended over a general CSE. In this regard, a research by Phelps (2005), proposes a model for measuring ISS self-efficacy. The above discussion implies that ISS compliance is one of those areas that needs a close examination of its association with a specialized security related CSE.

When we come to the exact relationship between ISSP compliance and self-efficacy, within the deterrence literature, there exists some evidence on the lesser influence of formal sanctions for individuals' with a higher level of skills and abilities related to criminal activities (Tittle, 1980; Pogarsky et al., 2004). Several risks taking activities like gambling among university students are highly influenced by perceived self-efficacy (Wyatt, 1990). This means, people

in most cases engage in risky activities when they feel competent in that area. In this respect, according to Workman and Gathegi (2007), when people believe that they have a very limited skill and capacity to control an outcome, then they are more receptive to external forces like threat of punishment. Given the fact that security violation is a risky activity, we might say that people with a higher level of CSE have a lower perception of threats pertaining to a security violation. Specifically, D'Arcy and Hovav (2009) reported the negative impact of CSE on compliance. Individuals with high CSE will perceive less certainty and severity of sanctions in response to deterrent security countermeasures, and hence they might be motivated to engage in IS misuse activities more than those individuals with low CSE (D'Arcy and Hovav, 2004). This idea is also strengthened by other criminological researchers, such as: Jacobs (2010), and Krueger and Dickson (1994), according to them, people with high self-efficacy leads them to believe that they can escape formal sanctions.

On the other hand, a study by Bulgurcu et al. (2010) reported that an employee's self-efficacy about compliance positively influences intention to comply. In addition to this, Kirsch and Boss (2007) reported the positive and significant influence of CSE on mandatory security compliance and in this regards, they advise companies to continually give training to their staffs on how to use a computer. The authors stated that as employees feel more confident in using the computer to execute their duties, they will be more likely to protect company IT resources. Still another study reported that employees' CSE is positively associated with the employee's compliance with ISSP (Son, 2011), the author justified the finding by saying that at least some level of CSE is a must to implement security related issues, such as: regularly scanning and updating anti-virus software.

In addition to this, the literature clearly indicates that gender does have an impact on how people interact with computer systems. Specifically, males are easily gravitated towards computer than females, providing them a higher chance to generate a higher CSE (Phelps, 2005). Many empirical studies found out that males score higher than females in CSE (Arch and Cummins, 1989; Busch, 1995; Karsten and Roth, 1998; Miller, 1996; Whitley, 1997 as cited in Phelps, 2005). Since our main focus is on the relationship between culture and RCT

constructs, we did not address the issues of CSE and gender; rather we encourage researchers to deal with this issue.

2.5.2. Users' Information Systems Security Awareness

The other important determinant of ISSP compliance is users' ISS awareness. Users' ISS awareness program is a kind of training and education program that mainly emphasis on the continuous rising of individuals' awareness around computer security responsibilities and more importantly, it reminds specific actions will be taken if one misuse the company IS (Straub and Welke, 1998). In this area, there exist many conceptual and empirical studies (Bulgurcu et al., 2010; D'Arcy et al., 2007; Punhakainen, 2006; Hentea, 2005; Whitman, 2004; Furnell et al., 2002; Lee and Lee, 2002; Siponen (2000, 2001); Whitman et al., 2001; Dhillon, 1999; Park, 1998; Wybo and Straub, 1989) that investigated the influence of users' security awareness on IS misuse. Almost all of these studies indicate the important contribution of users' security awareness to reduce IS misuse. Sommestad et al. (2014) conducted a systemic review of 29 empirical IS compliance/misuse studies. In their review, the impact of user awareness varies from study to study but, on average, security awareness is classified to be the best predictor of ISS compliance and misuse. Some of the studies in security awareness (Bulgurcu et al., 2010; Furnell et al., 2002; Siponen (2000, 2001); Whitman et al., 2001) suggest mechanisms through which companies can motivate their employees to accept and implement security policies. While some (Punhakainen, 2006; Lee and Lee, 2002; Siponen, 2000) propose different types of conceptual and theoretical models that might help in increasing the successfulness of security awareness programs. Even though all of the above studies do not examine the exact impact of users' security awareness across different cultures, we conclude from the literature that almost all researchers agree on the contribution of users' awareness to security compliance.

2.5.3. National Culture

When we come to the third determinant of ISSP compliance, we find national culture. According to Hofstede (1980) it is defined as the collective programming of the human mind that distinguish individuals in a group from individuals in other groups. Leidner and Kayworth (2006) reviewed 82 articles that conduct studies around IT and Culture in the period 1990-2006 and we also added additional literature review to inculcate more recent papers. When we analyze these studies, there are very few researchers that try to evaluate the impact of culture in security related behaviors.

In this regards some studies (Alfawaz et al., 2010; Ernest and Lin, 2007; Hu et al., 2012; Parsons et al., 2013) investigated the effect of organizational culture on security related issues, and their result shows the substantial influence of organizational culture. On the other hand, very few of the studies tried to relate national culture to ISS issues, such as: security management concerns (Ifinedo, 2009), ISS noncompliance (Dols and Silvius, 2010), level of software piracy (Husted, 2000), privacy concern (Milberg et al., 1995; Einings and Lee, 1997), and intellectual property rights (Shore et al., 2001). The output of these cultural based studies shows the considerable effects of national culture on ISS related concerns. But, to the best of our knowledge, there exists no research work that tries to investigate the moderating impact of national culture on the relationship between RCT constructs and ISSP violation. Thus, our research focus is to investigate the moderating influence of national culture.

Summary

Generally, in our literature review, we come to highlight the impact of different variables on ISSP compliance and, more importantly, we show the current gaps in the security compliance literature as well as the gaps we select to focus on. According to our review, the most important limitation of the majority of ISS studies is using fear based mechanisms as the only antecedent of security compliance, while they ignore very decisive variables, such as: perceived benefits, and moral beliefs.

As can be understood from the ISS literature, organizations are increasingly suffering the consequence of ISS breaches caused by their own employees. Even though IS scholars increasing shift their attention to the behavioral security issues, very few empirical studies investigate the ISSP compliance topic (e.g. Chan et al., 2005, Herath and Rao, 2009 a, b; Siponen and Vance, 2012). If we take a few of those studies that focus on security compliance, we can understand that many of them do have some limitation in inculcating important constructs into their research model. For instance, researchers like Herath and Rao (2009 a, b), Pahnila et al. (2007), Siponen et al. (2006), uses either GDT or/and PMT to explain individual's compliance with ISSP. This might be an indication of how prior studies, in most cases, address the employee ISSP compliance problem: focus on fear based strategies.

According to the RCT, individual's violation of organizational policies is not only explained by fear of sanctions, but people always consider perceived benefits and moral evaluations to commit security violation. On the other hand, in many other disciplines (e.g. Politics, labor markets, formal organizations, and criminology), they realized the influential power of RCT, and it is now spreading across their studies. (Hechter and Kanazawa, 1997). One of the most plausible reasons as to "why many studies use the RCT?" is due to its parsimonious and elegant explanation (McCarthy, 2002). When we come to the ISSP compliance, it is very recently (around 2010) that researchers try to use this theory to explain the compliance issue (Vance and Siponen, 2012). Even these recent studies do not investigate the RCT in a cross cultural setup. Thus, in our research, we use the RCT together with the culture theory to fill the gap left by previous studies. In addition to this, despite the existence of proof on the considerable influence of culture on the interaction between people and IT, many of the current studies in the ISS area assume the impact of different variables/countermeasures to be uniform across cultures. Consequently, this might create opportunity for future researchers to embark on this issue. If we see some of prior studies (see Table 2.2) around computer misuse or systems security, none of them investigate the impact of culture as a moderating variable for ISSP compliance/noncompliance. But we can find some, on other security related areas like intellectual property right (Shore et al., 2001), software piracy (Husted, 2000), and privacy (Milberg et al., 1995).

Table 2.2: Some Prior Studies on Information Systems Security Misuse/Compliance

Theory	Constructs	Studies
GDT	-Formal Sanctions -Informal Sanctions -Shame	Straub, 1990;Tudor, 2000; Kankanhalli, 2003; Herath and Rao, 2009a; Siponen et al.,2007; Harrington, 1996; Siponen and Vance, 2010; Pahnila et al., 2007
RCT	-Perceived Benefits _Moral Beliefs	Siponen and Vance, 2012; Bulgrucu et al., 2010
Others	-Culture	Eining and Lee, 1997; Husted, 2000; Kettinger et al., 1995; Shore et al., 2001, Milberg et al., 1995
	-Security Awareness	Bulgurcu et al., 2010; D'Arcy et al., 2008; Punhakainen, 2006; Hentea, 2005; Whitman, 2004; Furnell et al., 2002; Lee and Lee, 2002; Siponen (2000, 2001); Whitman et al., 2001; Dhillon, 1999; Park, 1998; Wybo and Straub, 1989
	-CSE	Phelps, 2005; D'Arcy et al., 2011; Son, 2011

Since it is not possible to study every gap discussed above, our research scope is limited to the investigation of the basic relationship between RCT constructs and employees intention to violate ISSP. In addition to this, we also investigated the moderating impact of national culture in the specified relationship. Thus, to deal with the above research gaps, we formulate the following research questions.

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

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

To answer these research questions we proposed the following high level model (see Figure 2.1).

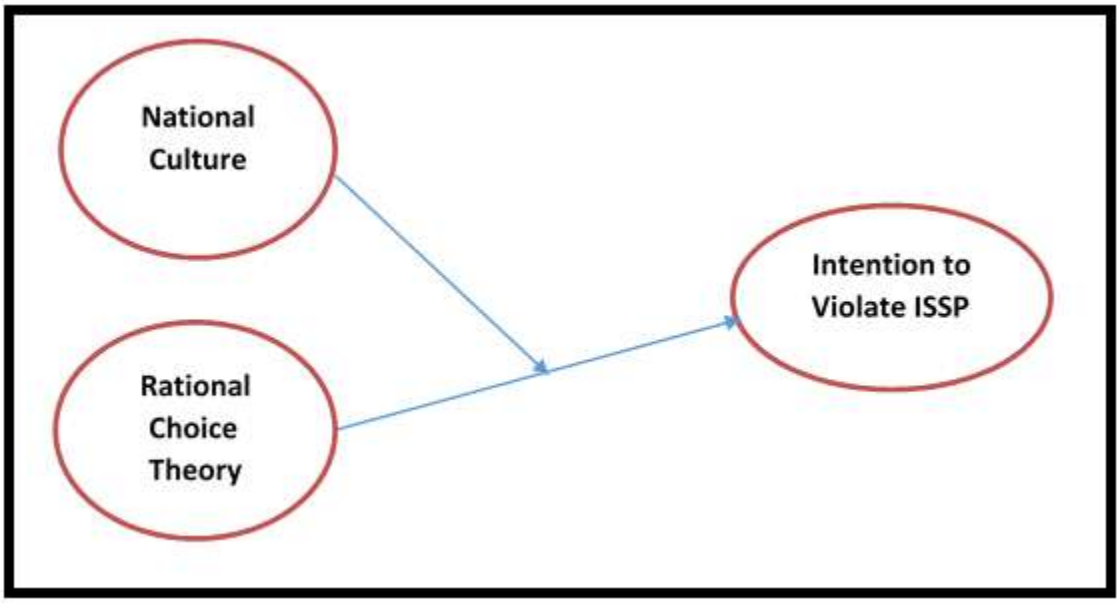

Figure 2.1: High Level Conceptual Model

2.6. RATIONAL CHOICE THEORY

To study employee ISS behavior, a number of theories have been used over the years. In this regards, theories such as: PMT (e.g. Pahnila et al., 2007, Siponen et al., 2006; Workman et al., 2008), GDT (Kankanhalli et al., 2003; D'Arcy and Hovav, 2007; D'Arcy et al., 2007; Straub, 1990), and agency theory (Herath and Rao, 2009b) have been used as a theoretical lens to study ISS compliance. According to Li et al. (2010) the majority of the studies in the ISSP 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. According to the authors, this will give only a partial explanation to the problem of ISSP violation.

Thus, in order to have a full view on "why employees violate ISSP?" we need to use theories that go beyond this horizon. In this regard, RCT goes beyond this limitation and includes perceived benefits of noncompliance and moral beliefs as additional determinants of ISSP compliance. The theory clearly states that individuals will always go through a utilitarian calculation of these and other factors when they make decision toward obeying or violate rules

(Vance and Siponen, 2012). Therefore, we believe that the use of RCT as one of our theoretical lenses is justified and also appropriate.

The RCT was first introduced by Becker (1968), and the driving assumption behind this theory is that people make decision that helps them to achieve their objective and maximize their utility. The theory has got five constructs (see Figure 2.2), namely: formal sanction, informal sanction, shame, perceived benefits, and moral beliefs. This theory has been used in different areas including ISSP compliance (e.g. Bulgurcu et al., 2010, Li et al., 2010; Vance and Siponen, 2012) to explain human security behavior. According to Paternoster and Simpson (1996), the theory has two main assumptions: the first one is, people who violate rules try to balance the cost and benefit of their act, and then choose the one with the best outcome, while the second assumption is, people's choice is all about how they perceive the cost and reward associated with their actions. Studies in different disciplines clearly show that RCT is well suited to explain white collar crime than a street level crime (Cao, 2004) and thus, it will be valuable to use this theory to better explain employees' ISSP compliance behavior. Researchers in many disciplines (e.g. Politics, labor markets, formal organizations, and criminology) realized the influential power of RCT and use this theory to investigate many social issues in their field. But there are limited works in the ISSP compliance area.

In this regard, we can mention some works (e.g. Bulgurcu et al., 2010; Li et al., 2010; Siponen and Vance, 2012) that go beyond the norm and inculcate some more constructs of the RCT like perceived benefits and moral beliefs into their empirical studies. When we analyze their contribution to the IS world, mainly they introduced the RCT theory to the ISSP compliance area, and that is an outstanding contribution. On the other hand, they are not free from limitation, for example, all of the studies mentioned above use sample from western culture and the result of their research might not be valid for other cultures and hence, this limitation/gap needs to be narrowed down. According to D'Arcy et al. (2007) given the difference in terms of cultural dimensions it is very important to bear in mind that users from different culture might respond differently to the same types of countermeasures. In addition to this, Dinev et al. (2009) reported that national culture dimensions moderate the relationship

between protective technologies with compliance, and they advise the inclusion of national culture when designing ISSP, practice and technology.

The other major theory we used in this study is national culture. Culture theory has been widely used to explain a variety of social phenomena in organizational settings (Keesing, 1974; Tushman et al., 1988). Hence, in the next section, we discussed this theory in detail.

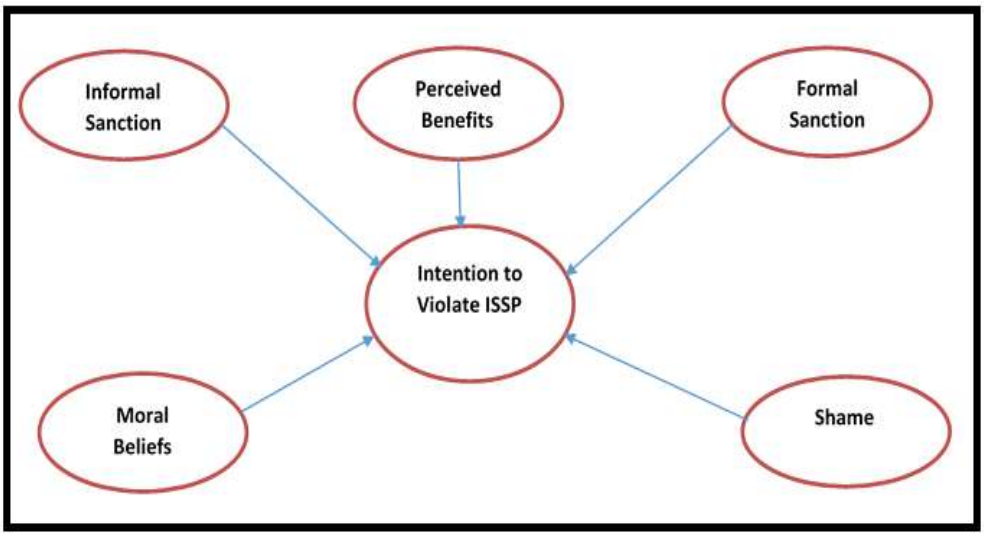

Figure: 2. 2: The Rational Choice Theory of ISSP Violation

(Source: Adapted from Siponen and Vance 2010, p. 80)

From the five constructs of the RCT, we focused on four of them, namely: moral beliefs, shame, formal sanctions, and perceived benefits.

2.7. NATIONAL CULTURE

Culture has been defined by scholars at different times. For example, the Anthropologist Geertz (1973) defines culture as a representation of the fabrics of meaning by which the society view its environment. While according to Hofsted (1980, 1984), culture is defined as a collective programming of mind that distinguish people in one group from others people in other groups. It can be studied at different levels, including subunit level, organizational level and national level (Leidner and Kayworth, 2006). In this respect, our main focus is the national

level culture and we used the Hofstede (1980, 1984, and 2001) model of national culture dimensions. The reason to choose Hofstede's dimensions is, because it has been rigorously validated in previous cross-cultural studies over time and in many countries (Sondergaard, 1994).

Around 1980's Hofstede come up with four national culture dimensions, namely: power distance, uncertainty avoidance, masculine/feminine, and collectivism/individualism (Hofstede, 2011). Later a new dimension called long/short term orientation was added based on a research by Canadian psychologist called Bond (Hofstede and Bond, 1988). The dimensions identifies core values that describe similarities and difference among cultures around the world. According to Hofstede (2011) many countries around the world have their own score for each of the national culture dimensions. Figure 2.3 shows the comparison between the Hofstede's scores and the scores based on the result of the quantitative survey used in this study. As can be seen from the Figure there exists some difference between the Hofstede's (1980, 1984, and 2001) scores and the current national cultural values of Ethiopian as measured by our main survey.

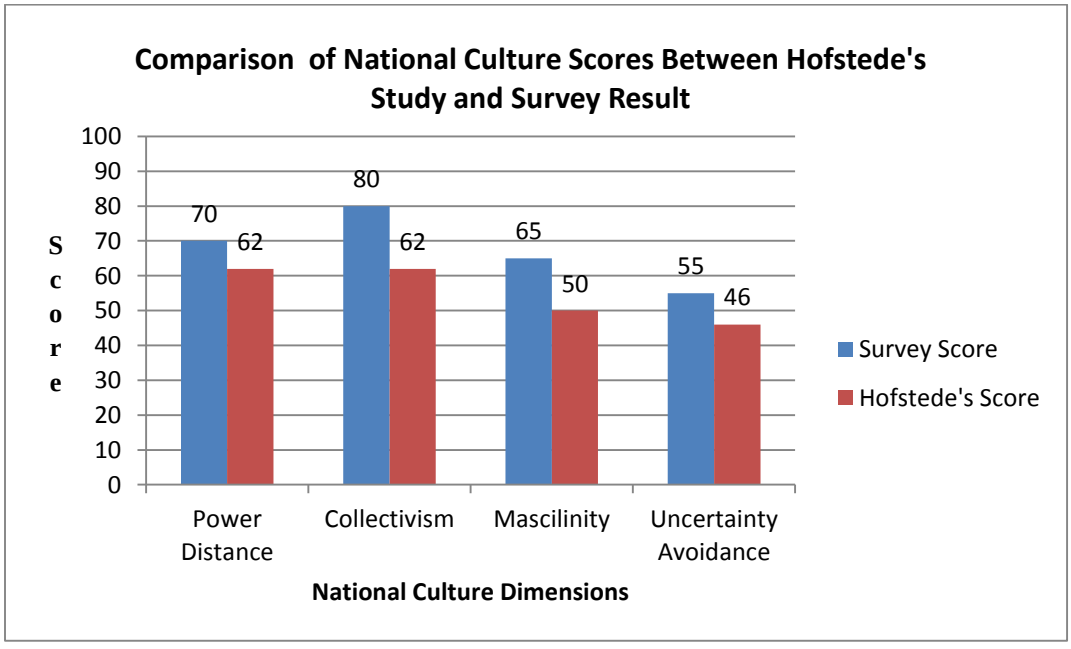

Figure 2.3: The Ethiopian Cultural Dimensions

2.8. NATIONAL CULTURE AND INFORMATION SYSTEMS SECURITY

Many scholars (e.g. Dhillon and Backhouse, 2001; Straub and Welke, 1998; Siponen, 2005) reported that the increasing number of security breaches in organizations is mainly attributed to the lack of focus for non-technical issues. Non-technical issues include: organizational policies, procedures, practices, and strategies that are enforced by organizations to create a more secure environment (Siponen, 2005; McPhee, 2008; Schatz, 2008). Even the existence of these policies and procedures could not be transformed into a secured environment by themselves, and in this respect, what is important is giving the required level of emphasis for the peoples who are expected to follow the policies and procedures. Some studies (Ernst and Young, 2008; Puhakainen, 2006) point out that no matter how the ISS practice or technique is best, it can only be successful if properly implemented by users.

Since end users or generally people do have their own culture, we need to understand some of the cultural values and their implication for the successful implementation of policies or practices. This is because, national culture dimensions are recognized to have influence in the implementation of different types of practices, which are exported from one part of the world to the other (Ifinedo, 2009). For example, Hofstede (2001) reported that management by objective (MBO) has a success story in countries with low power distance, but when it comes to countries with high power distance, it fails to be successful. This might be a very good indication of "the level of attention we should give to national culture values when we bring new technologies, practices and procedures from abroad". Consequently, the culture theory has been commonly used to explain a variety of social issues in an organization setting (Gordon, 1985; Hussain, 1998; Xie et al., 1998, as cited in Leidner and Kayworth, 2006). More specifically, there exist some studies that investigate the relationship between national culture and IT. In this regards, we can mention the work on IS development (Tan et al., 2003; Walsham, 2002), IT adoption and diffusion (Vreede et al., 1998; Hasan and Dista, 1999; Hussain, 1998), IT management and strategy (Burn et al., 1993; Husted, 2000; Shore et al., 2001), IT use and outcome (Choe, 2004; Chow et al., 2000; Johns et al., 2002). Almost all of

the above studies found a very interesting relationship between IT related issues and cultural values.

When we come to ISS related studies, there exist some studies that investigate how the two are related. In this respect, Eining and Lee (1997) examined attitudes of Chinese and US students on how they handle IT related ethical dilemmas, and their result suggests that Chinese students give more emphasis for friendship than rules when they face with IT related ethical dilemmas. While Husted (2000) reported the significant influence of individualism cultural dimensions on reducing software piracy rate. Moreover, Kettinger et al. (1995) examined privacy concerns in 30 countries and they reported the existence of considerable differences in privacy concerns across the countries. In addition to this, Shore et al. (2001) conducted a cross cultural study on attitudes towards intellectual property right, and their output showed that culture plays a big role in influencing people's attitude towards intellectual property right. But, when we come to the impact of national culture in ISSP noncompliance/compliance, there exist hardly any research at this level, which tries to explore their relationship.

2.9. RESEARCH MODEL AND HYPOTHESES

In order to investigate ISSP violation, we develop a model based on RCT and national culture theory. Specifically, from RCT we include formal sanctions, perceived benefits, moral beliefs, and shame. In addition to this, our model also inculcates four of the national culture dimensions, namely: power distance, collectivism/individualism, masculine/feminine, and uncertainty avoidance. The research model is shown in Figure 2.4 and each of the elements of the model and their corresponding hypotheses are discussed below.

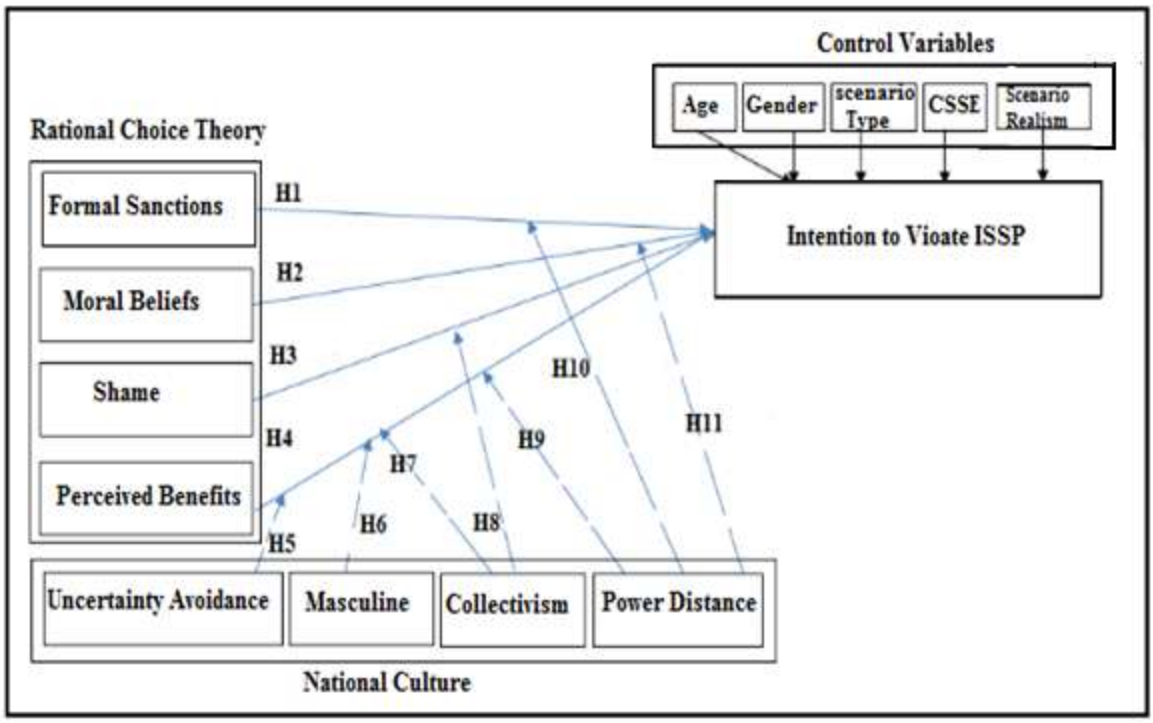

Figure 2.4: The Research Model

Formal Sanctions

When we come to the formal sanction, a research conducted by Straub (1990) reports that formal sanctions are found to have a high impact on reducing IS abuse; he include 1,211 organizations as part of the research. Some researchers like (Tudor, 2000; Kankanhalli, 2003; Herath and Rao, 2009a; Siponen et al., 2007) tried to investigate whether the use of sanction reduce IS security problems or not, and found out 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 employees' intention to violate companies ISSP. In addition to this, certainty of detection is found to have a significant impact while severity of punishment is found to have a negative impact on security behavior intention (Herath and Rao, 2009a).

Following the above discussion, we formulate the following hypothesis:

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

Moral Beliefs

RCT is not only about the cost and benefit aspect of a decision, but it has also a very important and integral construct, moral beliefs. In this research, moral beliefs refer to an individual's judgment about engaging in ISSP violation as morally wrong or right. If a person has a strong moral belief, then he/she consider a rule breaking as morally wrong, and according to Bachman et al. (1992), sanctions for such type of people are even irrelevant. On the other hand, if a person has weak moral beliefs, then rule breaking is not morally wrong for him/her, and according to Bachman et al. (1992), the influence of sanction would be considerable for such people.

Criminological studies show that moral beliefs or personal norms explain individuals intention to engage in a deviant behavior like corporate crime (Paternoster and Simpson, 1996), tax evasion (Wenzel, 2004), and also in sexual abuse (Bachman et al., 1992). On the other hand, studies in the area of Psychology (e.g. Blasi, 1980; King and Mayhew, 2002; Rest, 1986, as cited in Myyry et al., 2009) also showed the strong and considerable power of moral reasoning in influencing individual's behavior. More specifically, other studies (e.g. Greenberg, 2002; King and Mayhew, 2002) reported the considerable influence of moral beliefs in policy violation decision.

When we come to the ISS area, Myyry et al. (2009) showed that moral reasoning and individuals' values can be a predictor of individual's compliance with ISSP. Particularly, the authors use two theories from psychology, namely: theory of cognitive moral development and theory of motivational types of values, and the empirical result showed that moral reasoning explains employees' compliance with ISSP. In addition to these findings, Li et al. (2010) study indicates that personal norm moderate the impact of sanctions on employees' compliance intention to internet use policy. Even more recently, Vance and Siponen (2012) reported that moral belief is very strong predictor of intention to violate ISSP. Following the above discussion, we infer that if individual perceive that disobeying the ISSP of his/her company is morally wrong, then he/she does not violate the security policies.

Following this discussion, we formulate the following hypothesis:

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

Shame

Shame is a feeling of guilt or embarrassment if others knew of one's socially undesirable actions (Paternoster and Simpson, 1996). Just like sanctions, shame or self-disapproval might deter people from engaging in illegal activities (Tibbetts, 1997). According to the deterrence literature (Grasmick and Bursik, 1990; Nagin and Paternoster, 1993; D'Arcy et al., 2011) shame is found to have impact in reducing undesirable actions. Unfortunately, Siponen and Vance (2010) reported the inability of shame in reducing computer abuse, and the reason for this finding could be many, but the study population might also contribute its own. Since the sample is taken from Finland (individualist society), the influence of shame might not be strong in such society (Hofsted, 2011).

Following the above discussion, we formulate the following hypothesis:

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

Perceived Benefits

When people engage in a rational decision making process, first they come up with the available number of choices (Paternoster and Pogarsky, 2009) and then analyze the outcome of each of the alternatives to choose the one that is perceived to bring more satisfaction/perceived benefits (McCarthy, 2002). Perceived benefits could be classified into two classes: the first one is an intrinsic benefit such as internal satisfaction one gets from engaging in rule violation activities (Wood et al., 1997), and the other one is extrinsic, such as: money or other material benefits one gets from violating rules and regulation (Lafree et al., 2005).

According to Pee et al. (2008), very large number of employees spend their time on online shopping sites on Monday after thanksgiving day, because it saves their time to shop from their desk than physically visiting a mall. In addition to this, Puhakainen (2006) reported that since ISSP are considered to slow peoples work by bringing many outlines or guidelines to be followed, people preferred to violate the policies to save time. Thus, time saving could also be taken as a motivational factor for employees to violate ISSP. In addition to this, Siponen and Vance (2012) reported the significant positive impact of perceived benefits on employees' intention to violate ISSP. Moreover, according to Li et al. (2010) perceived benefit is found to have a significant negative influence on employees' compliance intention to internet use policy.

Following the above discussion, we formulate the following hypothesis:

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

Uncertainty Avoidance

According to Hofstede (1991) uncertainty avoidance refers to the level of fear people encounter when they come across uncertain and ambiguous condition. According to the author, uncertainty avoidance does not mean risk avoidance, but it tells to what extent society tolerate ambiguous conditions. According to Hofstede (2011) on the contrary, people in a high uncertainty avoidance culture engage in risky activities if they think that this activity will reduce future ambiguity. The author added that on the other hand, people in a low uncertainty avoidance culture are mentally prepared to handle uncertain and ambiguous situations, as a result of this they do have less anxiety. In addition to this, low uncertainty avoidance society is less rule-oriented, more readily accepts change, and takes more and greater risks (Clark et al., 2003). While a high uncertainty avoidance society are always striving to come up with many standards, rules and regulation in order to make sure that everything goes in order.

According to Hofstede (2011), people in a high uncertainty avoidance culture will not tolerate deviant people and ideas, while people in a low uncertainty avoidance culture tolerate deviant

behavior and ideas. If we consider ISSP violation as a deviant behavior, we might say that no matter how much perceived benefits exist; people in high uncertainty culture do not want to violate as well as see people violating ISSP, than their low uncertainty avoidance culture counterparts.

In addition to this, according to Timo (2009), since people in low uncertainty avoidance culture do not fear the risk of becoming jobless or making a wrong choice, they often change jobs, than the high uncertainty avoidance people. With a similar logic, since ISSP violation might bring a number of unknown consequences or threats to individuals, high uncertainty avoidance people prefer not to go to that state, even if there are some benefits of violation. Moreover, uncertainty avoidance is also related to the degree of formalization in organizations, high uncertainly avoidance society having tighter control than lower uncertainty avoidance society (Hofstede, 1980). Consequently, the existence of a greater level of control in high uncertainty avoidance culture might not initiate employees to violate the ISSP of their company. In addition to this, Timo (2009) reported that low degree of uncertainty avoidance might lead to security problems.

Following the above discussion, we formulate the following hypothesis:

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

Masculinity / Femininity

Just like the previous dimension, masculinity/femininity is universal, because in most societies we consider male and female as having distinct role. According to Hofstede (2011), people in femininity culture are modest and caring while masculine society are assertive and competitive. The author added that in masculine society there exists a great role difference between male and female. Masculine society always struggle and compete for a performance society and their goal is to accumulate wealth in "unjust world", on contrary to this, in a more masculine society, most of the time people care, worry and struggle for others life and generally view the world as a "just" place (Hofstede, 2001).

From the above explanation, we might infer that people in feminine society do not only think for themselves, but also for others and hence they are not as selfish as people in masculine society. This selfish and material oriented nature of masculine society might initiate them more than feminine society, to engage in violation of rules.

A research conducted by Timo (2009), has found that masculinity has a slightly negative effect on ISS risks. According to the author, even though the correlation is not as strong as power distance and individualism, it seems masculinity is related to ISS risks. A study conducted by Husted (1999) reported that a masculine society is highly prone to corruption. This could mean, if there exists any benefit of breaking the rule, then the masculine society might not hesitate to break the law more than their feminine counterparts. If we bring this same scenario to ISSP violation, we might incline to say that people in high masculine society, are more exposed than feminine society, to engage in ISSP violation as long as they get some benefit from their action.

Sometimes the outputs from different researchers on same area seem to consistently contradict, for example from the financial reporting literature, 5 out of 9 studies found that higher masculine society is more likely to disclose important information for outsiders (Doupnik and Tsakumis, 2004). Even though the outputs are mixed, most of them indicated that high masculine is related to violation of rule. This situation is clearly related with ISSP compliance, because employees are expected to follow the rule of their company and in this case they do not, and we expect these employees to give security related information, in exchange of some benefit, for others and consequently expose their company data to others.

Following the above discussion, we formulate the following hypothesis:

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

Individualism/Collectivism

This dimension refers to the extent to which individuals in the society are integrated into group (Hofstede, 2011). The author stated that in the individualistic society, there is a very poor relationship between individuals, and people always take care of themselves or only their immediate family members. While in the collective society, people do have a very strong social bonds between them. Moreover, in the individualistic society, everyone is seen as a unique and as a whole, or having self-identity which is separated from the group, while in the collectivist society, it is the group not the individual person, which is seen as the basic unit of the society (Tsakumis, 2007).

When we come to the related works, Shore et al. (2001) reported that national culture affects individual's intention toward intellectual property rights. A research conducted in China by Timo (2009) showed that individualism is positively correlated with a high level of ISS. According to the author, individualist societies provide a more secure environment than collectivist societies. Another study, which is conducted by Tan et al. (2003), investigated the influence of national culture on the predisposition to report bad news about failing IS development projects. Their research showed that individualistic societies were more predisposed than collective societies to report bad news on troubled IT projects. Similarly, an Airplane on its way from Columbia to New York was crashed upon landing after circling a number of times due to bad weather and finally run out of fuel (Leidner andKayworth, 2006). They added that when the flight recorder is examined it showed that the copilots, who came from national culture where subordinates do not tell bad news to supervisors in order to maintain harmony, are failed to provide the worsening condition of the fuel to the captain or ground stations.

In this regards, people in collectivist society give more emphasis for harmony, while in an individualistic society, speaking one's mind is considered to be normal (Hofstede, 1980). Thus, in collectivist society, the perceived benefits of not exposing what they see, is the basic need of keeping themselves in harmony with other people in their society. In this regards, according to Husted (1999), collectivist society's concern for the individuals in their group can motivate them to break the law, and hence he proposed that collective society is prone to

corruption. In addition to this, Tsakumis (2007) reported that higher level of tax evasion exists in collectivist than individualist societies. From the above discussion, we can say that in collectivist society the existence of benefit motivates individuals to violate rule more than their individualistic society.

On the other hand, in the collectivism culture, transgression of norms leads to shame feeling while in individualist society breaking norms resulted in guilty feeling (Hofstede, 1980). If we consider violation of ISSP as breaking norms in the company, then we can say that shame will have a stronger impact in collectivist society than individualist society to deter such policy violation.

Following the above discussion, we formulate the following hypotheses:

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

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

Power Distance

People in low power distance society believe that no one is above the law, while in high power distance society, people rarely disagree with their supervisors and they rarely question their boss (Hofstede, 1980). In addition to this, high power distance society is known for accepting inequality and its implementations in different types of societal hierarchies, which assign different peoples to their respective place (Tsakumis, 2007). According to a study by Bjork and Jiang (2006), security related risks in high power distance culture (Singapore) and low power distance culture (Sweden) are handled in a different ways. Accordingly, in low power distance society, IT manager prefers to solve security issues by reaching consensus directly with the employee involved, while in high power distance society, executives and managers at an upper level are sought out for their advice and guidance. This is a clear indication of how decision making in high power distance culture is very much hierarchical and time taking, due to the number of people involved from different positions.

According to Husted (1999), an increased power distance within a country is found to have a high association with corruption. Moreover, countries with high power distance are found to be associated with a high level of tax evasion (Tsakumis, 2007). As a matter of fact, one can easily guess that people in most cases, engage in corruption or tax evasion by considering the perceived benefits (might be money) of doing that illegal act.

By applying the same logic, in high power distance society, the perceived benefits of violating ISSP, encourage people to violate ISSP than their low power distance counterparts, at least, for the following reason: The point here is, in high power distance society, supervisors will not be asked in most case for whatever they do, and hence they do have a higher chance of violating ISSP without being penalized. And even if they are asked, the process should go many hierarchies and hence measure taken against them will not be fast enough to deter other similar illegal activities. Based on the rational choice of human behavior, measures against illegal activities should satisfy three things to be effective, one of which is swiftness (D'Arcy and Herath, 2011). This situation opens the door for them to engage in illegal activities that are considered to have perceived benefits. Thus, we might say that in high power distance culture, perceived benefits of noncompliance will have a strong influence for employees to engage in ISSP violation than their low power distance counterparts. But when we come to low power distance society, the environment is totally different from high power distance in the following ways: (1) there exist a close communication between supervisor and employees, (2) decision are not made in a long hierarchy, (3) no one is above the law and these conditions hampers individual's intention from committing violation, even if there exists a perceived benefits of noncompliance. On the other hand, according to D'Arcy et al. (2007), employees in high power distance countries show a very big loyalty to their supervisors and they will act unethically if they are ordered by their supervisors. In an empirical research by D'Arcy et al. (2007), security policies are found to be more successful in low power distance (the USA) as opposed to a high power distance country (South Korea). Still, in another empirical work by Dols and Silvius (2010), they found out that if a manager or partner in high power distance society (in this case Belgium) asks employee to break the IT security rules, then he/she will more likely do so than the low power distance society (in this case Netherland). The above

discussion indicates the fact that formal rules or sanctions might be less powerful in reducing noncompliance in high power distance society than low power distance society.

Following the above discussion, we formulate the following hypothesis:

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

H10: The higher the degree of power distance, the weaker the impact of formal sanctions is on employees' intention to violate ISSP

On the other hand, Von Solms and Von Solms (2004) clearly stated that one of the important elements to create an effective ISS culture is to encourage employees to take part in the process of setting up of ISS management goals. This type of cooperation is usually common in low power distance culture. According to Moores (2003), Countries with low power distance scores prefer a more consultative approach to leadership: suggesting a greater interdependence between managers and subordinates in making decisions. Creating a participatory management style do have a considerable influence in creating employees' job satisfaction (Kim, 2002). According to Schappe (1998), job satisfaction is found to be a very good predictor of organizational citizenship behavior (OCB). This OCB intern associated with a higher degree of compliance with organizational rules (Organ and Konovsky, 1989) and consequently create an environment where every individual feels belongingness and morally more tied up to the wellbeing of their company. In this regards, organizational ethical climate can be a significant factor in shaping the behavior of employees (e.g. Dieterly and Schneider, 1974; Fleishman, 1953, as cited in Wimbush et al., 1997). This same concept is strengthened by Vardi and Wiener (1996), noncompliance inside organizations has got two antecedents: individual factors (e.g. dissatisfaction) and organizational factor (e.g. ethical climate). In this regards, even though the degree of influence varies, both individual's supervisors and people at home, do have an influence on individual's decisions concerning ethical dilemmas like noncompliance with organizational rules (Peterson et al., 2001).

Thus, following the above discussion, if people with a higher power engage in rule breaking activity like corruption and tax evasion, then some subordinates even with a strong moral beliefs might gradually come to perceive that breaking policies is not a big problem (even respected people did it), and this actually might weaken the moral beliefs of employees to some extent.

Following the above discussion, we formulate the following hypothesis.

H11: The higher the degree of power distance, the weaker the impact of moral beliefs is on employees' ISSP violation

2.10. SUMMARY

Generally, in this chapter we have tried to give a detailed literature review of important topics that are closely related to our research topic. In doing so, we show the current gap that exists in the area of ISSP compliance/noncompliance and specifically we indicated which of these gaps are of interest for us. In addition to this, we also indicate some gaps that could attract the attention of researchers in the information security area. Finally, we proposed our hypotheses based on the literature we get from different disciplines. The next chapter discusses the research methodology.

CHAPTER 3

RESEARCH METHODOLOGY

3.1. INTRODUCTION

The second chapter discussed important topics around ISSP compliance. In doing so, we tried to give an overview of what are the gaps that need to be addressed by ISS researchers, and more importantly, we highlighted which of these gaps are addressed by our research. Following this, we come up with a research model and hypotheses that shed light on the identified gaps. This third chapter discusses the research method used to test the hypotheses formulated in the previous chapter. Specifically, it discusses the research philosophy that guides this research, the methods and techniques used in the development of research instruments, sample design, data analysis approaches and tools, treatment of the data, and issues related to human subjects. Finally, we summarized the chapter and give a brief description of what is covered in the next chapter.

3.2. RESEARCH PARADIGM

Since researchers are expected to clearly formulate their research methodology in advance, we illustrate the research's underlying philosophies: ontology, epistemology, and method (see Figure 3.1). Ontology focuses on the question of what is taken as real and how to know if something is real or not (Orlikowski and Baroudi, 1991; Guba and Lincoln, 2005; Merterns, 2007). In this respect, a researcher can take the position that the investigated situation has objective reality without the researcher’s methods of inquiry, or one can take the other position, which says the issue under investigation has a subjective reality that can only exist through human action (Kassahun, 2012).

The underlying ontology used here is a position that consider reality as a contextual field of information and it is close to positivist paradigm. The choice for this paradigm is done because the purpose of the current research is to develop and validate an empirical model consisting

of testable hypotheses and also to conduct a qualitative review of important theories that are related to employees' ISS behavior.

The epistemological assumptions are concerned with the nature of knowledge and how it can be gained. The main issue in epistemology is the relationship between the researcher and the researched object or phenomenon (Orlikowski and Baroudi, 1991). Crotty (1998) identified and discussed three distinct epistemological views, namely: 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 (Crotty, 1998).

When we come to the research methodology, according to Creswell (2013), it is a strategy or plan of action that directly connects methods to outcomes, which governs our choice and use of methods. Thus, it does not directly relate to specific methods and techniques that are used for data collection purpose. Basically, there are three methodologies: quantitative, qualitative, and mixed approach (Creswell, 2013).

In this research, our methodology is quantitative method. According to Creswell (2013), the quantitative studies in earlier times mainly focus on: true experiments, quasi-experiments, and correlational studies, and also the single subject experiments. But in recent times, quantitative studies have shifted to a more complex experiment with many variables and treatments; moreover, they include SEM that involves causal path and investigation of the collective impact of many variables (Creswell, 2013). The rationale for adopting a quantitative method is because it provides the ability to produce objective, quantifiable and reliable data that can be generalized to a larger population. Whenever the purpose of a study is hypothesis testing, quantitative survey research is the most appropriate approach (Creswell, 2009).

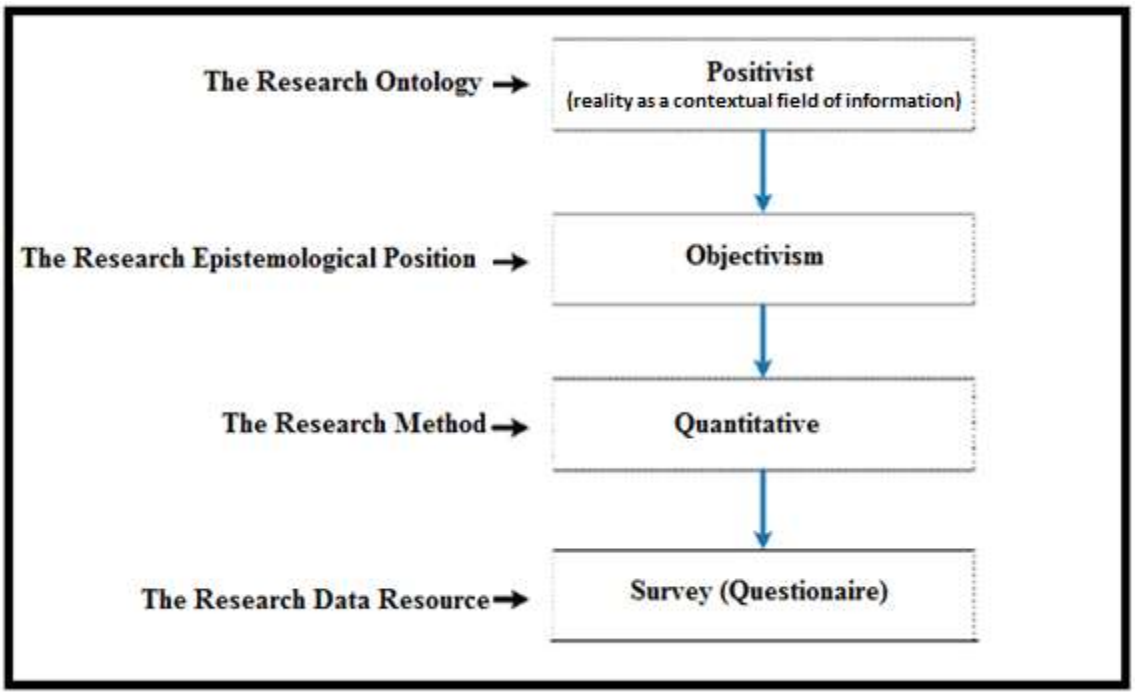

Figure 3.1: The research's underlying Ontology, Epistemology, and Method

3.3. INFORMATION SYSTEMS SECURITY PARADIGMS

According to Dhillon and Backhouse (2001), if researchers want to appropriately and systematically use different security approaches, they must first understand the conceptual basis of various security approaches. In this regards, there are scholars who come up with different types of sociological paradigms. For example, Chua (1986) prefers three primary alternatives: positivism, interpretivism, and critical, while Burrell and Morgan (1979) propose four sociological paradigms: functionalist, interpretive, radical humanist, and radical structuralist that can assist researchers to understand the conceptual basis of their studies. Even though the Burrell and Morgan (1979) sociological paradigm has been widely used in the literature, it has been criticized by other theorists (e.g. Hopper and Powell, 1985; Chua, 1986; Dirsmith et al., 1985; Willmot, 1993, as cited in McFadzean et al., 2006). Based on Burrell and Morganm (1979) framework, Dhillon and Backhouse (2001) execute the most pervasive literature review in the ISS studies to understand the conceptual basis behind the different studies, so that they classify the studies in one of the four quadrants (McFadzean et

al., 2006). Thus, in this section, we discussed some of the basic characteristics of two of Burrell and Morgan's (1979) paradigms. In addition to this, we indicated and justified our paradigm choice for this research.

The security of IS in an organization is a critical activity for information intensive organizations (Herath and Rao, 2009b). Nowadays, organizations are expected to keep their system secure at least, but not limited, for the following reasons: (1) the growing dependency of companies on e-commerce (Barsanti, 1995), (2) growing need for IS to provide the backbone of organizational structure (kankanhalli et al., 2003), and (3) the increasing requirement for regulatory compliance in the wake of financial scandals (Abu-Mussa, 2004). Unfortunately, the Cyber Security Watch Survey (2010) annual report indicated that more than US $2 billion in losses to organizations due to ISS breaches between 1997 and 2007. Similarly, studies conducted in Europe (Anderson, 2001; Earnest and Young, 2001; and DTI study, 2001, as cited in Koskosas, 2004) clearly indicate the increasing trend of security breaches.

A number of ISS approaches have been developed to help security managers to protect their IS from security threats. Reviews of literature in the ISS area indicate the existence of two main approaches: technical, and socio-technical (Holgate et al., 2012). We should note that some researchers like Dhillion and Backhouse (2001) use the word socio-technical and socio-organizational interchangeably (Holgate et al., 2012) and in our research too we use them indiscriminately. According to some studies (e.g. Workman et al., 2008; Siponen and Willison, 2007) in the ISS literature, it is realized that the technical approach mainly focuses on technology and processes but fails to give emphasis on social, organizational, and human aspects. Despite its shortcomings, there exist considerable number of researchers who investigate ISS issues from the technical view only, and in this regards, Siponen (2005) reported that the technical approach predominates the ISS literature. The shortcoming of the technical approach initiates ISS researchers to embark on socio-organizational approach (Dhillion and Backhouse, 2001).

Despite the growing agreement by ISS scholars to shift from technical centric to socio-organizational perspective, there still exist unclear understanding of what does the word social means in socio-organizational, provided that there are many disciplines that use their own way of understanding and evaluating of social dynamics (Holgate et al., 2012). This might indicate the existence of different perspectives as to "how to investigate the socio-organizational concerns?" In this regards, we can mention the work of some researchers that use different sociological perspective to address the social issues.

A study by Dhillon and Backhouse (2001) used the interpretive approach to deal with social and organizational issues, while a study by Holgate et al. (2012) prefered to use the social constructionism perspective. According to Holgate et al. (2012), their first reason to embark on this perspective is based on what Griffith and Dougherty (2001) state: human and organizational outcomes can only be understood if we can investigate the cumulative effect of the interaction among social, environmental, psychological, and technological issues as a whole, while their second rationale is that some types of technologies (processes that depends on technology) might need a special configuration of social setting (Pinch, 2008). On the other hand, Hu et al. (2007) grounded themselves in the sociological neo-institutional approach to examine the impact of institutional factors on organizational action and behavior using a positivist case study approach. In addition to the above researchers, Whitman (2003) used the risk analysis method to come up with possible categories of threats to IS, and according to Swart (2007) "Though Whitman's paper can be categorized as functionalist, it is apparent that his concern extends beyond the technical system to the interaction of users or other actors within the IS". A more recent study by Dols and Silvius (2010) used the functionalist positivist approach to investigate the impact of national culture on employees' non-compliance behavior. These works could be an example of how the functionalist paradigm can go beyond technical only view to include social issues.

According to Palvia (2006), within the functionalist paradigm, the positivist approach can be defined as an approach where facts are precisely defined and results are measurable. In line with this idea, Myers (1997) clearly states that the main purpose of positivist studies is to test

theories in an attempt to increase the predictive understanding of phenomena. As discussed in the previous chapter, one of the main purposes of our research is first to conduct a detailed qualitative literature review about theories (constructs) that are related to individuals ISS compliance behavior. In addition to this, we also planned to create a model that is constituted from these theories, so that we can test different hypotheses from there. Thus, in our study, we found the a position which is close to the functionalist positivist approach (i.e. reality as a contextual field of information) to be appropriate to investigate or test how social factors specifically national culture, as defined and measured by Hofsted (1980), influence employees' compliance behavior with ISSP.

Within the functionalist paradigm, the first and the most commonly used approach is the technical approach, which mainly focuses on checklists, risk analysis, and evaluation, while the socio-organizational approach focuses on the use of social theory as their basic theoretical foundation to investigate ISS issues (Dhillon and Backhouse, 2001). Since the two main and opposing paradigms in the field of IS are positivist (Burrell and Morgan's functionalist paradigm) and interpretive (Information Resources Management Association, 2006), our discussion will focus on these two paradigms.

3.3.1. The Functionalist Paradigm

The functionalist paradigm refers to the search for explanations of social events from the view of a realist - what can be described as a positivist perspective (Palvia, 2006). In the same way, according to Dhillon and Backhouse (2001), this paradigm approaches the subject under consideration from an objective point of view and also in the sociology of regulation. This approach views the world as tangible, made of hard and immutable structure (Dhillon and Backhouse, 2001). The authors added that since the social world is composed of concrete empirical artifacts, any relationship between the artifacts could be understood by using approaches from the natural science. According to Wheeler and Venter (2006), this paradigm is primarily influenced by the notion of predictive knowledge and hence this knowledge guides the rules, policies and guidelines of the functionalist approach.

The functionalist structured approach to ISS has been the focus of many ISS researchers (e.g. Straub and Welke, 1998; Siponen, 2000; Von Solms and Von Solms, 2005; Vorster and Labuschagne, 2006, as cited in Njenga and Brown, 2008) and it is characterized by having many policies, guidelines, standards and frameworks to create a stable and protected IS environment. Some of the techniques used in this paradigm are discussed below.

1. Check List

From the technical approaches, the checklist is considered to be the most commonly used method, and it mainly focuses on identifying every controlling mechanisms that can be used in securing IS from security breaches **(**Dhillon and Backhouse, 2001). Security managers will always assess the effectiveness of the current evaluation guidelines, and if they find any gap or inefficiency among the current evaluation guidelines, then they will recommend modifications (if necessary exclusion) of current guidelines and in case inclusion of additional guidelines that are believed to improve the security of the IS (Baskerville, 1993; Dhillon and Backhouse, 2001). The foundation concept of this method focuses on "what can be done rather than what needs to be done" (Baskerville, 1993), and consequently researchers like Hirschheim and Klien (1989) criticized this approach by stating: "The checklist method focus on means rather than ends". In addition to this, Crossler (2013) clearly stated that even though checklist is one of the most widely used methods, it fails to inculcate the social aspect of systems' security, and according to him, this method is overly concerned with the observable aspect of systems. Dhillion and Backhouse (2001) added that the checklist method is known for its analytic instability due to the frequent change of its procedures.

Almost all of the well-known checklist methods focus on issues like disaster recovery planning, encryption, off-site backup, access and change control, contingency planning, and physical security. To mention some of the typical examples of the checklist methods: IBM's 88 point security questionnaire (IBM, 1972), the SAFE checklist (Krauss, 1972; Krauss, 1980), the Computer Security Handbook Checklist (Hoyt, 1973; Hutt et al., 1988), and the AFIPS Checklist for Computer Center Self Audits (Hutt et al., 1988). Unlike others, the

AFIPS does not simply classify threats, but it contains a core framework of threats together with their remedial action (Baskerville, 1991).

2. Risk Analysis Approach

Risk analysis had been the motto of ISS just a decade ago, and hence it attracted the focus of many researchers (Dhillon and Backhouse, 2001). The main idea of this method is stated as "Negative events can be avoided and IS can be made safer by implementing countermeasures in sequential and logical fashion" (Koskosas, 2004). This approach is considered to be the most widely used among IS community. Baskerville (1991) stated that almost all researchers in ISS use risk analysis in one way or the other. He added that even though the risk analysis model has got a very limited predictive power, it can be used to establish IS control, particularly it has a paramount importance of being an effective communication tool between security and management professionals.

By thoroughly examining the cost and benefit (financial benefit Vis-a-Vis the initial investment) associated with the new ISS method, the risk analysis method helps managers to avoid the implementation of expensive and inappropriate approaches (Dhillon and Backhouse, 2001). This type of management science principle made the mathematical bases for techniques that are used to calculate the risk associated with an event (e.g. Courtney, 1977; Wong, 1977). Courtney (1977) tried to mathematically calculate the risk (R) by taking into account the probability of exposure per year (P) and the loss or cost (C) associated with the exposure, and hence R=P*C. This technique is used as a standard measure of risk by the US Department of commerce (Reed, 1977). There are also other risk management techniques that were proposed by different scholars in the past. For example, RISKPAC (Computer Security Consultants, 1988), CRAMM (CCTA Risk Analysis Management Methodology), and MERION (Birch and McEvoy, 1995).

3. Evaluation Methodology

Another very important approach of ISS in the positivist paradigm is the evaluation method, which mainly focus on determining or measuring the security level of IS (Caelli, 1991). Within this methodology, there were a number of models and techniques, sponsored by the US Department of Defense, which can be used to grade or measure the degree to which IS are secure. The Bell La Padula model (Bell and La Padula, 1976) is one of the most commonly known models to protect unauthorized access of information. The Trusted Computer Systems Evaluation Criteria (TCSEC) also called Orange Book, which was published in 1983 by the National Computer Security Center in USA, was widely used by computer vendors as a base to produce computer systems that are more resistant to security related problems, and more importantly the US Department of Defense currently uses these criteria as essential part of their overall security strategy **(**Dhillon and Backhouse, 2001**).** TCSEC (Orange Book) was combined with a similar document known as the "Red Book" that contains evaluation criteria for network related security issues (Interpretation, 1990). Finally, the combined document of the Orange Book and the Red Book become an international standard for computer security in the 1990's, and this process was sponsored by the International Standards Organization (ISO) (Pfleeger and Pfleeger, 2003)

Since then, a number of improvements have been made to the evaluation method (specifically to TCSEC), and one of them is the INFOSEC (Information Security) approach, which was proposed by Chokhani (1992), Unfortunately, this new method is criticized for being more of technical oriented, which delimit it from the social context. The SECURATE evaluation method, proposed by Gottfredson et al. (1978), is an automated approach that can automatically calculate the security level of IS using fuzzy set logic theory, moreover, it discusses the strength and weakness in the IS design (Dhillon and Backhouse, 2001). In addition to the above evaluation criteria, which are mainly developed and used in the US, European countries have been trying to come up with a standardized ISS procedure. For example, series of versions of the 'GREEN Books' were released in the UK, while the 'White Books' evaluation criteria was published in 1990 by some European countries as part of their attempt in standardizing their ISS procedures.

Despite its huge public support, the evaluation criterion has failed to answer many critical questions raised by researchers (e.g. McLeen, 1990). In addition to this, the evaluation method is criticized for being more of technical approach and also it is found to have less use in the long term. According to Dhillon and Backhouse (2001**),** the traditional evaluation approach and techniques have worked well in the military environment, but it is not adequate for the business environment, because the business organizations have a different environmental setting and realities, and this creates a compatibility and coherence problem. The authors clearly stated that the traditional evaluation criteria should be translated into commercial context so that they can be used efficiently in another area.

As can be understood from the above discussion, technically oriented researchers in the factionalist paradigm mainly focus on technical issues concerning the design and implementation of security systems (Choo, 2011; Zafar and Clark, 2009). To this end, we can mention the following works: Hanson et al. (2007) advanced techniques for prevention of cyber terrorism through dynamic and evolving intrusion detection, Zhi-Jun et al. (2012) detection of denial of service attacks, and Ayuso et al. (2012) advanced solutions for firewall protection. Actually, the contributions of these technical and externally focused studies are very valuable, but they lack a very important and critical ingredient of the ISS, the human element. Even though the technical and externally oriented attempts are important, one area that is predominantly weak in properly securing IS is the employee within the company (Leach, 2003; Posey et al., 2013; Sasse et al., 2001; Stanton et al., 2005; Von Solms and Von Solms, 2004, as cited in Warkentin and Willison, 2009).

Even though the methods discussed under the functionalist perspective look to take a very narrow technical view of ISS, the general belief of this paradigm is IS can be made secure by investigating the behavior of the various components of the IS (Dhillon and Backhouse, 2001; Goldspink, 2000, as cited in McFadzean et al., 2006). As one of the main components of IS Human beings do have their own behavior, which is in part a direct result of their culture (Al-Awadi and Renaud, 2007), and hence the functionalist approach can be used to investigate the influence of national culture on individuals ISSP compliance/noncompliance behavior. In

this regards, there are researchers who use this same functionalist positivist perspective to successfully deal with such social issues. For example, the work of Shaw (2012) examined the contributing factors in the relationship between organizational culture and employee attitudes towards ISSP. Another example is the work of Dols and Silvius (2010), who investigated the influence of national culture on employees' noncompliance behavior.

3.3.2. The Interpretive Paradigm

An alternative perspective to the functionalist paradigm is the interpretive paradigm. According to Cardoso and Ramos (2012), "The interpretivist research poses an epistemological assumption that knowledge is gained by social constructions". According to researchers, the interpretive approach is believed to provide some advantages as well as disadvantages. For example, according to Dhillon and Backhouse (2001), the interpretive approach is considered to provide a holistic view of the problem domain instead of a simple unidirectional explanation. On the other hand, the explanations are difficult to comprehend, because of the sophisticated philosophical and sociological bases of the paradigm, and thus this paradigm is confined to a small number of academicians (Dhillon and Backhouse, 2001).

Before 2/3 decade or so, most IS researchers were confined to the functionalist approach, and hence the interpretive paradigm has been given little attention. But, gradually there are more and more attempts to use the philosophical assumption of the interpretive paradigm in the IS studies (Dhillon and Backhouse, 2001). From the forefront research works, we can mention the work of Orlikowski and Baroudi (1991) that tried hard to introduce the interpretive paradigm into the IS discipline, specifically they studied IS use within the organization by using the well-known structuration theory. A very important point that needs to be raised here is that almost all attempts in the interpretive paradigm focus on the mainstream IS discipline, and in most cases they ignore the ISS area (Dhillon and Backhouse, 2001).

According to Dhillon and Backhouse (2001), most approaches to ISS management seem to stick to the 'organization as a machine' metaphor, and completely ignore the human element. Siponen (2001) also added that during that time, many approaches to manage the security of

IS relied heavily on techniques and methods that are available in the computer science and database management systems.

Even though it is isolated and limited, during the 1990's, there was an emerging trend in the IS studies to consider the socio-technical aspect of ISS management (e.g. Dhillon and Backhouse, 1991; Hitching, 1996; James, 1996, as cited in Dhillon and Backhouse, 2001). In addition to the above mentioned researchers, we can mention the research work of Willcocks and Margetts (1994) who tried to analyze the risk of breaches in ISS, and they come to conclude that social and qualitative elements play a very critical role in ISS. Other researchers like Straub and Welke (1998) use the interpretive paradigm to develop guidelines to be used in protecting IS from security breaches. While Baskerville's earlier works focus on structured and mechanistic approaches, lately he has shown an interest in using the interpretive approach to design ISS, specifically in the area of risk analysis (Dhillon and Backhouse, 2001). Other researchers (e.g. Dobson, 1991; Stren and Dobson, 1993) apply the traditional interpretive social theories in understanding ISS problem (Dhillon and Backhouse, 2001).

3.3.3. Summary

As can be understood from the IS literature, there is an increasing dissatisfaction in the IS discipline with the formal, rational, and overly mechanical conceptions of the analysis and design of IS. For example, if we take the risk analysis method and evaluation method, which are grounded in functionalist paradigm, their main focus is to apply a valid and complete model for the commercial setting, but they are highly narrowed down to managing access control. According to Dhillon and Backhouse (2001), this view might work if the computer service provision was limited to a single function (a centralized processing) and the organization structure is hierarchical, but the methods will be insufficient to handle modern day organization with a flatter and more organisms like in their nature. Hence, researchers should address the ISS issues from a broader point of view by considering the system together with its interaction with people and every other social issue. Due to this fact, there is an increasing trend in IS discipline (other than the security area) to inculcate the soft sides. According to Dhillon and Backhouse (2001), in contrast to the mainstream IS studies, the ISS

research focus on formalized rule structure, while it lag behind in considering the softer issues. They added that ISS does not only mean to protect tangible and hard elements nor just 'lock and key'; rather, attention should be given to the intangible components of the system, like social grouping and behavior.

In general, the ISS literature indicates the importance of context of use of the various security models/frameworks. Thus, one can infer how much inappropriate or difficult it would be to manage the ISS by using only the conventional technical only approaches. Even though the technical approaches show preponderance in the ISS area, there is an emerging trend in IS studies in moving away from the narrow technical paradigm. Researchers like Sharma and Thomas (2008) have clearly indicated the fact that the IS disciple has progressed from having a purely technical focus, to inculcate issues that are increasingly considered to be very important in the security environment such as behavioral and economic ones.

According to Crossler et al. (2013), even though there is increasing number of studies in the behavioral ISS area, still there exists a huge obstacle that should be dealt by future work. The authors take input from different sources, including the following: the International Federation for Information Processing working group (which is known for promoting behavioral research works), researchers in the behavioral ISS area, and also from the IS community. Finally, they summarized and set forth five different themes for future work and two of them are: improving ISS compliance, and cross-cultural ISS research. As can be understood from the literature, the functionalist positivist approach is in most cases used by researchers to focus only on technical issues, so that we prefer to rely on a position that is close to positivist but capable of exploring social phenomenon and human behavior, that is reality as a contextual field of information (Morgan and Smircich, 1980).

3.4. RESEARCH DESIGN

In this research, we employed the hypothetical scenario method to assess respondents' intention to violate ISSP. The choice for this method is based on its potential advantages in the area of ISSP violation. Thus, in the following subsections, we discussed issues related to the research design, such as: why we chose the scenario method, how the scenarios are designed, how pretest is conducted, and the overall process of instrument development.

3.4.1. Scenario Method

In this research, we assessed our model by using a scenario method. This method gives a clear description of a realistic situation or phenomenon and respondents give their answer on a scale that measures the dependent variable (Trevino, 1992). The scenario method provides many advantages over the traditional survey method, which asks general questions. We summarize the most important advantages of the scenario method in the following paragraphs.

First, according to Pogarsky (2004), the scenario method is well suited to study issues that measure or asks about ethical/unethical behavior. In this respect, the scenario method offers an indirect way of measuring the intention of people to commit socially undesirable act, which might be difficult to measure by using the traditional questionnaire, because an individual will most likely conceal his/her real intention and respond in a way that is acceptable by society (Trevino, 1992). The author also added that since the scenario method describes the behavior of a third person in a hypothetical way, responds will not be intimidated to show his/her support to what the person in the scenario did (Trevino, 1992). Since ISSP violation is socially undesirable behavior, it is more appropriate to use the scenario method than the conventional survey approach.

Second, since the scenario method offers a very detailed situational context, it offers very strong theoretical benefits for research that use the RCT. According to Becker (1968), what RCT posits is that a potential offender always calculate the cost and benefit of his/her action in a particular context (Becker, 1968), and this contextual detail is clearly offered by the scenario method. On the other hand, if we use survey questions that ask people in general

term without any context, they will create their own ideal context and respond to the question based on their own imaginary context (Bachman et al., 1992). The author added that this might create a measurement error if their imagination of the contextual detail is different from what the researcher think. This idea is also strengthened by Alexander and Becker (1978) who stated that the scenario method will always improve the realism of the decision making situation by offering a well prepared contextual details and these detail are uniform across respondents.

Third, the scenario method has methodological advantages in measuring socially undesirable behaviors prospectively (Pogarsky, 2004). According to Bachman et al. (1992), the traditional survey methods are confined to measure past behavior with the present perception of constructs in the survey and hence they recommend prospective measures of behavior like "intention to commit an act" when the survey involve ethical dilemmas.

3.4.2. Scenario Design

When people design the scenario method, they should keep in mind that the scenarios should represent very important and commonly found ISS issues. According to Piquero and Hickman (1999), a very important point in designing the scenarios is to make sure that they are realistic and well known to participants. Thus, to make our scenarios realistic and common, we interviewed ISS officers from five different organizations in Ethiopia. We also interviewed seven ISS officers from the US.

According to Vance and Siponen (2012), in order to design the scenarios that do have a practical relevance in the context of employees ISSP violation, researchers can follow either one or more of the following approaches. The first approach is using a quantitative approach, where the researchers will analyze the literature and based on that they will come up with a list of ISSP violation statements, which will be then given to ISS officers to evaluate and rank them based on their relevance. The second approach is to fully design different scenarios and give it to the ISS officers to evaluate, comment, and rank based on their relevance. The third approach is to ask the ISS officers to come up with their top four/five common and relevant

ISSP violations. According to Vance and Siponen (2012), from the three approaches the first approach mainly focuses on verifying and ranking existing knowledge, while the remaining two approaches allow us to come up with additional knowledge of the ISSP violations. Thus, in this research, we used the third approach to come up with more recent, common and appropriate scenarios.

During the survey process, we asked ISS officers to list their top three ISSP violations that are important and happen more often in their company. After receiving their response, we tried to organize the most commonly raised security concerns into nine groups. Accordingly, the top nine ISS concerns that are raised by most ISS officers are organized as: sharing customer information, password sharing, failing to report computer virus, going out while their computers are logged-in, writing passwords in visible places, using the internet for non-work related activity, playing games on computers during work hours, failing to update their computer antivirus in a timely manner, and directly using their personal flash disk without scanning with antivirus software.

Following this, we sent the nine statements to all ISS officers and we gave them a chance to rank the top three common and relevant ISSP violations, 80% of them voted the top three as: password sharing, going out while their computers are logged-in, and sharing customer information. The reason why we choose more scenarios is to give our research a comprehensive view, so that we can be sure that at least the research cover more ISS violations problems and our findings can be more generalizable than using a single scenario. According to Vance and Siponen (2012), to improve the generalizability of a research across variety of ISSP, it is important to come up with different scenarios with different types of security violation issues.

Following this, we start to design the scenarios for the three cases. When we design the scenarios we take into account a number of factors, such as: scenarios should describe details like names of a person (Piquero and Hickman, 1999), and scenarios should come up with common and important security issues (Piquero and Hickman, 1999). Since two of our scenarios are similar to Vance and Siponen's (2012) scenarios, we use them with a little

modification, while we build the third one. Finally, we give these scenarios for the ISS officers followed by language editors and based on their comment, we finalize the design of the scenarios. The hypothetical scenarios are located at Appendix 2.

3.4.3. Instrumentation

In this section, we discussed the way the constructs in our research are operationalized. Generally, all the constructs are operationalized by using previously validated instruments, and prior to conducting the pilot test there were a total of 44 items and after this test the items are reduced to 37 and the average score (based on the final survey) for each of the constructs is shown on Appendix 3. The scale for all the constructs is on five point Likert type scale and all the initial items and their sources are shown in Appendix 4. In this regard, the response scale for some of the constructs (i.e. perceived benefits, moral beliefs, power distance, uncertainty avoidance, collectivism/individualism, masculine/feminine, CSSE, intention to violate ISSP) ranges from 1 (strongly disagree) to 5 (strongly agree), while for the remaining constructs (i.e. shame, formal sanction) it ranges from 1 (highly unlikely/not problematic) to 5 (highly likely/very problematic). Below is the detailed discussion concerning the operationalization of each of the theoretical constructs.

Perceived Benefits

In this research, perceived benefit is defined as "The offender's subjective analysis of the cost–benefit associated with ISSP violation" (Li et al., 2010). Specifically, in the case of ISSP violations, time saving is considered to be the most significant incentive to violate ISSP (Puhakainen, 2006). Since time saving is given a very big emphasis in the violation of ISSP, we use Vance and Siponen's (2012) instruments to operationalize the perceived benefits construct. Vance and Siponen (2012) develop instruments that include the sense of time saving by violating ISSP. Accordingly, this construct is measured by four items and each use an ordinal scale to allow the respondents to rate their agreement or disagreement related to statements to the construct of perceived benefits.

Moral Beliefs

In this research, moral beliefs refers to "an individual's personal judgment about engaging in ISSP violation as morally wrong or right" (Bachman et al., 1992). Operationalization of this construct is based on the research work of Vance and Siponen (2012). Accordingly, this construct is measured by three items and each use an ordinal scale to allow the respondents to rate their agreement or disagreement related to statements to the construct of moral beliefs.

Shame

Shame is defined as "a feeling of guilt or embarrassment if others knew of one's bad actions" (Paternoster and Simpson, 1996). Operationalization of this construct is based on the research work of Vance and Siponen (2012). Accordingly, this construct is measured by six items, and each use ordinal scale to allow the respondents to rate the likelihood or the level of problem related to statements to the construct of shame.

Formal sanction

Formal sanction is defined as "penalties that is given for specific forms of violation" (Vance and Siponen, 2012). Operationalization of this construct is based on the research work of Vance and Siponen (2012). Accordingly, this construct is measured by six items, and each use an ordinal scale to allow the respondents to rate the likelihood or the level of problem related to statements to the construct of formal sanctions.

National Culture

With respect to culture, since it is defined at national level, we must make sure that the individuals being studied show similar cultural score with their country score as predicted by Hofstede's (1980, 1984, and 2001) work (Yoo et al., 2011). Because it is not possible to blindly bring the national score to individual people, Yoo et al. (2011) advised researchers to use a measure that conceptualize Hofstede's (1980) national culture dimensions at the individual level. Following this, Yoo et al., (2011) develop the first comprehensive scale to

assess Hofstede's cultural dimensions at the individual level. The new scales make it possible to directly link individual's attitude and behavior to their level of cultural orientation, because this data comes from the primary source (individual survey response) rather than using Hofstede's score (secondary source) (Yoo et al., 2011). Yoo et al. (2011) work is not the only study that develops a scale to measure the national culture dimension at individual level. There are some works that come up with their scale of national culture at individual level but they are criticized for the following shortcomings (Yoo et al., 2011). First, some develop scales to measure one dimension at a moment (e.g. Triandis, 1995; Bearden et al., 2006) and this creates a problem of methodological uniformity between different scales developed at different times by different scholars for different purposes. Second, there is hardly any attempts to develop scales for all the five dimensions and even for those who develop scales for more than one dimension, it is limited to specific area like management (e.g. Dorfman and Howell, 1988; Erdem et al., 2006). Third, researchers like Furrer et al. (2000) develop with a scale for all five dimension of Hofstede's national culture dimension but the psychometric properties of the scale is found to be poor. Finally, there is a recent attempt by Sharma (2010) and his scales show a very good psychometric properties. But, the study re-conceptualizes Hofstede's five dimensions into 10 dimensions and this create a difficult and confusing situation to measure Hofstede's original dimensions (Yoo et al., 2011).

Power Distance

Power distance is defined as "the degree to which inequality between people is seen as irreducible fact of the society life" (Hofstede, 1980, p.26). Operationalization of this construct is based on the research work of Yoo et al. (2011). Accordingly, this construct is measured by five items, and each use an ordinal scale to allow the respondents to rate the level of agreement or disagreement related to statements to the construct of power distance.

Uncertainty Avoidance

Uncertainty avoidance is defined as "the degree to which people in a society prefer a more structured over unstructured situation" (Hofstede, 1980, p. 24). Operationalization of this construct is based on the research work of Sirte (1999). Accordingly, this construct is

measured by six items, and each use an ordinal scale to allow the respondents to rate the level of agreement or disagreement related to statements to the construct of uncertainty avoidance.

Collectivism/ Individualism

Collectivism refers to "the extent to which individuals in the society are integrated into group" (Hofstede, 2011, p.22). Operationalization of this construct is based on the research work of Yoo et al. (2011). Accordingly, this construct is measured by six items, and each use an ordinal scale to allow the respondents to rate the level of agreement or disagreement related to statements to the construct of collectivism/ individualism.

Masculine/Feminine

Masculine/Feminine is defined as "the degree of focus on work goals and assertiveness, as opposed to personal goals (friendly environment, getting along with others) and caring for others" (Hofstede, 2011, p.23). Operationalization of this construct is based on the research of Yoo et al. (2011). Accordingly, this construct is measured by four items, and each use an ordinal scale to allow the respondents to rate the level of agreement or disagreement related to statements to the construct of masculine/feminine.

CSSE

The other important control variable is CSSE. It is defined as "an employee's judgment of personal skills, knowledge, or competency about fulfilling the requirements of the ISSP" (Phelps, 2005). Operationalization of this construct is based on the research work of Herath and Rao (2009a). Accordingly, this construct is measured by three items, and each use an ordinal scale to allow the respondents to rate their level of agreement or disagreement related to statements to the construct of CSSE.

Intention to violate ISSP

Intention to violate ISSP is the dependent variable of this study. Operationalization of this construct is based on the research of Vance and Siponen (2012). Accordingly, this construct is measured by a single item, and the item use an ordinal scale to allow the respondents to rate level of their agreement or disagreement related to a given scenario case. According to Cook

and Campbell (1979), researchers should not use a single item measure because it is prone to mono-operation bias, which prevent constructs from being reliably measured. However, according to Straub (2004), in specific situations using only a single item measure is the most important and appropriate decision. One of these specific cases is measuring of people's intention in scenario based survey (Pogarsky, 2004). In addition to this, measurement error is not expected for this type of item, and hence it is advisable to use a single item measure (Paternoster and Simpson, 1996). As discussed in the Scenario design section, we already prepared three different scenarios and each of the randomly selected scenarios is given to respondents. It is not possible to give all the three scenarios for every respondent because each scenario is associated with many questions.

Control Variables

In addition to the dependent, independent and moderator variables, we also include items that serve as a control variables in our study. The main reason for the inclusion of such variables (age, gender, CSSE, scenario realism, and scenario type) is because they are believed by previous researchers to have impact on individuals' intention to misuse their organizational IS. In this regard, age and gender are reported to have influence on IS misuse intention (Leonard and Cronan 2001; Leonard et al. 2004) while CSSE also reported as having a considerable influence on IS misuse intention (Compeau and Higgins, 1995; Son, 2011). In addition to these variables, scenario realism and scenario type are also included as a control variable. Scenario realism refers to the extent to which respondents perceive the hypothetical scenario they received is a common and probable case in their workplace while scenario type refers to which of the three scenarios does each respondent received. According to Vance and Siponen (2012), scenario realism has a significant impact on individuals' intention to violate security policies. We include the scenario type because we randomly assigned each of the three scenarios to participants.

3.4.4. Pretest

After the survey instrument is finalized, pretest is the next step of the research process. According to Converse and Presser (1986), the pretest process is a critical examination of the

survey instruments that helps to know if the survey instruments will function properly as a valid and reliable research tool. By using the pretest mechanism, researchers can make sure that their survey items are clearly described and the response options are important, complete, and mutually exclusive. According to Converse and Presser (1986), before proceeding with the collection of data, researchers need to know that both the researchers and the respondents understand the instruments in the same way. Moreover, the authors stated that pretest can help researchers to make correction on inevitable instances of vague terminologies, unfamiliar references, and ambiguous words and phrases that the researchers do not observe before. In addition to this, pretest allows the researchers to evaluate response latency, the amount of time needed to complete each item as well as the whole survey (Bassili and Scott, 1996).

According to Jansen and Hak (2005), when we pretest our survey items, we should ask experts to provide an assessment of individual questions, particularly ask them to rate on a Likert scale. The main purpose is not to collect the expert opinion and belief, but to get their judgment on how well the instrument items reflect the construct. For the pretest, we used a group of ISS experts (panels of experts) to go through all the scenarios and the survey instruments to make sure that the survey instruments do have a strong content validity (Lewis et al., 2005). According to Sheatsley (1983), the rule of thumb is to select 12 to 50 experts. Thus, we selected 18 ISS experts from Ethiopia and the US to examine the scenarios and the instruments. 6 of them are practitioners while 12 are academicians. The reason we include both types of experts is to get as much of a broad view as possible on our survey instruments. In this regards, the practitioners' comments on the scenarios are found to be invaluable due to their rich experience of dealing with the different types of ISSP violations in their day to day life. Based on their comments, we find areas of improvement on the scenarios, such as: fine-tuning the way and the context in which the ISS violations happen in most cases, changing some words to make sure that everyone will have the same understanding of the statements (e.g. changing workstation to computer, and changing some difficult words by commonly known words, like reprimanded by criticized). Except the above minor changes, all the experts agreed that the three scenarios discussed common ISSP violation issues, which actually help us to make sure that all the respondents are familiar to what the scenarios state.

Accordingly, we make the changes to our scenarios and the final hypothetical scenarios are located at Appendix 2.

The academician experts gave a lot of comments concerning the instruments, such as: whether the survey items flow perfectly from question to question, the quality of the instrument to accurately measure the constructs, modification of the wording of some items. Accordingly, we make some changes in the sequence of the questions, like bringing the questions that are related to the scenarios just below the scenario, so that respondents can directly answer scenario related questions after reading the scenario. According to Olson (2010), survey instrument items should have a logical and intuitive layout to reduce the burden on the respondents and to increase the quality of data we get from the respondents. In addition, we changed the wording of the some of the questionnaires; for example, we make changes to statements that says "What is the chance that you would do what [the scenario character] did in the described scenario?" is changed to "What is the chance that you would do what Jack did in the described scenario?" When we come to the measurement issue raised by the academicians, they comment to use a specialized measure of CSSE rather than using the general self-efficacy measure. Based on these comments, we changed the instruments accordingly.

In addition to the advice and comments we received from the panel of experts (POE), we also administered the pretest survey to a small subsample of the sample population. One of the useful pretest is done when researchers pretest their instruments on a subsample of the sample population because the respondents fit the cultural and demographic profile of the bigger sample to be examined later (Ferketich et al., 1993). For this purpose, we gave the questionnaire for 30 employees in Ethiopia and asked them to give their comment on issues, such as: the clarity of the questions and the instructions, any practical problems they encountered when filling the questionnaire, and the amount of time it takes to finalize the questionnaire. By sending two reminder emails to the respondents who did not return the questionnaire on time, we received 23 (76%) usable response from the respondents. All respondents stated that the questions and the instructions were clear and they understood them

well. There was one minor comment on the use of abbreviation like IS, suggesting some respondent might not be aware of the exact meaning of the abbreviation and hence we change it to information systems. In addition, they commented on the amount of time required to fill the questionnaire. In this regards, our first assumption was to give 25 minutes, but the average response from respondents is around 19 minutes. To make it convenient for respondents, we decided 20 minutes as the response latency for the completion of the questions. Based on the pretest conducted both on experts and subsamples of the sample population, we make adjustments to our instruments and the final questionnaire is located at Appendix 5.

3.5. SAMPLE DESIGN

When researchers conduct an empirical quantitative survey research, a great care needs to be taken to design a sample that truly reflects the theoretical population (Bell and Bryman, 2007). The population for this study includes all current employees located in Ethiopia who are working in companies that do have ISSP. In this section, we discussed the sample design process followed in collecting the final data. Sample design involves making different types of decisions, such as: sampling frame, the sample size, and respondent selection.

With respect to the survey respondents, even though there is no single agreed upon criteria to determine the total number of respondents needed in the survey, there are some formulas and suggestions that can help researchers to determine the approximate number. In this regards, we determines the sample size by following suggestion of researchers' (e.g. Hair et al., 2006; Kline, 2005; Weston and Gore, 2006; Lewis et al., 2005) and with reference to prior studies. In this regards, we can mention the formula recommended by Tabachnick and Fidell (2001). According to the authors, the sample size can be calculated based on the following formulas:

Sample Size = 104 + M

Or

Sample Size = 50 + 8M

Where **M** refers to the number of independent variables in the research model.

Thus, based on the first and the second formulas, the expected sample size is 112 and 114 respectively, where **M** equals eight independent variables in our research. On the other hand, Kline (2005), and Weston and Gore (2006) recommended to have a minimum sample size of 200 for any SEM analysis. Since this study intended to use confirmatory factor analysis using AMOS, it requires a minimum usable sample size of 100–200 (Lewis et al., 2005; Hair et al. 2006). Research on required sample size also indicates that a sample size of 200 is good for various types of statistical analysis (MacCallum et al., 1996). Further, a review of 154 previous studies conducted on organizational setup showed that the average actual sample size (actual responses) obtained was 157 (Kassahun, 2012).

Since we use SEM based statistical analysis, we believe that the number of usable responses should be greater than or equal to 200 and as can be seen from Table 3.1 after the main survey we get 210 usable responses and this number is well above the minimum threshold set forth by Weston and Gore (2006) .

To select potential respondents, first we selected major cities around Ethiopia followed by selection of organizations that do have some form of ISSP. Since many organizations in Ethiopia do not have a well-documented ISSP (Yigezu, 2011), it was a very challenging task to get those few organizations at least with a simple ISSP. Despite this difficulty, we managed to get organizations with ISSP and by communicating with the human resource departments of each organization, we randomly selected employees. The next paragraphs show how we conducted the overall selection process.

In the course of the survey, we strived as much as possible to have employees from different regions, so that our respondents can be a better representative of the Ethiopian national culture. In this regards, first we made a detailed discussion with people who do have a detailed knowledge of the demographic and cultural setup of Ethiopian regions (Interview with researchers in the area of sociology, Addis Ababa University). According to these sociologists, there exist five cities in Ethiopia that are believed to be a representative of the core of Ethiopian cultural characteristics. Following their suggestion we select cities, namely:

Addis Ababa, Mekele, Bahir Dar, Hawassa, and Dire Dawa as cities that contain the sampling frame of this study.

To implement this frame, first we were expected to identify organizations in those cities that do have a well-established set of ISSP. In the identification process, an essential contact was formed with the regional and federal level Ministry offices (i.e. The Ministry of Communication and Information Technology (MCIT), the Information Network Security Agency (INSA), and the National Regional State Information and Communication Technology Development offices in each of the cities) and various key personnel in charge of coordinating and managing the implementation of ISSP in Ethiopia. Following this communication we get list of organizations (i.e. 729) that are known or registered by the offices as having ISSP. Since it is not possible to include all of these organizations, we used a random sampling method (i.e. lottery method) to select representative organizations and finally the following are selected: banking and insurance companies in all cities, universities in each of the cities, city administrative offices, and Ethiotelecom offices in some of the cities.

Thus, our sampling frame in Ethiopia includes banking and insurance organizations, universities, city administrative offices and some Ethiotelecom offices that are located in different regions of the country. By conducting a very long and tiresome communication with the human resource department and other concerned bodies in each of the organizations, we managed to get a consent to reach individual respondents. During our communication with the different offices, we tried to make some description about the objective of the study research and we gave them a document that clearly discuss issues, such as: purpose of the research, procedures, risks and benefits, extent of anonymity and confidentiality, compensation, freedom to withdraw, subject's responsibilities, and subject's permission. The consent document is located at Appendix 6. The sampling technique used to select each respondent is a random sampling technique, specifically, the offices gave us the list of employees' names from which we randomly selected some respondents. All respondents received a hand delivered paper-based questionnaire. The reason for the paper-based survey is the web based survey needs the availability of internet connection and email address for each of the respondents, which is difficult to meet this requirement in Ethiopia case. After the

random selection of employees, we directly go to the respondents' offices and provide them with the survey instruments, which is organized into three parts: the first part focused on items that are related to the national culture constructs and also on employees' self-efficacy to comply with their organization ISSP, the second part focuses on the scenario based questions that are related to the constructs of perceived benefits and moral beliefs, and the third part mainly focus on collecting some demographic information about the respondents. The data collection instrument was pilot tested. After handling the questionnaires to the participant, we managed to get back the filled questionnaires almost within 2 months and in between we have made a continual follow-up visits to the respondents which actually help us to increase the response rate. At the end of the data collection process we obtained 210 usable responses, which means 21% response rate, which is more than the minimum requirement.

3.6. PROFILE OF RESPONDENTS

This section details the profiles of the respondents (i.e. in the main survey) in terms of gender, age, educational status, and their location (city) based on their answers to the questionnaire items. The statistics associated with each of these factors is shown in Table 3.1.

Table 3.1: Profile of Respondents

Location				Sex			Age			Educational Status		
Cities	Questionaire Sent	Questionaire Received	Percent	Gender	Frequency	Percent	Age Range	Frequency	Percent	Level	Frequency	Percent
Addis Ababa	237	62	29.52	Male	119	56.7	<30	40	19	Master & Above	33	15.7
Mekele	180	38	18.1	Female	91	43.3	30-40	95	45	First Degree	141	67.14
Dire Dawa	190	34	16.19	Total	210	100	41-50	60	29	Diploma	24	11.43
Bahir Dar	198	39	18.57				>50	15	7	Certificate	12	5.73
Hawassa	195	37	17.62				Total	210	100	Total	210	100
Total	1000	210	100									

Note: In this Table we only include employees whose response is included in the final data Analysis

3.7. DATA ANALYSIS APPROACHES AND TOOLS

In this research, we make use of SEM techniques to test the relationships shown in the research model. According to Kline and Santor (2010), SEM is a very good technique to test construct validity and the theoretical relationship between constructs. In addition, we also conducted a validity and reliability test by using techniques available in AMOS (Analysis of Movement of Structures) and SPSS respectively. To test the different types of relationships shown in our model, we make use of AMOS version 22.

3.8. TREATMENT OF THE DATA

As mentioned in the previous sections, the questionnaires are dispatched through a paper based survey. Before we start the final comprehensive analysis of the response data, we rigorously make sure that the data collected from the main survey is ready and complete by examining issues, such as: examining missing values and outliers, checking normality, testing for common method bias, and estimating the non-response bias. Thus, in the upcoming subsections, we discussed these issues in detail.

3.8.1. Examination of Missing Values and Outliers

In this research, we include all completed questionnaires where data about the dependent, independent, moderator, and demographic data are all completed. After we received the filled out questionnaires from employees' the next step was to deal with missing values and outliers. In this regards, those questionnaires where respondents filled all the questions related to the dependent, moderator, and independent variables are found to be 200 (20%). In addition to this, those respondents who filled every information related to the moderator, independent and dependent variables but failed to complete some demographic information (i.e. years of computer use, and current employment status) are found to be 10 (1%) and we include them for future analysis. On the other hand, we found 30 (3%) questionnaires where more than half of the questions related to the independent and/or moderator variables are missing and thus we exclude them from the response pool. Incomplete questionnaires, which have got many missing values for a number of questions, should be excluded (Alreck and Settle, 2004). Even

though there is no established cutoff point for an acceptable percentage of missing values, Schafer (1999) stated that a missing rate up to 5% is tolerable. Finally, we left with 210 (21%) questionnaires to be ready for further analysis. The next step is to bring all the completed responses from the paper to Excel in order to change the respondents' response to the corresponding numbers on the Likert scale so that it make the data ready to be loaded into SPSS and AMOS for further analysis.

After we loaded the data into SPSS, we conduct analysis to check the existence of outliers in the dataset. Outliers are data values that show a considerable difference from the majority of a set of data. According to Hair et al. (2010), outliers are observations with values for variables that are extremely different from those in other observations. Since this study has many variables, we conducted a multivariate test to check the existence of outliers on two or more variables.

According to Hair et al. (2010), multivariate tests for outliers can be conducted by using the Mahalanobis distance (D^2). Mahalanobis' distance can be thought as a metric of estimating how far each of the individual cases from the center of all the variables' distributions (Starkweather, 2013). To detect an outlier, we should examine the value of D^2, and in this regard, if a particular D^2 value departs considerably from the remaining D^2 values, then we can say that it is an outlier. Particularly, the rule of thumb states that, if the value of D^2 divided by DF (degree of freedom) is greater than 3 or 4 then the case can be considered as an outlier (Hair et al., 2010). Thus, based on this technique, we analyze our dataset and there exists no outliers in the whole data set, the complete result of the Mahalanobis distance is shown at Appendix 7, while Table 3.1 presents the result of the Mahalanobis distance for some of the cases.

Table 3.2: Mahalanobis D^2 Distance Matrix for Selected Cases

Case	D^2	D^2/df	Case	D^2	D^2/df
114	62	2	185	48	1
32	58	2	119	48	1
108	56	2	198	47	1
65	53	2	155	47	1
150	52	2	126	47	1
5	51	2	161	46	1
1	50	2	100	46	1
51	50	2	72	46	1
133	49	1	170	45	1
131	49	1	110	44	1

3.8.2 Test for Normality

As recommended by researchers, before we proceed with the manipulation of the model using the cleaned data, it must be investigated to determine whether or not variables were normally distributed. The dataset needs to be tested if there exists any significant departure from normality, which is a common assumption in multivariate analyses (Hair et al., 2010) According to Field (2009), there exist two main ways in which a distribution can deviate from normal distribution: the first one is lack of symmetry (called skew) and, the second one is pointiness (called kurtosis). A positive skewness result shows positive (right) skew and a negative result shows negative (left) skew. The higher the absolute result, the greater the skewness. In the same way, a positive kurtosis result indicates positive kurtosis (peaked distribution) and a negative one shows negative kurtosis (flatter distribution) and the higher the absolute value will be the greater the kurtosis. According to Field (2009) a distribution with a positive Kurtosis has many scores around the tails and it is called Leptokurtic distribution, while a distribution with a negative Kurtosis is thin in the tails (and it is flatter) and it is called Platykurtic. Even though we can assess the normality of the dataset by using visual inspection of the shape of the variable's distribution using histograms and/or box plots, it is advisable to use statistical approaches with objective and precise techniques. Thus, we used the statistical techniques of skewness and Kurtosis to check the data for normality.

According to Morgan and Griego (1998), if a frequency distribution of a variable shows a big positive or negative skewness and/or kurtosis against their standard error, then we can say that the variable deviates from normality. For both measures, a perfectly normal distribution should return a score of 0, and according to Hair et al. (2006), if we divide either score by its standard error and the absolute value of the result is greater than 1.96 (at .05 significance level) or it is greater than 2.5 (at .01 significance level), it suggests that the data are not normal with respect to that statistic. Other researchers also come up with their own thresholds to judge the normality of a distribution. For example, Bulmer (1979) suggests that if the absolute value of the skewness result is greater than 1 then the distribution is highly skewed, while if it is between 1 and .5 then we can expect a moderate degree of skewness. On the other hand, a kurtosis value between -3 and 3 is considered acceptable in order to prove normal univariate distribution (Bulmer, 1979). As can be seen from Appendix 8, the frequency distribution of each variable in the collected dataset does not violate the normality assumption for all the variables. As an example, Table 3.3 shows the result of the normality check for some of the constructs.

Table 3.3: Test of Normality for Selected Variables

Variables	Skewness[1]	Kurtosis[1]	Variables	Skewness[1]	Kurtosis[1]
CSSE1	-1.82	-0.33	*PB2*	0.43	-1.39
CSSE2	0.27	-1.26	*INT*	2.39	0.21
CSSE3	-0.85	-1.32	*MB1*	-1.8	-0.34
PD1	2.42	0.67	*MB2*	0.17	-1.16
PD2	0.35	-1.4	*MB3*	-0.75	-1.22
PD3	2.45	0.81	*PB3*	-1.6	0.02
PD5	1.34	0.15	*PB4*	-2.42	0.28
UA1	2.25	0.79	*FSS1*	-2.24	0.24
UA2	2.33	0.32	*FSS2*	-2.23	-0.02
UA3	-0.04	-0.45	*SC1*	-2.35	-0.48

[1] Standard error for skewness is .343 and standard error of kurtosis is .674 . The skewness and kurtosis values are critical ratios (Zskewness and Zkurtosis values) i.e. after each skewness and kurtosis value was divided by their respective standard error value.

3.8.3. Estimating Non-response Bias

Non-response bias arises if non-respondents differ from respondents in observable characters (Armstrong and Overton, 1977). Thus, non-response bias might lead to a situation where it will be difficult to generalize the result of a research to the whole population. According to Armstrong and Overton (1977), over the years, the most commonly known and recommended protection against nonresponse bias has been the reduction of nonresponse itself. According to some researchers (e.g. Linsky, 1975; Kanuk and Berenson, 1975), nonresponse can be kept under 30% in most situations if appropriate procedures are followed.

Thus, in this research, we have been working hard to increase the response rate by doing a number of activities, such as: communicating the respondents through follow up emails, and creating a continuous personal contact by directly going to the organizations and sometimes by using telephone communication with respondents. Consequently, we can reduce the non-response rate to much lower number, which is 76%. Following this, we conduct a statistical analysis to find out the impact of non-response bias in the research. Particularly, we conduct a statistical comparison between respondents who respond early and respondents who respond lately. According to Lewis-Beck et al. (2003), those respondents who are interested in the survey would most probably respond earlier than those who are not, and therefore, those who respond lately are assumed not to respond.

We conducted a thorough analysis of the response related to the variables in the model to figure out the statistical difference, if any, between the early respondent and late respondents. In the paper survey, we take the first 50 (24%) and the last 50 (24%) as early and late respondents respectively. According to Kassahun (2012), researchers can use a two sample t-test result to see the statistical difference between two samples. Following this, we conduct analysis of the mean of every variable in the two cases and resulting value serves as a proxy to response bias. The result of this test is shown in Table 3.4. As can be seen from the result, there is no significant statistical difference between the early respondents and late respondents at 95% confidence interval.

Table 3.4: Independent Samples Test Result

	t-test for Equality of Means				
	t	Df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
Intention	-1.580	36	.124	-0.471	0.298
Perceived-benefit	-.302	36	.464	-0.088	0.292
Formal-sanctions	-1.208	36	.236	-0.264	0.219
Shame	-.157	36	.276	-0.049	0.312
Moral-belies	-.360	36	.322	-0.098	0.273

3.8.4. Test for Common Method Bias

Common method bias is defined as variance or systemic error variance shared in the research variables that is caused by the measurement method (Podsakoff et al., 2003). One of the widely used methods to test for common method bias is Harman's single-factor test (Podsakoff et al., 2003) and hence we used this method in our research. In this respect, Table 3.5 shows the result of the exploratory factor analysis (EFA) for the top 11 factors using the unrotated principal component analysis.

As can be seen from the output the biggest factor explains only 22 % of the variance in the measures and this value is less than the minimum percentage (that is >=50%) required to indicate common method bias (Kassahun, 2012). This is a clear indication of the fact that there is no single factor that dominates in explaining the variance in the measures. In Appendix 9, we showed 30 factors that account for 98 % of the variance in the measures.

Table 3.5: Test for Common Method Bias:-Total Variance Explained

Component	Initial Eigenvalues		
	Total	% of Variance	Cumulative %
1	9.902	22.505	22.505
2	4.077	9.266	31.771
3	3.279	7.452	39.224
4	2.757	6.265	45.489
5	2.415	5.488	50.977
6	2.270	5.159	56.136
7	2.195	4.988	61.124
8	1.877	4.266	65.390
9	1.600	3.637	69.027
10	1.484	3.372	72.399
11	1.220	2.774	75.172

3.9. HUMAN SUBJECT APPROVAL

A request for proposal to conduct research involving human subjects was submitted to Virginia Tech University's Institutional Review Board for the Protection of Human Subjects Office of Research Compliance. The office approved the research proposal, data collection instrument and data collection procedures.

3.10. SUMMARY

This chapter discussed the perspective of this research with respect to epistemology, ontology, research methods, and data collection mechanisms. This research takes the view reality as a contextual field of information and hence it is close to the positivist paradigm and it uses the quantitative research method with a survey based data gathering techniques. In addition to this, we discussed the activities accomplished in the research design process, such as: scenario design, instrumentation, sample design, and data analysis tools and techniques. Moreover, in order to make the data ready for the next phase of data analysis, we conducted preprocessing activities, such as: examining missing values and outliers, and checking normality of the

dataset associated with each of the research variables. Moreover, we conducted a pretest, which helps the content validity of the instruments.

In general, we dispatched a large number of questionnaires and before we started the data collection process, we used a recruitment document (Appendix 10) to ask potential respondents if they were willing to contribute their opinions, perceptions, and attitudes to the survey questions concerning to ISSP violation. Those who agreed to participate were given the survey questionnaires (see Appendix 5). The data were collected using paper-based questionnaire.

In the next chapter, we conducted the pilot test by using employees' data obtained from Addis Ababa University and commercial banks, while the final data analysis was conducted by using the main survey data collected from different parts of Ethiopia.

CHAPTER 4

PILOT STUDY AND DATA ANALYSIS

4.1. INTRODUCTION

In the scientific community, one of the important issues that are believed to be thoroughly conducted before the final collection of data is instrument validation. According to Straub et al. (2004), unless researchers sufficiently validate their research instruments, the output of their research will not be acceptable to the larger part of the scientific community. The authors also added that, since IS as a field has a great level of relation with social science or behavioral science disciplines, there are techniques that help researchers to rigorously execute their studies. The rigor of a research refers to the level to which the collected data is the real representation of the latent constructs (Coombs, 1976, as cited in Straub et al., 2004). In this regards, to verify constructs in IS studies, it is a common practice to investigate the reliability and validity of instruments that are used to collect data. If researchers use valid and reliable measures, then the research data can be collected in an objective and appropriate way (Straub, 1990).

In this chapter, we covered the following main topics: first, we made a detailed discussion about the pilot test. Particularly, we explained the activities and steps followed to insure the reliability and validity of the measurement instruments by using data obtained from employees who works in Addis Ababa University and commercial banks. Second, we provide an analysis of the data collected from the main survey (i.e. from cities located across Ethiopia), more specifically, the following tasks are accomplished in the given order: revalidation of the instruments by using the data collected from the main survey, testing the reliability of the instrument items, constructing the structural model that clearly shows the result of hypotheses testing, discussing the result of the hypotheses test, and finally, we summarized the chapter and provide a brief description of what the next chapter covers.

4.2. RELIABILITY AND VALIDITY

Reliability is measurements within the theoretical construct (Straub et al., 2004). Reliability helps to answer the question "to what extent do the instruments that are believed to represent a construct are the error free operationalization of that constructs?" There exist six different types of techniques used to assess reliability: internal consistency, split half, test-retest, alternative form/equivalent form, unidimensional reliability, and inter-rater reliability (Straub et al., 2004, p. 400). In this research, we used internal consistency technique to conduct the reliability test. Coefficient of Cronbach's α is considered to be the most commonly used statistics to assess internal consistence (Straub et al., 2004) and according to Hair et al. (2010), Cronbach's α should be above .7.

Validity refers to the degree to which an instrument measures what it was purported to measure (Field, 2009). Thus, the main goal of validation process is to give a proof for the positivist approach selected as the appropriate means of getting the knowledge we are searching for (Nunnally, 1978). According to Straub et al. (2004), there exist different types of validities tests, including but not limited to: content validity, factorial validity, and construct validity. In the following paragraphs, we discussed the scientific procedures followed to come up with valid and reliable measures or instruments.

4.2.1. Content validity

Content validity is the level to which the elements within a measurement procedure contain the core character of the construct (Straub et al., 2004). According to the authors, if the measures include items that do not represent the construct, it will create a measurement error. In the same way, if the measures exclude items that need to be included, it will also affect the content validity of the instruments (Straub et al.,, 2004). Thus, researchers need to make sure that the instrument items are important and representative of the construct they intend to measure.

According to Straub et al. (2004), the commonly used method of evaluating content validity is through the judgment of POE and literature review. Even though some researchers (e.g. Lawshe, 1975) recommend a statistical approach of testing the content validity; others (e.g. Straub et al.,, 2004) believe that empirical examination of content validity is not required. In addition to this, Straub et al. (2004) argue that since there is no clear and well agreed upon methods to determine the content validity in the positivist science, validating content is a recommended but not mandatory practice in IS.

In this research, we have conducted a procedure that help us to ensure the content validity of the research instruments. In this regards, one of the major tasks accomplished is to make sure that the newly introduced scenario and all the adapted instruments items are based on a thorough literature review. If researchers draw constructs based on the theoretical essence of what they propose to measure, then the content validity can be improved (Straub et al., 2004). In this respect, we clearly and appropriately define and operationalize all the research constructs based on the literature (see section 3.4.3).

The other important task that was conducted to insure the content validity is a pretest of all the research instruments through a POE. As discussed in section 3.4.4 (pretest section), we used a group of ISS experts to go through all the survey instruments to make sure that the survey instruments have a strong content validity. To make sure that the survey instruments do have a very good content validity, they need to pass the experts pretest process (Lewis et al., 2005). Moreover, we also administered the pretest survey to very small subsamples of the sample population. One of the useful pretest is done when researchers pretest their instruments on a subsample of the sample population, because the respondents fit the cultural and demographic profile of the bigger sample to be examined later (Ferketich et al., 1993). Thus, the above procedures show that all the appropriate steps and procedures are followed to ensure content validity.

4.2.2. Construct validity

Construct validity is mainly focused on making sure that all the instrument items that are selected to represent the latent construct to be a reasonable operationalization of that construct (Cronbach and Meehl, 1995). On the other hand, Cook et al. (1979) defined construct validity as the extent to which the measures true score corresponds to the construct it is purporting to measure or operationalize. Basically, construct validly focus on measuring of individual constructs and there exist many types of construct validities tests, and the two main types addressed in this research are discriminant and convergent validities. In the upcoming paragraphs, we discussed scientific procedures followed to make sure that both types of validities are conducted in correct and appropriate way.

Convergent validity is evident when items that are believed to represent a particular construct indeed show a high correlation with themselves relative to their correlation with items of different construct (Straub et al., 2004). In this regards, there exist different methods to test the convergent validity of constructs.

One of the oldest methods of testing convergent validity is using multitrait-multimethod (MTMM) but most researchers in the IS do not base on this method to test for construct validity for a number of reasons (Straub et al., 2004). The first reason is MTMM has a very complex rule of thumb, while the second reason is MTMM is a labor intensive method, because it requires researchers to collect data by using different methods. Due to this and other reasons, currently many researchers in the area of IS mostly use the various types of factor analysis to test for construct validity (Straub et al., 2004). In this regards, convergent validity is accessed by using one or a combination of the following: goodness of fit (GOF) measures, squared multiple correlation (SMC), the average variance extracted (AVE), and construct reliability (CR) (Straub et al., 2004; Hair et al., 2010). After the GOF measures show satisfactory results, the convergent validity is further assessed by using AVE and CR (Hair et al., 2010).

According to Hair et al. (2010) there exists different categories of goodness of fit measures: absolute fit index (Chi-square, goodness of fit index (GFI), adjusted goodness of fit index (AGFI), root mean-square error of approximation (RMSEA), root mean-square residual (RMSR), standardized root mean-square residual (SRMR)), incremental fit index (comparative fit index (CFI), normed fit index (NFI), tucker lewis index (TLI), incremental fit index (IFI)), and parsimonious fit index (parsimony comparative fit index (PCFI), parsimony normed fit index (PNFI)). According to Hair et al. (2010), since there are many measures of goodness of fit, it is a very good approach to select only three or four of the fit index to test how well the theory and the data fit together. The author also added that in reporting research outputs it is recommended at least to include chi-square test, any of the incremental fit index, and any of the absolute fit index.

The other type of construct validity is discriminant validity, and it refers to the degree to which the measurement items that are believed to reflect a construct are different from those that do not make up the construct (Straub et al., 2004). Just like the convergent validity, the classical methodology of testing for discriminant validity is MTMM. Since MTMM has a number of shortcomings, almost current researchers in the area of IS do not use the MTMM (Straub et al., 2004). In this research, we used Confirmatory factor analysis (CFA) to investigate the discriminant validity of the constructs. CFA is one of the most commonly used analytic tools for construct validity (Brown, 2015). The author also added that CFA's result (GFI, NFI, and AGFI) provides a very reliable evidence of discriminant validities. Discriminant validity is said to be strongly held if indicators of different constructs don't have a high inter-correlation (Brown, 2015).

In addition to the above criteria, discriminant validity is also assessed by comparing the AVE value of each factor with the squared inter-factor correlation associated with that factor (Hair et al., 2010). Table 4.1 shows the rule of thumb used to check constructs validity.

Table 4.1: Rule of Thumb for Construct Validities

Validity	Types of measures	Name of the measure	Heuristic	Reference
Convergent validity	Absolute fit indices	GFI, AGFI	GFI> .90, AGFI> .80	Hair et al. (1998) , Hair et al. (2000), Gefen et al.(2000)
		Chi-square(X^2) with df, P	P-value can be less than .05	Hair et al. (2010)
		Normed chi-square(X^2/df)	Value between 1 and 5	Bagozzi et al. (1991)
		RMSEA	Value<.08/.1	Lewis et al. (2005), Hair et al. (2006), Hair et al. (2010)
		RMR	Value< .09	Hair et al. (2010)
		SRMR		
	Parsimony fit indices	PNFI, PCFI	Values>=.5	Hair et al. (2010)
	Incremental fit indices	NFI, TLI, IFI, CFI	Values >= .92	Hair et al. (2010)
	Additional measures	standardized item loading and SMC	standardized item loading should be > .5 preferably >=.7) and SMC from .3 (preferably >=.5)	Hair et al. (2010)
		AVE	Values >=.5	Hair et al. (2010), Holmes-Smith (2010)
		CR	Values >=.6	Hair et al.(2010), Holmes-Smith(2010)
Discriminant Validity	Absolute fit indices	GFI, AGFI	GFI> .90, AGFI> .80	Hair et al. (1998) , Hair et al. (2000), Segars (1997), Gefen et al.(2000)
	Incremental fit indices	NFI	NFI >= .90	Hair et al. (1998) , Hair et al. (2000), Segars (1997), Gefen et al.(2000)

In the following subsections, we present the results of the validity tests for each of the theoretical constructs and then the construct validity of the full measurement model is also presented. For this pilot test we used data collected from employees who work in Addis Ababa University and commercial banks located in Addis Ababa.

4.2.2.1. The Measurement Model of the Power Distance Construct

As can be seen from Appendix 4, this construct has five indicators and Figure 4.1 and Table 4.2 show the result of the proposed measurement model and the goodness fit statistics respectively.

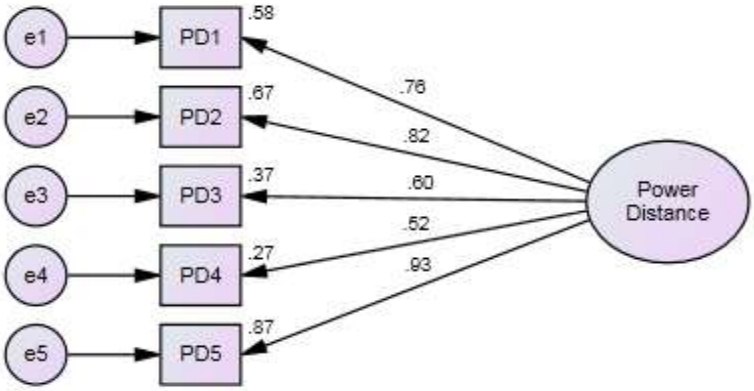

Figure 4.1: The Measurement Model for Power Distance

Table 4.2: Goodness of Fit Statistics for Power Distance

Absolute Fit Index		Incremental Fit Index		Parsimony Fit Index	
X2(P-value)	5.3(.379)	CFI	.997	PCFI	.50
DF	5	IFI	.997	PNFI	.50
X2/DF	1.06	TLI	.994		
RMSEA	.037				
RMR	.016				
SRMR	.05				
GFI	.959				
AGFI	.876				

As can be seen from the result of the measurement model in Figure 4.1, PD4 has SMC value below the minimum threshold (that is below .3) and therefore we removed it from the model. On the other hand, the goodness of fit measure in Table 4.2 clearly shows that all the statistical measures are within acceptable range. Thus, after dropping the item with low SMC (item PD4) from the measurement model, the measurement model is rerun and the resulting measurement model and goodness of fit statistics are shown in Figure 4.2 and Table 4.3 respectively. As can be seen from the output all the SMC values and the goodness of fit statistics show acceptable values.

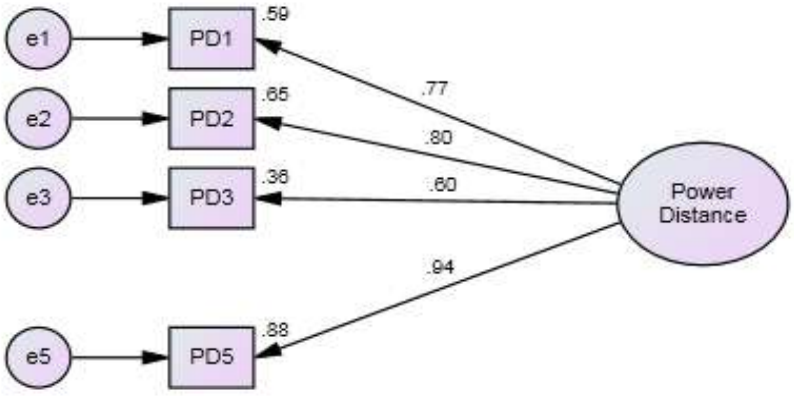

Figure 4.2: The Final Measurement Model for Power Distance

Table 4.3: Goodness of Fit Statistics for Power Distance

Absolute Fit Index		**Incremental Fit Index**		**Parsimony Fit Index**	
X2(P-value)	.374(.829)	CFI	1	PCFI	.53
DF	2	IFI	1.01	PNFI	.52
X2/DF	.0178	TLI	1.06		
RMSEA	.001				
RMR	.006				
SRMR	.01				
GFI	.996				
AGFI	.979				

4.2.2.2. The Measurement Model of the Uncertainty Avoidance Construct

As can be seen from Appendix 4, this construct has six indicators and Figure 4.3 and Table 4.4 show the result of the proposed measurement model and the goodness of fit statistics respectively.

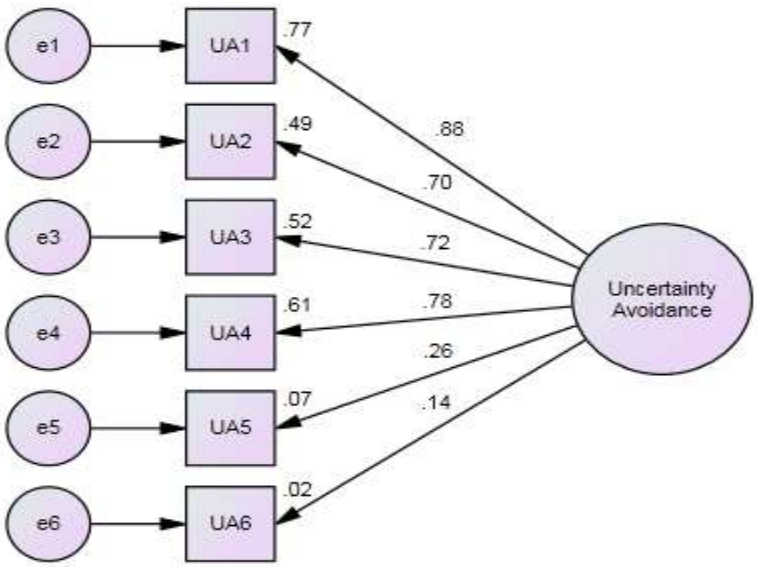

Figure 4.3: The Measurement Model for Uncertainty Avoidance

Table 4.4: Goodness of Fit Statistics for Uncertainty Avoidance

Absolute Fit Index		**Incremental Fit Index**		**Parsimony Fit Index**	
X2(P-value)	17.8 (.08)	CFI	.93	PCFI	.54
DF	9	IFI	.91	PNFI	.50
X2/DF	2	TLI	.83		
RMSEA	.146				
RMR	.05				
SRMR	.08				
GFI	.90				
AGFI	.80				

As can be seen from the result of the measurement model in Figure 4.3, UA5 and UA6 have SMC value below the minimum threshold and therefore we removed them from the model. On the other hand, the goodness of fit measure in Table 4.4, shows that some of the goodness of fit statistical measures (RMSEA, IFI, and TLI) are not within the acceptable range. Thus, after dropping the items with low SMC (item UA5 and UA6) from the measurement model, the measurement model is rerun and the resulting measurement model and goodness of fit statistics are shown in Figure 4.4 and Table 4.5 respectively. The SMC values and the goodness of fit statistics show acceptable values.

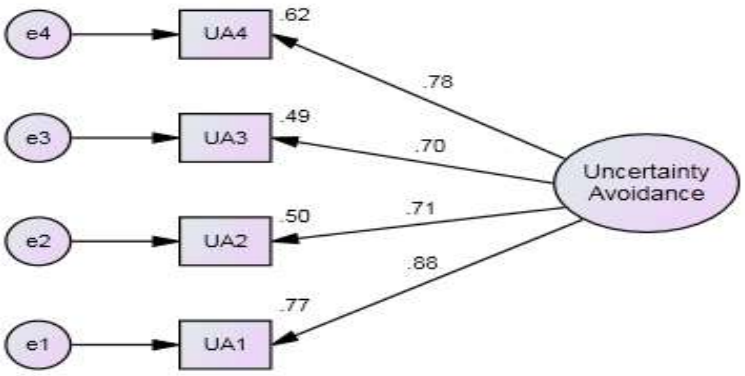

Figure 4.4: The Final Measurement Model for Uncertainty Avoidance

Table 4.5: The Final Goodness of Fit Statistics for Uncertainty Avoidance

Absolute Fit Index		**Incremental Fit Index**		**Parsimony Fit Index**	
X2(P-value)	.717 (.699)	CFI	1	PCFI	.53
DF	2	IFI	1.02	PNFI	.52
X2/DF	2.8	TLI	1.05		
RMSEA	.001				
RMR	.01				
SRMR	.02				
GFI	.99				
AGFI	.96				

4.2.2.3. The Measurement Model of the Collectivism/Individualism Construct

As can be seen from Appendix 4, this construct has six indicators and Figure 4.5 shows the result of the proposed measurement model of this construct, while Table 4.6 shows the goodness of fit statistics.

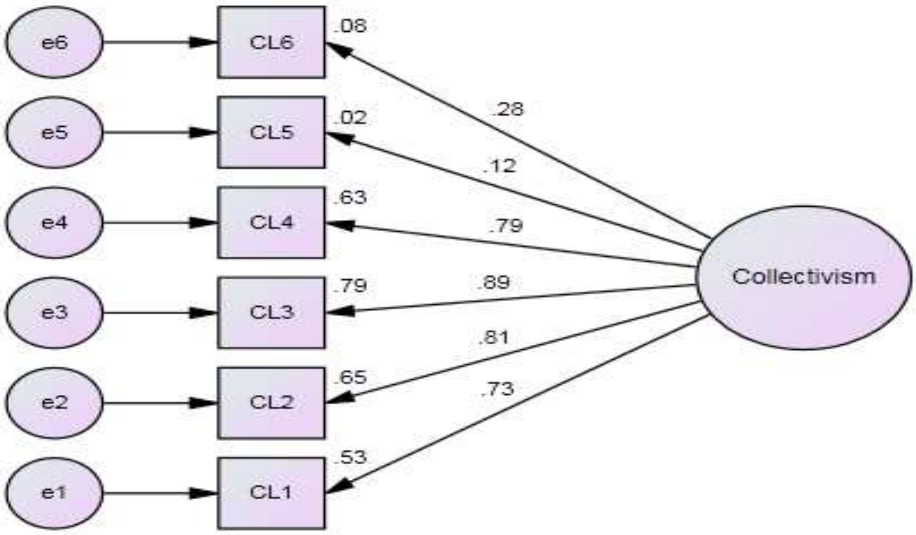

Figure 4.5: The Measurement Model for Collectivism/Individualism

Table 4.6: Goodness of Fit Statistics for Collectivism/Individualism

Absolute Fit Index		**Incremental Fit Index**		**Parsimony Fit Index**	
X2(P-value)	14.9 (.09)	CFI	.94	PCFI	.57
DF	9	IFI	.95	PNFI	.52
X2/DF	1.7	TLI	.90		
RMSEA	.12				
RMR	.07				
SRMR	.08				
GFI	.86				
AGFI	.77				

As can be seen from the result of the measurement model in Figure 4.5, CL5 and CL6 have SMC value below the minimum threshold and therefore we removed them from the model. On the other hand, the goodness of fit measure in Table 4.6, shows that some of the goodness of fit statistical measures (RMSEA, GFI, AGFI, and TLI) are not within the acceptable range. Thus, after dropping the items with low SMC (item CL5 and CL6) from the measurement model, the measurement model is rerun and the resulting measurement model and goodness of fit statistics are shown in Figure 4.6 and Table 4.7 respectively. As can be seen from the output all the SMC values and the goodness of fit statistics show acceptable values.

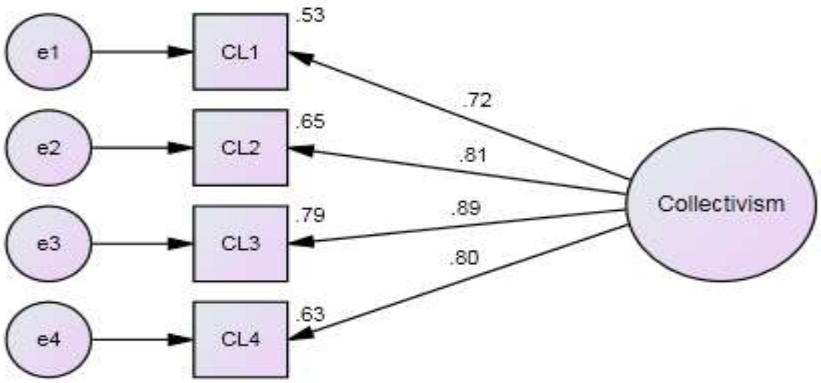

Figure 4.6: The Final Measurement Model for Collectivism/Individualism

Table 4.7: The Final Goodness of Fit Statistics for Collectivism/Individualism

Absolute Fit Index		**Incremental Fit Index**		**Parsimony Fit Index**	
X2(P-value)	.64 (.42)	CFI	1	PCFI	.71
DF	1	IFI	1	PNFI	.56
X2/DF	.64	TLI	1.02		
RMSEA	.001				
RMR	.006				
SRMR	.08				
GFI	.993				
AGFI	.931				

4.2.2.4. The Measurement Model of the Masculine/Feminine Construct

As can be seen from Appendix 4, this construct has four indicators. Figure 4.7 shows the result of the proposed measurement model of this construct, while Table 4.8 shows the goodness of fit statistics.

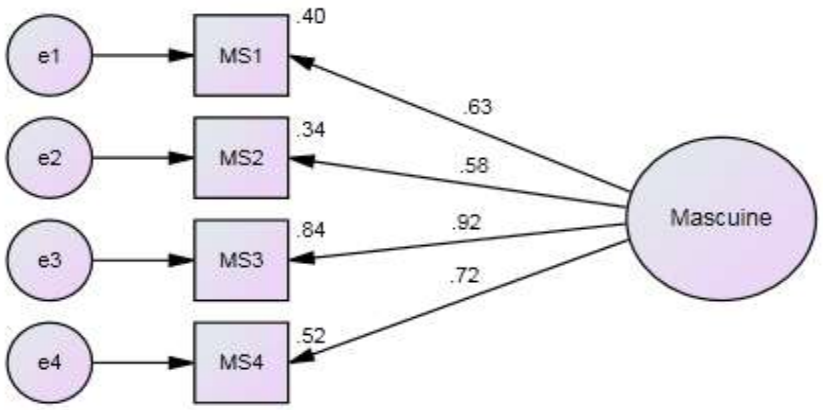

Figure 4.7: The Measurement Model for Masculine/Feminine

Table 4.8: Goodness of Fit Statistics for Masculine/Feminine

Absolute Fit Index		**Incremental Fit Index**		**Parsimony Fit Index**	
X2(P-value)	3.7 (.15)	CFI	.97	PCFI	.63
DF	2	IFI	.97	PNFI	.61
X2/DF	1.85	TLI	.92		
RMSEA	.08				
RMR	.07				
SRMR	.05				
GFI	.96				
AGFI	.81				

The result of the measurement model (Figure 4.7), shows that the all the SMC value are above the minimum threshold. Moreover the goodness of fit statistics shown in Table 4.8 are in the range of acceptable values.

4.2.2.5. The Measurement Model of the Perceived Benefits Construct

As can be seen from Appendix 4, this construct has four indicators. Figure 4.8 shows the result of the measurement model of this construct, while Table 4.9 shows the goodness of fit statistics.

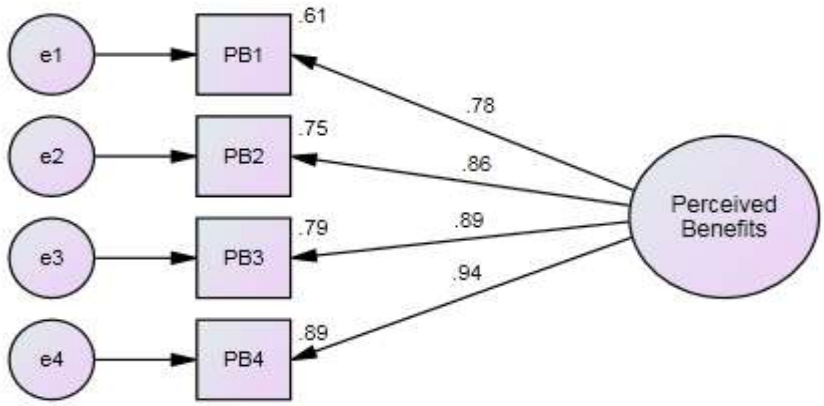

Figure 4.8: The Measurement Model for Perceived Benefits

Table 4.9: Goodness of Fit Statistics for Perceived Benefits

Absolute Fit Index		**Incremental Fit Index**		**Parsimony Fit Index**	
X2(P-value)	5.4 (.07)	CFI	.98	PCFI	.56
DF	2	IFI	.98	PNFI	.52
X2/DF	2.5	TLI	.93		
RMSEA	.09				
RMR	.02				
SRMR	.03				
GFI	.94				
AGFI	.85				

Examination of the goodness of fit statistics and also the values of SMC clearly satisfy the criteria for the minimum thresholds and thus all the results are acceptable.

4.2.2.6. The Measurement Model of the Moral Beliefs Construct

As can be seen from Appendix 4, this construct has three indicators. Figure 4.9 shows the result of the measurement model of this construct, while Table 4.10 shows the goodness of fit statistics.

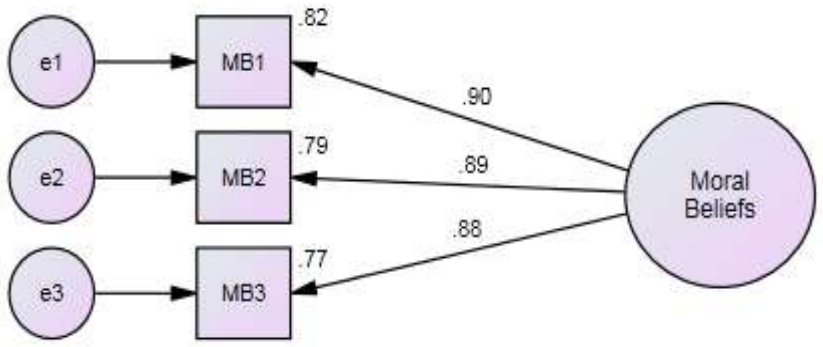

Figure 4.9: The Measurement Model for Moral Beliefs

Table 4.10: Goodness of Fit Statistics for Moral Beliefs

Absolute Fit Index		**Incremental Fit Index**		**Parsimony Fit Index**	
X2(P-value)	3.7 (.15)	CFI	.99	PCFI	.76
DF	2	IFI	.93	PNFI	.62
X2/DF	1.8	TLI	.92		
RMSEA	.09				
RMR	.04				
SRMR	.05				
GFI	.96				
AGFI	.87				

Examination of the goodness of fit statistics in Figure 4.9 indicates that all the values meet the criteria for good model fit. In addition to this, in Table 4.10 the values of SMC satisfy the criteria for the minimum thresholds and thus all the results are acceptable.

4.2.2.7. The Measurement Model of the Shame Construct

As can be seen from Appendix 4, this construct has six indicators and Figure 4.10 shows the result of the proposed measurement model, while Table 4.11 shows the goodness of fit statistics.

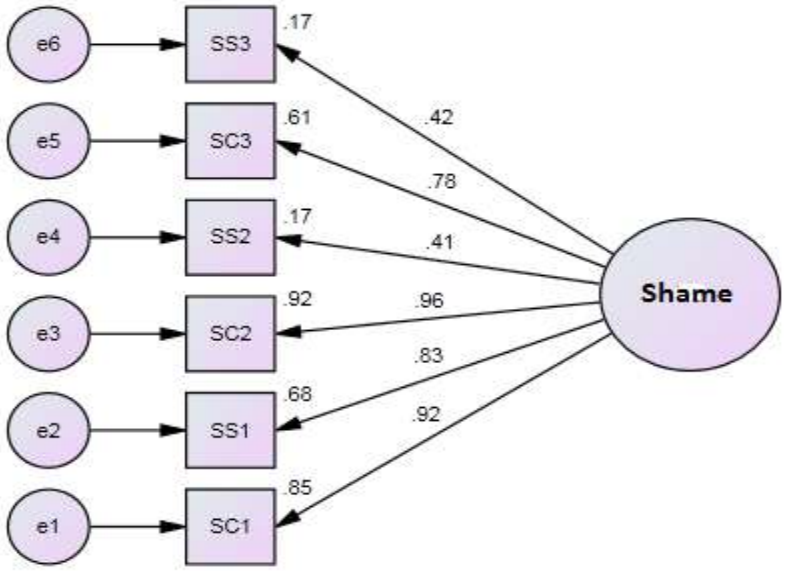

Figure 4.10: The Measurement Model for Shame

Table 4.11: Goodness of Fit Statistics for Shame

Absolute Fit Index		**Incremental Fit Index**		**Parsimony Fit Index**	
X2(P-value)	7.3 (.61)	CFI	1	PCFI	.6
DF	9	IFI	1.01	PNFI	.58
X2/DF	.8	TLI	1.02		
RMSEA	.001				
RMR	.03				
SRMR	.04				
GFI	.95				
AGFI	.86				

As can be seen from the result of the measurement model in Figure 4.10, SS2 and SS3 have SMC value below the minimum threshold and therefore we removed them from the model. On the other hand, the goodness of fit measure in Table 4.11, shows that all the statistics are within the acceptable range of a good model fit. Thus, after dropping the items with low SMC (item SS2 and SS3) from the measurement model, the model is rerun and the resulting output of the proposed measurement model and the goodness of fit statistics are shown in Figure 4.11 and Table 4.12 respectively. As can be seen from the output all the SMC values and the goodness of fit statistics show acceptable values.

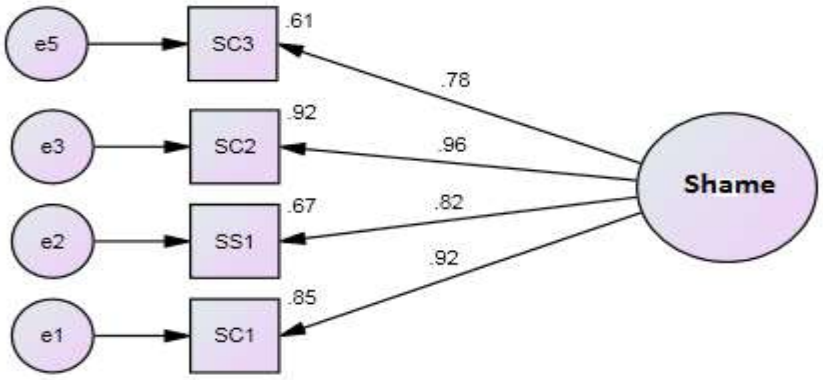

Figure 4.11: The Final Measurement Model for Shame

Table 4.12: The Final Goodness of Fit Statistics for Shame

Absolute Fit Index		**Incremental Fit Index**		**Parsimony Fit Index**	
X2(P-value)	2.44 (.295)	CFI	1	PCFI	.51
DF	2	IFI	1	PNFI	.5
X2/DF	1.22	TLI	.99		
RMSEA	.07				
RMR	.02				
SRMR	.02				
GFI	.98				
AGFI	.89				

4.2.2.8. The Measurement Model of the Formal Sanctions Construct

As can be seen from Appendix 4, this construct has six indicators. Figure 4.12 shows the result of the proposed measurement model of this construct, while Table 4.13 shows the goodness of fit statistics.

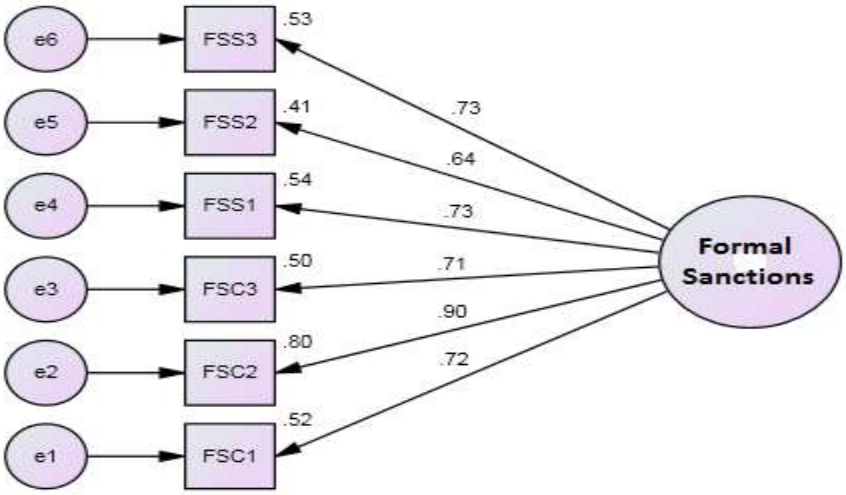

Figure 4.12: The Measurement Model for Formal Sanction

Table 4.13: Goodness of Fit Statistics for Formal Sanctions

Absolute Fit Index		**Incremental Fit Index**		**Parsimony Fit Index**	
X2(P-value)	9.35 (.41)	CFI	1	PCFI	.6
DF	9	IFI	1	PNFI	.56
X2/DF	1.04	TLI	1		
RMSEA	.03				
RMR	.02				
SRMR	.04				
GFI	.94				
AGFI	.87				

Examination of the goodness of fit statistics in Table 4.13 indicates that all the values meet the criteria for good model fit. In addition to this, in Figure 4.12 the values of SMC satisfy the criteria for the minimum thresholds and thus all the results are acceptable.

4.2.2.9. The Full CFA Measurement Model

In the previous section, we have successfully demonstrated how well each and every theoretical construct fit with the collected data. The final step in the process of constructing the measurement model is to bring together all the individual constructs together to come up with a model that helps to assess the validity of the full CFA measurement model. In this regard, the convergent validity of the full measurement model is evaluated based on the goodness of fit statistics, while the discriminant validity of each construct is assessed by comparing the AVE value of every construct with the squared inter construct correlation of that factor (Hair et al., 2010). The author also added that discriminant validity is exhibited if the AVE value is consistently higher than the squared inter factor correlation. In this regards, we assessed the discriminant validity of each and every constructs of the full measurement model. As shown in Figure 4.13 the full measurement model consists of eight latent constructs and 33 items. Table 4.15 presents all the necessary goodness of fit statistics of the full measurement model while Table 4.14 shows the result of the discriminant validity. As can be seen from Table 4.14, all the CR values are within the acceptable range and all AVE values are higher than the squared inter factor correlation and hence discriminant validity is supported.

Table 4.14: Construct Correlation Matrix (Square Root of the AVE on the Diagonal)

	CR	AVE	Power Distance	Perceived Benefit	Masculinity	Formal Sanction	Shame	Moral Beliefs	Collectivism	Uncertainty Avoidance
Power Distance	0.887	0.663	0.814							
Perceived Benefit	0.926	0.760	0.231	0.872						
Masculinity	0.810	0.524	0.244	0.277	0.724					
Formal Sanction	0.881	0.554	-0.237	-0.274	-0.366	0.744				
Shame	0.928	0.765	-0.163	-0.755	-0.384	0.226	0.875			
Moral Beliefs	0.919	0.792	-0.245	-0.693	-0.443	0.124	0.645	0.890		
Collectivism	0.878	0.645	0.277	0.508	0.067	0.015	-0.280	-0.255	0.803	
Uncertainty Avoidance	0.854	0.596	-0.268	-0.189	-0.015	0.299	0.315	0.391	0.082	0.772

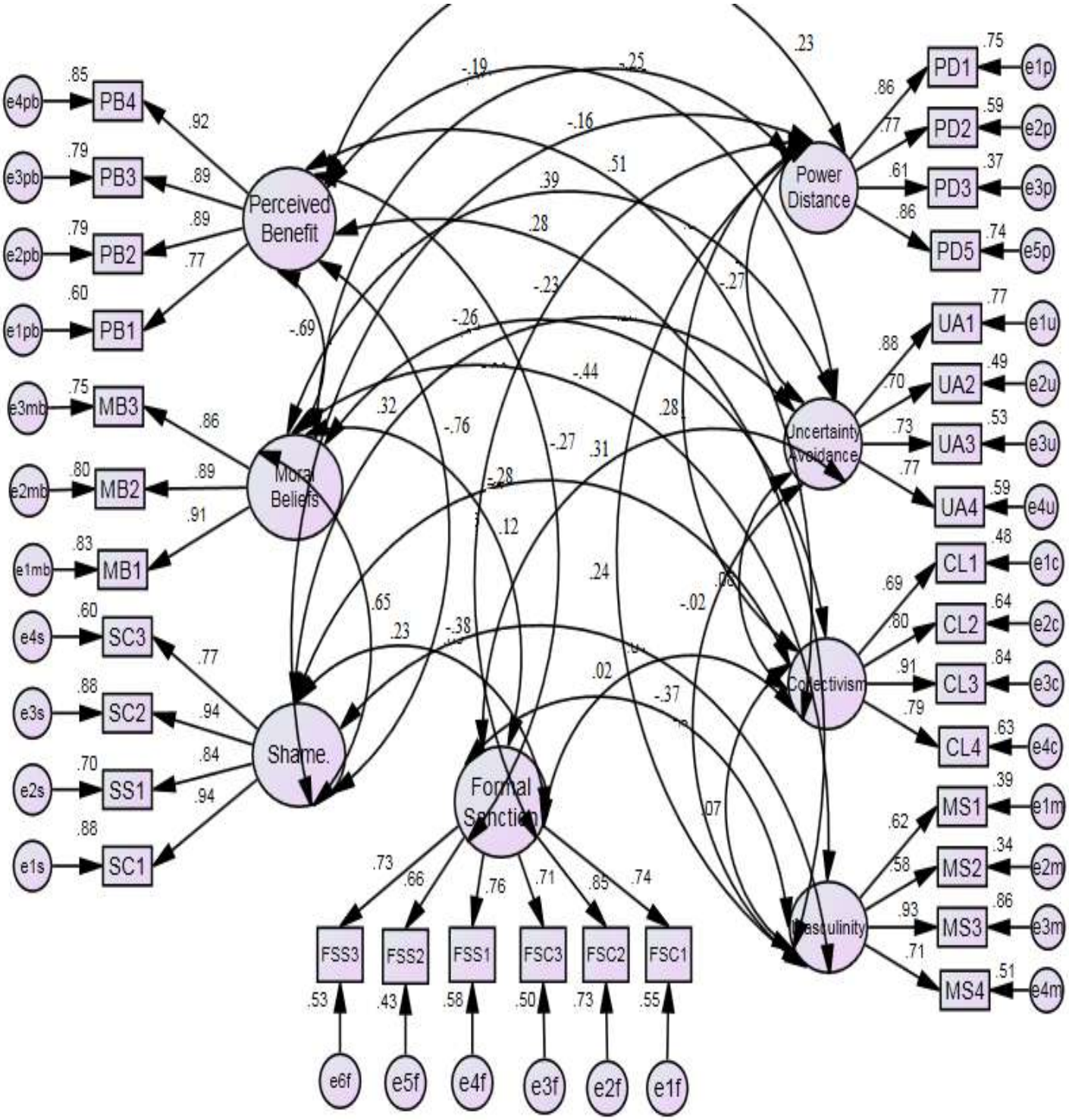

Figure 4.13: The Proposed Full Measurement Model

Table 4.15: Goodness of Fit Statistics for the Full Measurement Model

Absolute Fit Index		**Incremental Fit Index**		**Parsimony Fit Index**	
X2(P-value)	696.6 (.056)	CFI	.93	PCFI	.72
DF	463	IFI	.94	PNFI	.54
X2/DF	1.51	TLI	.92		
RMSEA	.07				
RMR	.05				
SRMR	.08				
GFI	.91				
AGFI	.84				

4.2.3. Final Reliability

Before proceeding with the structural model, researchers should finalize the test for instrument reliability (Straub et al., 2004). Basically reliability measures how consistently instrument items measure a construct of interest and in this regard we used a type of reliability test called internal consistency.

Accordingly, the Cronbach's α is used to test the construct reliability and Table 4.16 shows the result. According to Churchill (1979) a reliability alpha of .5 or .6 is considered to be satisfactory for studies in its early stage, while Hair et al. (2010) stated that a Cronbach's α of .7 or more is the commonly accepted threshold. As can be seen from Table 4.16 all the values are greater than the minimum value and hence construct reliability is satisfied.

Table 4.16: Instrument Reliability

Constructs	No of Items	Cronbach's α Value
Power Distance	4	.86
Uncertainty Avoidance	4	.85
Collectivism	4	.88
Masculine	4	.81
Perceived Benefits	4	.93
Moral Beliefs	3	.92
Shame	4	.93
Formal Sanction	6	.88

4.3. DATA ANALYSIS AND RESULT

In this section, we provide a detailed analysis of the data collected from the main survey. As discussed in the third chapter (section 3.8) the data collected from the main survey has passed a series of preliminary processing steps. More specifically, the following tasks are accomplished in the given order: revalidation of the instruments by using the data collected from the main survey, testing the reliability of the instrument items, and constructing the structural model that clearly shows the result of hypotheses testing.

4.3.1. The Measurement Model of the Power Distance Construct

After the pilot test (initial construction of the measurement model) was completed, the power distance construct left with four indicators that do have factor loadings above the minimum value (see Appendix 11). In this section, we conducted CFA for the data obtained from the main survey (210 cases). As can be seen from Figure 4.14, the result of the measurement model for the main survey shows that all the indicators SMC values are above the minimum threshold value of .3 (Preferably .5) as defined by Hair et al. (2010). The results of selected model fit statistics are shown in Table 4.17 and the remaining statistical details are shown at Appendix 12.

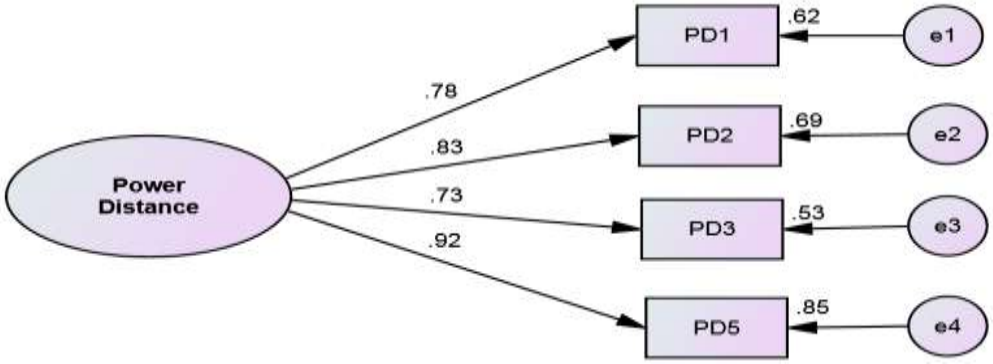

Figure 4.14: The Measurement Model of Power Distance Construct for the Main Survey

Table 4.17: The Goodness of Fit Statistics of Power Distance construct for the Main Survey

Absolute Fit Index		**Incremental Fit Index**		**Parsimony Fit Index**	
X2(P-value)	5.5(.066)	CFI	.993	PCFI	.513
DF	2	IFI	.993	PNFI	.512
X2/DF	2.73	TLI	.980		
RMSEA	.091				
RMR	.006				
SRMR	.015				
GFI	.988				
AGFI	.938				

As can be seen from Table 4.17, all the statistical measures are within acceptable range.

4.3.2. The Measurement Model of the Uncertainty Avoidance Construct

As can be seen from Appendix 11, after the pilot test was conducted, the uncertainty avoidance construct left with four indicators. By using the data obtained from the main survey, we construct the measurement model shown in Figure 4.15. The result of the goodness of fit statistics is also shown in Table 4.18 and the remaining statistical details are shown at Appendix 12.

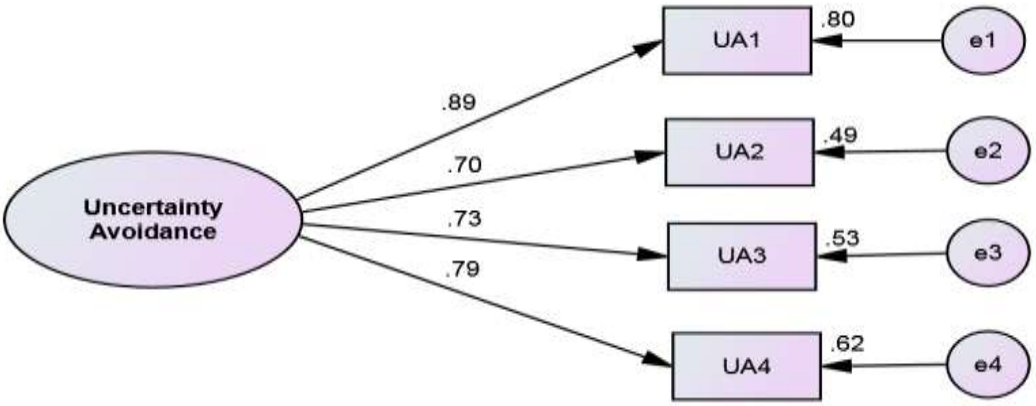

Figure 4.15: The Measurement Model of Uncertainty Avoidance Construct for the Main Survey

Table 4.18: The Goodness of Fit Statistics of Uncertainty Avoidance construct for the Main Survey

Absolute Fit Index		**Incremental Fit Index**		**Parsimony Fit Index**	
X2(P-value)	8.24 (.16)	CFI	.979	PCFI	.64
DF	2	IFI	.980	PNFI	.63
X2/DF	4.12	TLI	.938		
RMSEA	.09				
RMR	.01				
SRMR	.03				
GFI	.98				
AGFI	.91				

As can be seen from the result of the measurement model, all SMC values are above the minimum threshold value and therefore the proposed measurement model is accepted. The goodness of fit measures in Table 4.18 clearly shows that all the selected statistics are within acceptable range.

4.3.3. The Measurement Model of the Collectivism/Individualism Construct

As can be seen from Appendix 4, collectivism/individualism construct used to have six indicators. After the pilot test was conducted this construct left with four final indicators (see Appendix 11) that satisfy the minimum SMC value. In this section we constructed the

measurement model and the goodness of fit statistics of this construct by using the data collected from the main survey. Figure 4.16 shows the result of the proposed measurement model of this construct, while Table 4.19 shows the goodness of fit statistics. Additional statistical details of this construct are shown at Appendix 12.

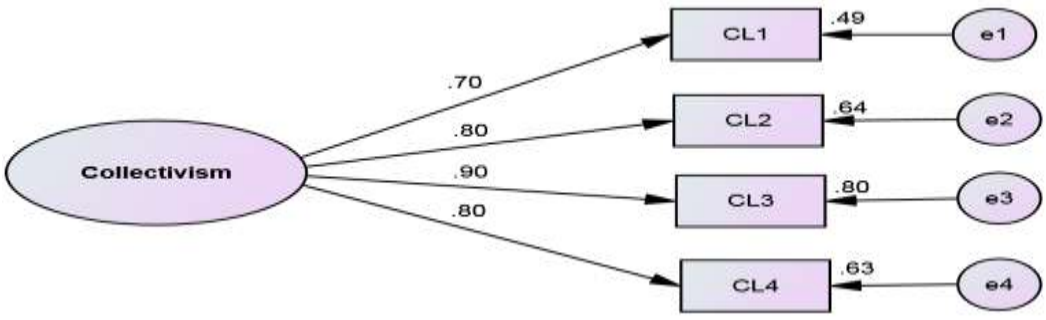

Figure 4.16: The Measurement Model of Collectivism Construct for the Main Survey

Table 4.19: The Goodness of Fit Statistics of Collectivism construct for the Main Survey

Absolute Fit Index		**Incremental Fit Index**		**Parsimony Fit Index**	
X2(P-value)	8.9 (.067)	CFI	.936	PCFI	.61
DF	2	IFI	.937	PNFI	.6
X2/DF	4.45	TLI	.90		
RMSEA	.06				
RMR	.02				
SRMR	.05				
GFI	.934				
AGFI	.81				

As can be seen from the result of the measurement model all indicators do have SMC value above the minimum threshold and all the goodness of fit statistics are in acceptable range.

4.3.4. The Measurement Model of the Masculine/Feminine Construct

As can be seen from Appendix 4, the Masculine/Feminine construct used to have four indicators and all of them pass the validation test and become part of the final instrument set (Appendix 11). Figure 4.17 shows the result of the proposed measurement model of this construct, while Table 4.20 shows the goodness of fit statistics. Additional statistical details of this construct are shown at Appendix 12.

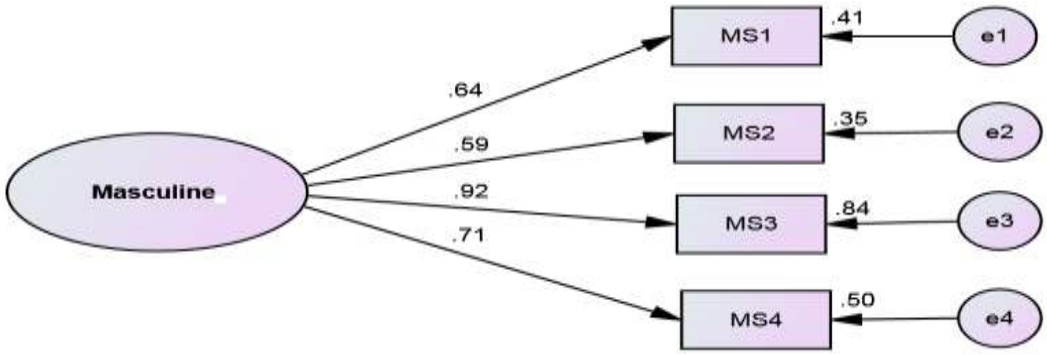

Figure 4.17: The Measurement Model of Masculine Construct for the Main Survey

Table 4.20: The Goodness of Fit Statistics of Masculine construct for the Main Survey

Absolute Fit Index		**Incremental Fit Index**		**Parsimony Fit Index**	
X2(P-value)	9.7 (.25)	CFI	.95	PCFI	.51
DF	2	IFI	.95	PNFI	.50
X2/DF	4.85	TLI	.93		
RMSEA	.09				
RMR	.01				
SRMR	.04				
GFI	.96				
AGFI	.80				

The result of the measurement model shows that the all the SMC values are above the minimum threshold and the goodness of fit statistics are also in the acceptable range.

4.3.5. The Measurement Model of the Perceived Benefits Construct

The perceived benefits construct has four indicators (see Appendix 4) and all of them pass the validation test (see Appendix 11). By using the data collected from the main survey, we constructed the measurement model as well as the goodness of fit statistics for the perceived benefits construct. Figure 4.18 shows the result of the proposed measurement model of this construct, while Table 4.21 shows the goodness of fit statistics. Additional statistical details about this construct are shown at Appendix 12.

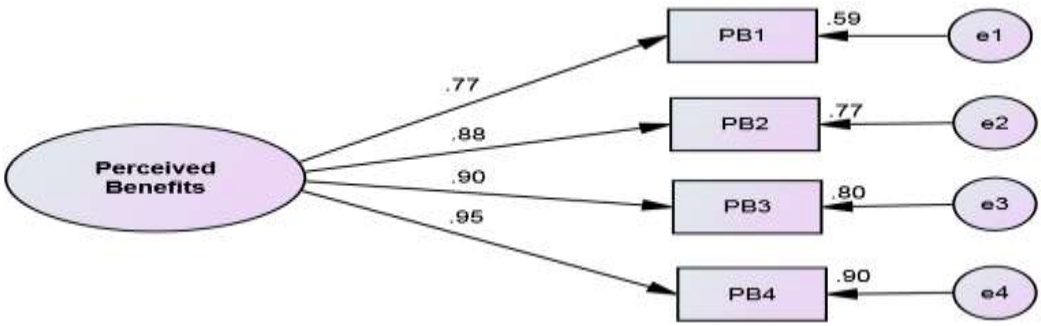

Figure 4.18: The Measurement Model of Perceived Benefits Construct for the Main Survey

Table 4.21: The Goodness of Fit Statistics of Perceived Benefits for the Main Survey

Absolute Fit Index		Incremental Fit Index		Parsimony Fit Index	
X2(P-value)	9.23 (.27)	CFI	.98	PCFI	.55
DF	2	IFI	.98	PNFI	.54
X2/DF	4.6	TLI	.93		
RMSEA	.07				
RMR	.01				
SRMR	.03				
GFI	.97				
AGFI	.85				

Examination of the goodness of fit statistics and also the values of SMC clearly satisfy the criteria for the minimum thresholds set for a good model and thus all the results are acceptable.

4.3.6. The Measurement Model of the Moral Beliefs Construct

This construct initially represented by three indicators (see Appendix 4) and after the pilot test was conducted it left with same number of items. In this section we run the final data obtained from the main survey and we found out that all the statistical outputs satisfy the criteria for a good model and hence all the items are included for further analysis. Figure 4.19 shows the result of the proposed measurement model, while Table 4.22 shows the goodness of fit statistics. Additional statistical details about this construct are shown at Appendix 12.

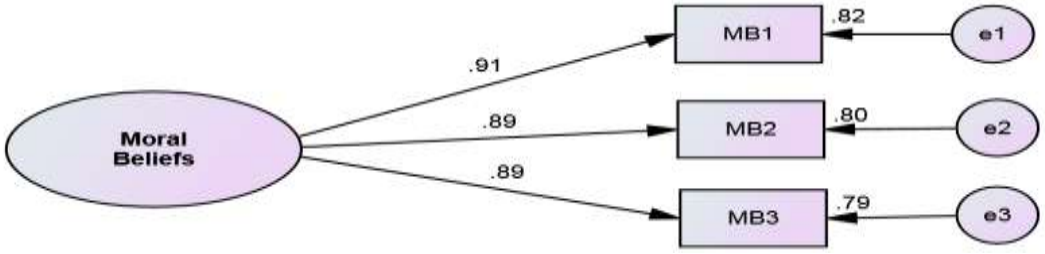

Figure 4.19: The Measurement Model of Moral Beliefs Construct for the Main Survey

Table 4.22: The Goodness of Fit Statistics of Moral Beliefs for the Main Survey

Absolute Fit Index		**Incremental Fit Index**		**Parsimony Fit Index**	
X2(P-value)	3.7 (.15)	CFI	.99	PCFI	.76
DF	2	IFI	.93	PNFI	.62
X2/DF	1.8	TLI	.92		
RMSEA	.09				
RMR	.04				
SRMR	.05				
GFI	.96				
AGFI	.87				

4.3.7. The Measurement Model of the Shame Construct

This construct initially represented by six indicators (Appendix 4) but after the pilot test we found out that there are four indicators (see Appendix 11) that do have SMC values greater than the minimum value. In this section, we took all the data obtained from the main survey to retest the measurement model and the goodness of fit statistics of the shame construct. Figure 4.20 shows the result of the proposed measurement model of this construct, while Table 4.23 shows the goodness of fit statistics. Additional statistical details of this construct are shown at Appendix 12.

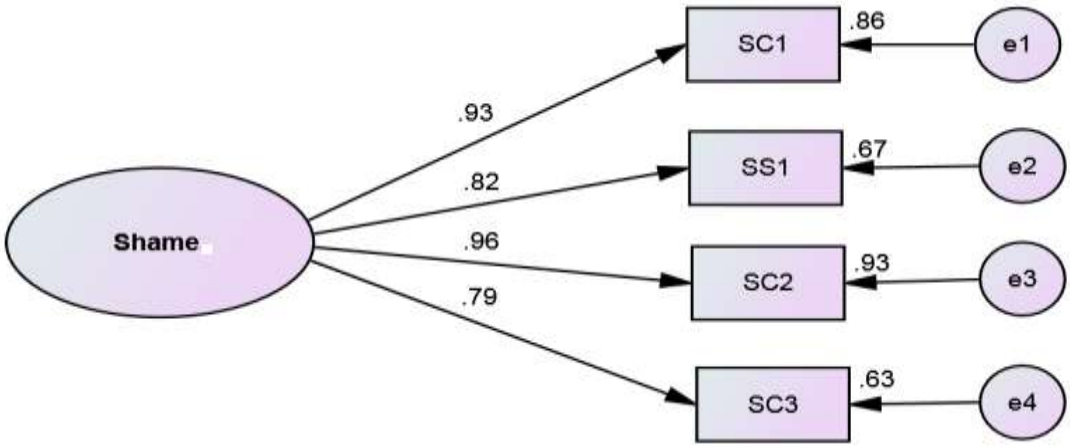

Table 4.23: The Goodness of Fit Statistics of Shame Construct for the Main Survey

Figure 4.20: The Measurement Model of Shame Construct for the Main Survey

Absolute Fit Index		**Incremental Fit Index**		**Parsimony Fit Index**	
X2(P-value)	1.12 (.57)	CFI	1.000	PCFI	.63
DF	2	IFI	1.002	PNFI	.63
X2/DF	.56	TLI	1.005		
RMSEA	.00				
RMR	.006				
SRMR	.007				
GFI	1				
AGFI	.99				

All indicators do have SMC value above the minimum threshold (see Figure 4.20) and therefore we accept the proposed measurement model. The goodness of fit measure in Table 4.23, shows that all the statistical values are within acceptable range of a good model fit.

4.3.8. The Measurement Model of the Formal Sanctions Construct

As can be seen from Appendix 11 all of the six indicators of the formal sanction construct pass the validation process. Similar to what we did for the other constructs, we rerun the measurement model by using the data collected from the main survey. Figure 4.21 shows the result of the proposed measurement model of this construct, while Table 4.24 shows the goodness of fit statistics. Additional statistical details about this construct are shown at Appendix 12.

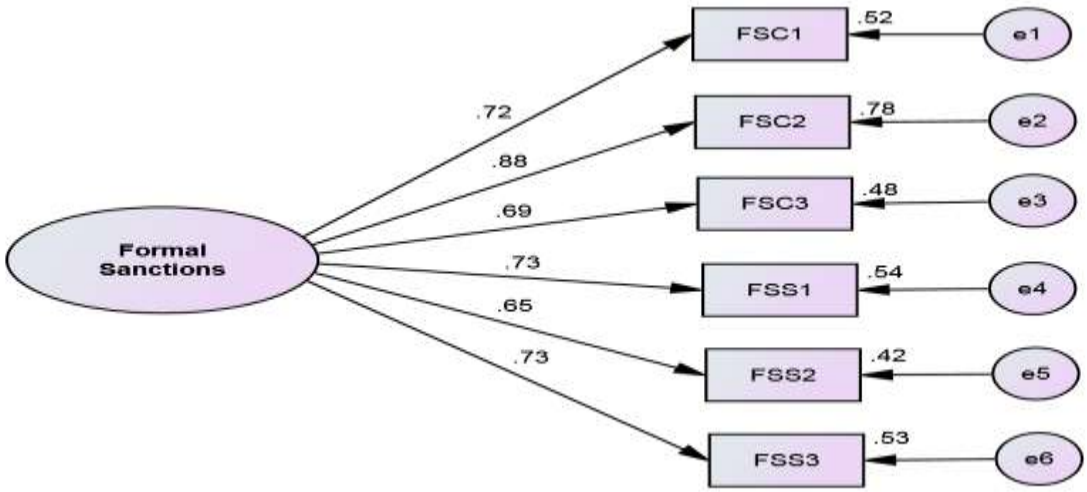

Figure 4.21: The Measurement Model of Formal Sanction Construct for the Main Survey

Table 4.24: The Goodness of Fit Statistics of Formal Sanction Construct for the Main Survey

Absolute Fit Index		**Incremental Fit Index**		**Parsimony Fit Index**	
X2(P-value)	44.2 (.84)	CFI	.94	PCFI	.57
DF	9	IFI	.95	PNFI	.56
X2/DF	4.9	TLI	.92		
RMSEA	.08				
RMR	.02				
SRMR	.04				
GFI	.93				
AGFI	.84				

Examination of the goodness of fit statistics in Table 4.24 indicates that all the values meet the criteria for good model fit. In addition to this, in Figure 4.21 the values of SMC satisfy the criteria for the minimum thresholds and thus all the results are acceptable.

4.3.9. The Full CFA Measurement Model

By using the data collected from the main survey, we show how the theoretical constructs fit with the collected data. Now we proceed to the final stage of constructing the measurement model: bringing together all the individual theoretical (latent) constructs shown in the previous sections so that we can assess the validity of the full CFA measurement model. In this regard, the convergent validity of the full measurement model is evaluated based on the goodness of fit statistics, while the discriminant validity of the theoretical construct is 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 constructs shown in the full measurement model. As shown in Figure 4.22 the full measurement model consists of eight constructs and 33 items. In addition to this, Table 4.26 presents all the necessary goodness of fit statistics of the full measurement model while Table 4.25 shows the result of

the discriminant validity. All the CR values are within the acceptable range and all AVE values consistently higher than the squared inter factor correlation and hence discriminant validity is supported.

Table 4.25: 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

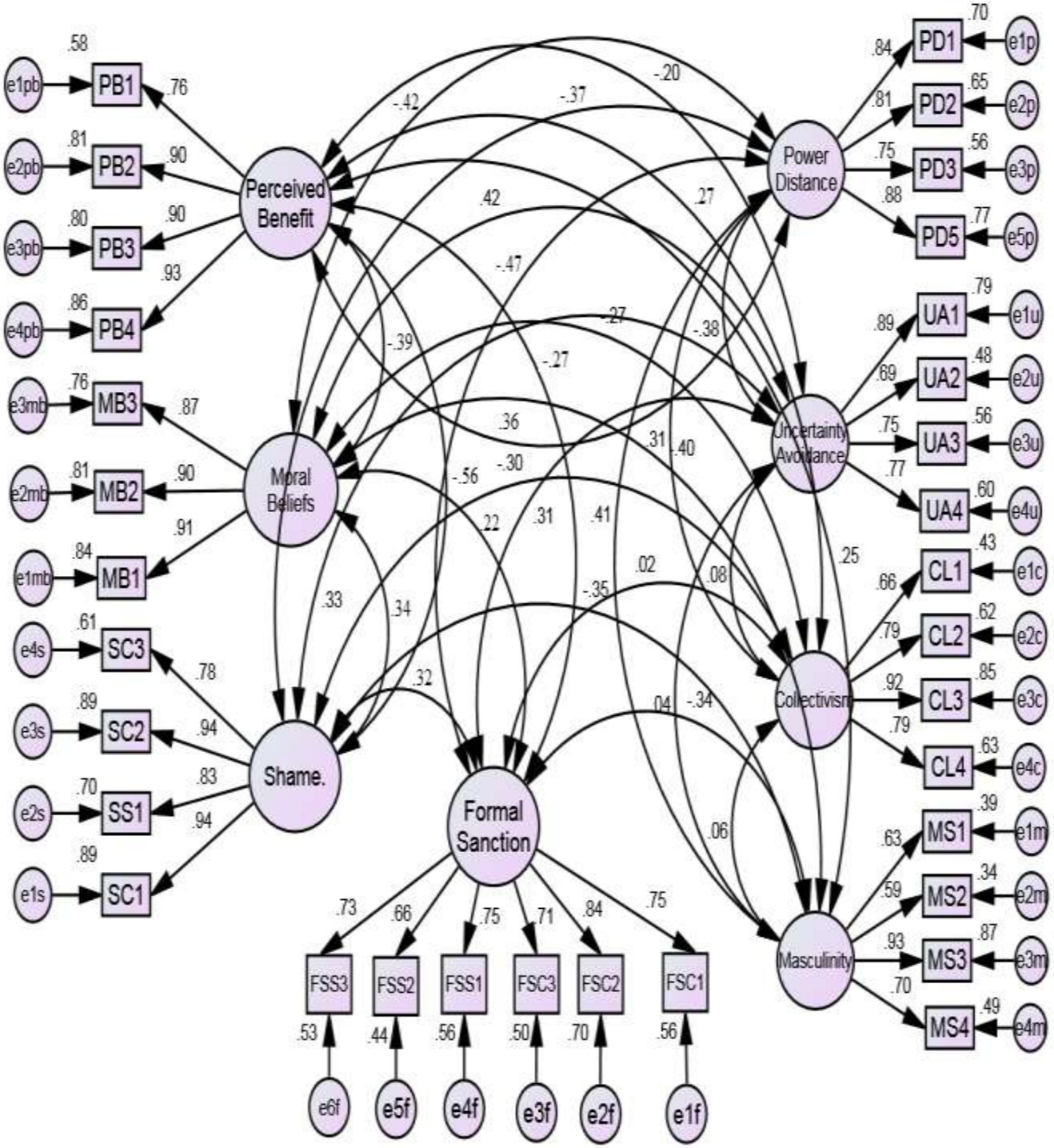

Figure 4.22: The Proposed Full Measurement Model for the Main Survey

Table 4.26: 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				

4.3.10. Final Reliability

In this section, we conducted 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 instrument reliability test (Straub et al., 2004). Reliability measures how consistently instrument items measure a construct of interest and in this regard we used a type of reliability test called internal consistency.

In this regards, the Cronbach's α is used to test the construct reliability of every constructs and Table 4.27 shows the result. According to Hair et al. (2010), a Cronbach's α of .7 or more is the commonly accepted threshold. As can be seen from Table 4.27, all the values are greater than the minimum value and hence the internal consistency of instruments or construct reliability is satisfied.

Table 4.27: Instrument Reliability

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

4.4. RESEARCH FINDINGS

Once the validity and reliability of the measurement model is checked, the next step is to test the structural model. Hence, in this section we focused on assessing the structural model, which is testing the relationship between the theoretical constructs shown on the research model. We used the SEM methodology for representing, estimating, and testing the network of relationships between the theoretical constructs. In addition, we presented and discussed the main findings of the research against the research questions shown in the second chapter. Thus, in the upcoming sections we discussed the following topics in detail: in section 4.4.1 we presented the final result of the structural model validity and hypotheses testing, while in section 4.5 we discussed the findings of the research, and finally in section 4.6 we summarized and conclude the chapter.

4.4.1. Assessment of the Structural Model Validity and Hypotheses 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 fit the reality or the collected data (Suhr, 2006). Thus, to evaluate the validity of the structural model we used different types of statistical tests available in SEM.

As clearly shown in the process of constructing the full measurement model, we depicted how well each of the theoretical constructs relates or correlate with each other. But the correlation shown on 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 regards, a measurement model could only be taken as a first step towards constructing the structural model (Hair et al., 2006). Since we have already finalized 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) Analyzing the goodness of fit statistics based on established criteria (see Table 4.1); (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) stated that the significance level of a parameter estimate should be less than .05. Figure 4.23 shows the theoretical structural model of the research.

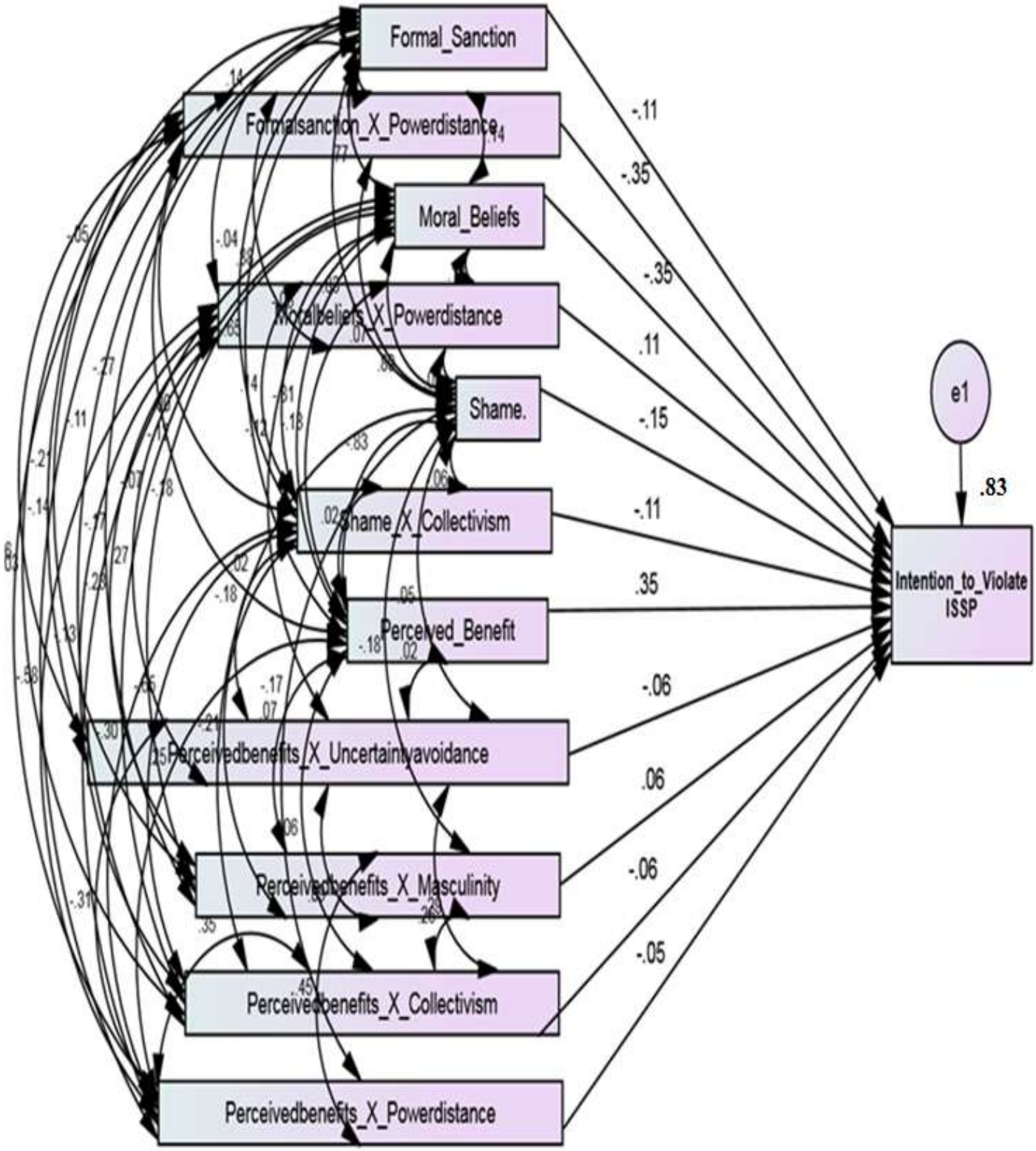

Figure 4.23: The Full Structural Model

We evaluated the structural model against the three criteria. Table 4.28 shows the goodness of fit for the whole structural model.

Table 4.28: The Goodness of Fit Statistics for the Structural Model

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

As can be seen from the goodness of fit statistics in Table 4.28, all the values satisfy the criteria for a good model. The Chi-square value of 292.2 (at P>.05) with 75 degree of freedom indicates good fit. With respect to the absolute fit index, all the statistics meet the minimum requirements (GFI>.90, AGFI>.80, RMR and SRMR <.09, and RMSEA <.08/.1) and the incremental fit index statistics (IFI, TLI, and CFI) do have values greater than or equal to .92. While the parsimonious fit indices (PCFI and PNFI) score above .5. 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. Figure 4.24 shows that 83% 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 standardized factor loadings,

the direction of the relationships, and the level of significance. To this end, Figure 4.24 and Table 4.29 shows these statistics.

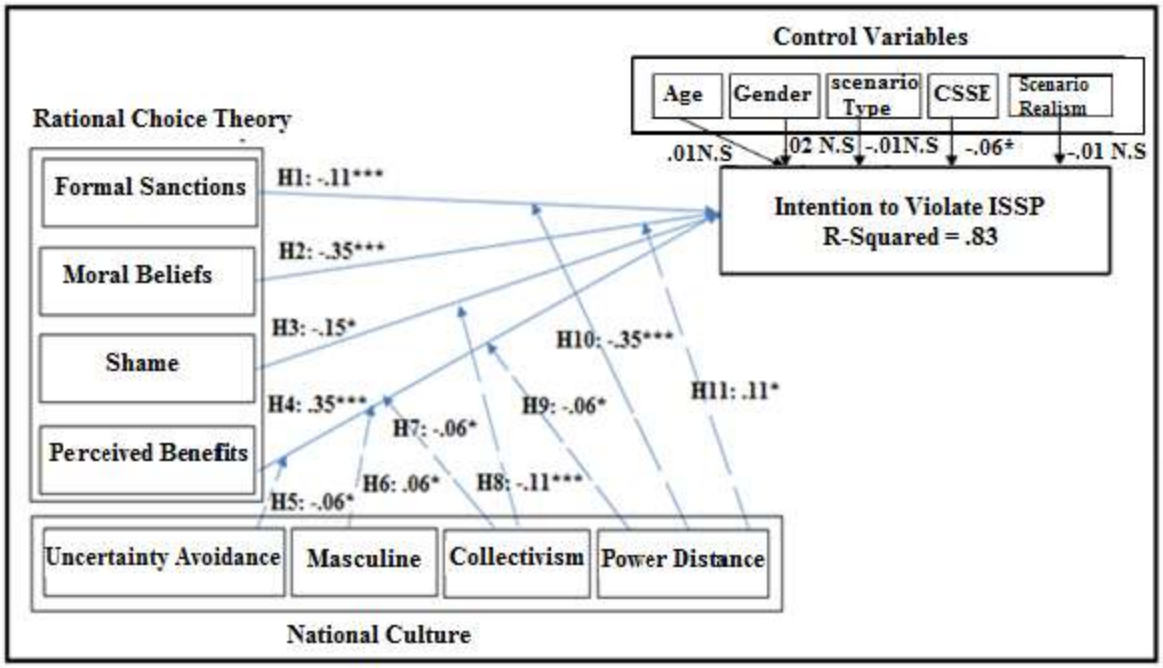

Figure 4.24: The Final Path diagram for the Research Model

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

Table 4.29: The Result from the Final Structural Diagram

Path	Hypothesis	Standardized 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	-0.06	0.026	-2.003	0.018
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

All the stated hypotheses except three are found to be significant at least at 95% confidence interval and hence they are accepted. On the other hand, Hypotheses 7, 9 and 10 are found to be significant, but in the opposite direction to what was stated in the research.

4.5. DISCUSSION

In this section, we discussed 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 formal sanctions, perceived benefits, moral beliefs, and shame on employees' intention to violate ISSP. By using a sample of data collected from organizations in Ethiopia, we found a 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 organizations 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 organization ISSP. As indicated in the IS literature, there exist inconsistent findings concerning the impact of formal sanctions on reducing computer abuse or IS misuse (D'Arcy and Herath, 2011). Despite this confusion, the result of our study is consistent with some research outputs in the area of criminology (e.g. Paternoster and Simpson, 1996; Pratt et al., 2006) and, more importantly, in the ISS area. For example, previous studies reported the ability of formal sanctions to reduce IS misuse intention (D'Arcy et al., 2007), unauthorized access intention (D'Arcy and Hovav, 2009), ISSP non-compliance (Siponen et al., 2007), 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 countries.

Second, moral belief is found to have a strong negative impact on employees' intention to violate their organization's ISSP. This means as employees have strong moral beliefs or commitment, they will intend not to violate their organization's ISSP. This finding is not only consistent with the basic principle of RCT (Becker, 1968) but also with criminological studies, which reported that people with low moral beliefs or personal norms are more incline to engage in a deviant behavior like corporate crime (Paternoster and Simpson, 1996), tax evasion (Wenzel, 2004). Further, research outputs in psychology (e.g. Blasi, 1980; King and Mayhew, 2002; Rest, 1986, as cited in Myyry et al., 2009) also reported that good moral reasoning helps people to develop desirable behavior. More importantly, in the area of ISS, personal norm (Li et al., 2010) and moral belief (Siponen and 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 organization ISSP. This result indicates that as employees feel that violating ISSP is a shameful activity, then they will distance themselves from such act. When we compare our finding against previous studies, it is consistent with studies in the criminology literature (e.g. Grasmick and Bursik, 1990; Nagin and Paternoster, 1993; Tibbetts, 1997).

But when we come to ISS literature, we can only find a single empirical study by Siponen and Vance (2010) that investigated the impact of shame as a deterrent construct and in that same study they reported the inability of shame to reduce employees' noncompliance to their organization ISSP. A plausible reason for the contradiction of our finding with Siponen and Vance (2010) might be due to the difference in the cultural makeup of the sample respondent in the two studies. In this respect, our sample was taken from a more collective society where violating of norms leads to shame feeling while Siponen and Vance (2010) sample was taken from individualistic society (Finland) where breaking norms resulted in guilty feeling 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 of their organization ISSP helps them to achieve some sort of benefits, then they will most probably engage in violating those rules. This finding is similar to what the RCT states: when people make choice they analyze 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 also consistent with empirical studies in ISS literature: Vance and Siponen (2012) reported the significant positive impact of perceived benefits on employees' intention to violate ISSP, while Li et al. (2010) reported a significant negative influence of perceived benefits on employees' compliance intention to internet use policy.

Hypothesis 5 proposed that "The higher the degree of uncertainty avoidance, the weaker the impact of perceived benefits is on employees' intention to violate ISSP" and as can be seen from figure 4.25, this hypothesis is supported. This means that, even though the perceived

benefits of noncompliance initiate employees to violate their organization's ISSP, the strength of this relationship is weaker for high uncertainty avoidance employees than their low uncertainty avoidance counterparts. In this regards, studies in the area of sociology (e.g. Hofstede, 2003, 2011) found that people who score high in uncertainty avoidance give a primary emphasis for the enforcement of rules and regulation than their low uncertainty avoidance counterparts. If we bring this same scenario to ISS, we might incline to say that low uncertainty avoidance employees might violate their organization'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 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 study the moderating influence of uncertainty avoidance in the relationship between perceived benefits and employees' intention to violate ISSP.

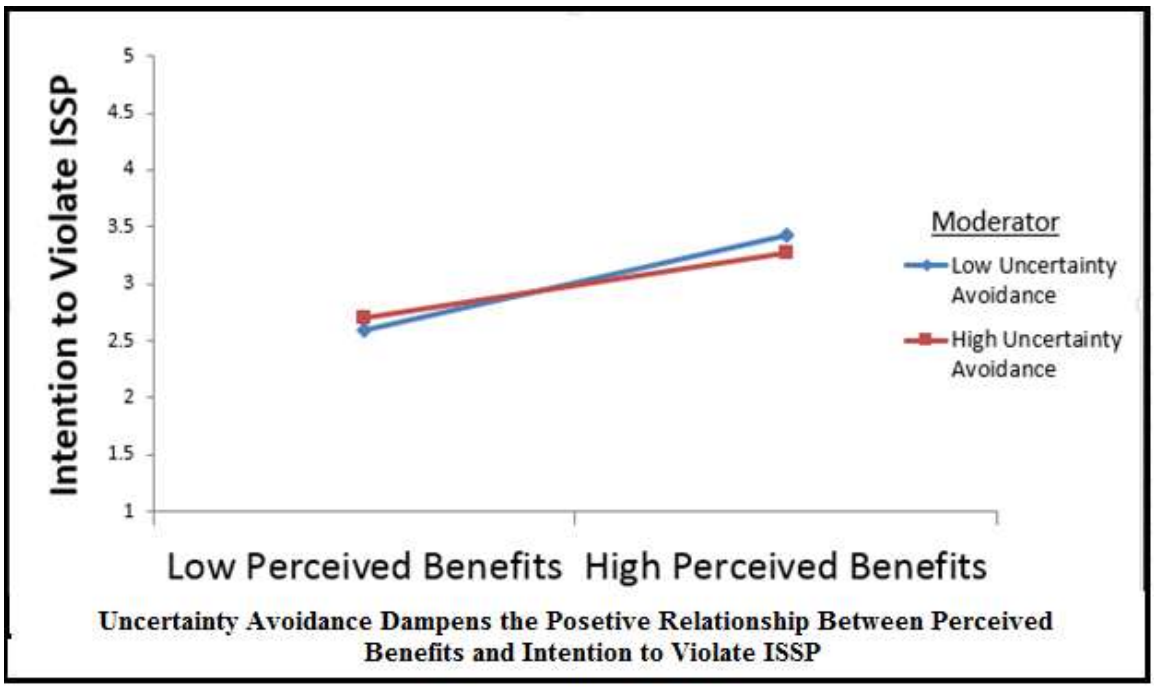

Figure: 4.25: Interaction Effect Between Perceived Benefits and Uncertainty Avoidance

When we come to the sixth hypothesis, it proposed that "The higher the degree of masculine, the stronger the impact of perceived benefits is on employees' intention to violate ISSP". As can be seen from Figure 4.26, it is supported. The finding of this research is consistent with conceptual cultural studies in the field of sociology. For example, Hostede (2001) stated that for people in high masculine society the world is "unjust" and if any activity helps them to achieve wealth then they will struggle to get it done in any ways. On the other hand, a financial reporting study by Doupnik and Tsakumis (2004) has found out as masculinity increases people show a tendency to disclose their organization'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 a 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 exists no study in the area of ISS that investigate the moderating influence of masculinity in the relationship between perceived benefits and employees' intention to violate their organization's ISSP.

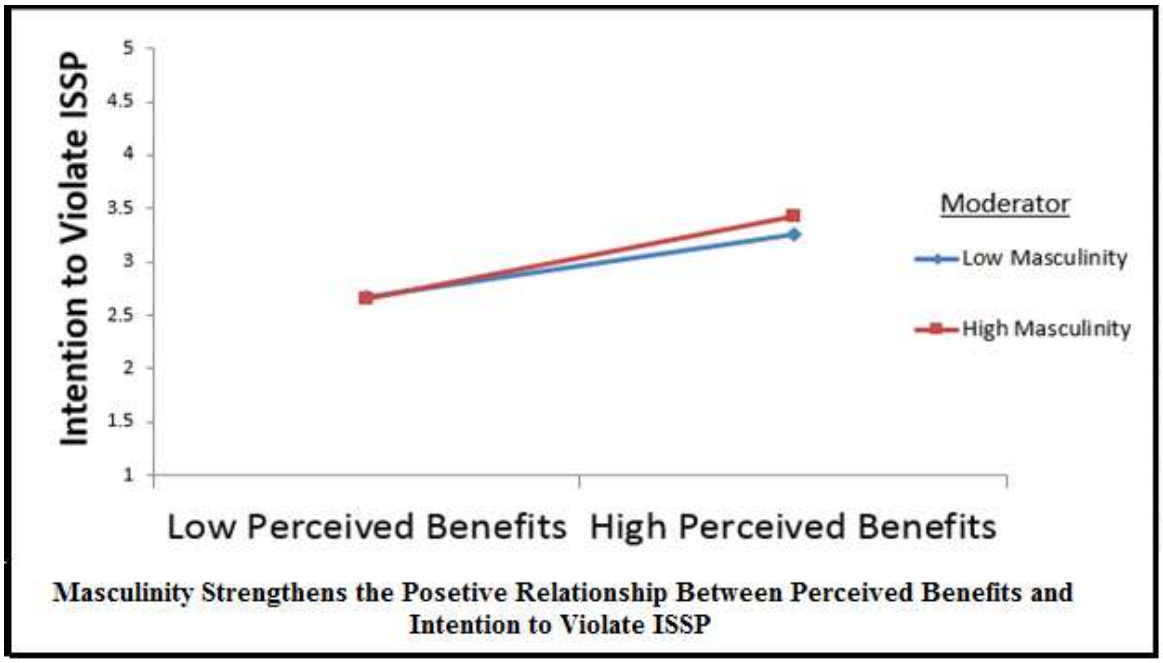

Figure: 4.26: Interaction Effect Between Perceived Benefits and Masculinity

The seventh hypothesis claimed that "The higher degree of collectivism, the stronger impact of perceived benefits is on employees' intention to violate ISSP". Unfortunately, this hypothesis is found to be significant in the opposite direction to what has been hypothesized and hence it is not supported by the collected data (see Figure 4.27).

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 a mixed support. In this regards, 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 wrong doings.

From this we might infer that, for the perceived benefit of being in harmony with friends and colleagues, employees in a collective society might not expose their friends for violating rules, and this might initiate employees to engage in violating of their organization's policies. However, in our study the perceived benefit of violating organization's ISSP was 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 scenario as the perceived benefit of saving time increases, employees in a more collective society might not violate their organization ISSP more often as employees in less collective society do. This is because people in an individualistic society are more inclined to show a self-centered character (Hofstede, 2011). This fact might initiate them to override their organization's rules in exchange for the perceived benefit of saving time.

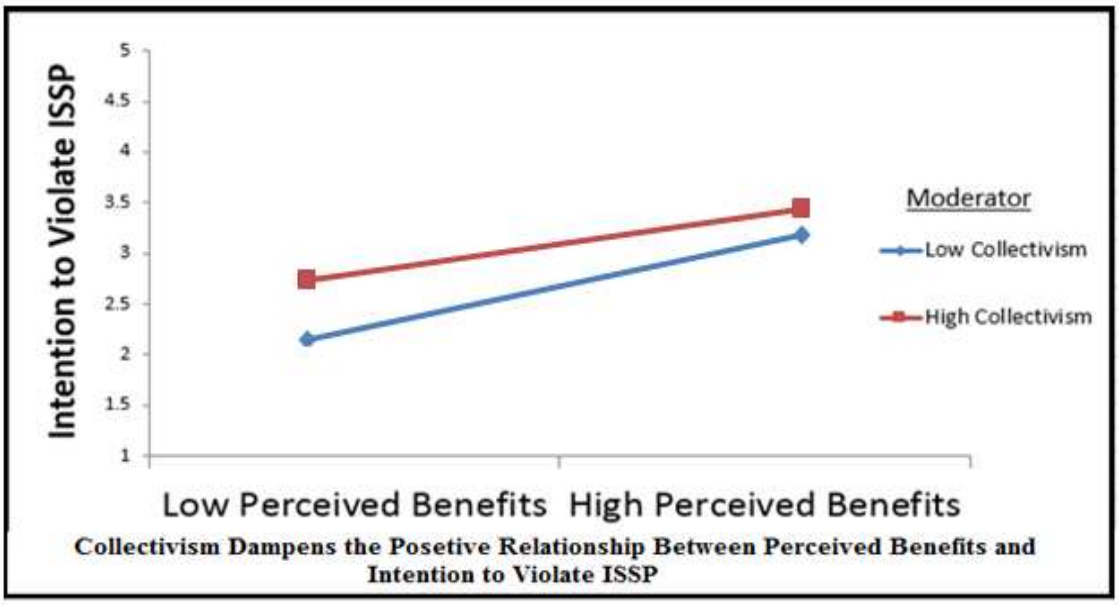

Figure: 4.27: Interaction Effect Between Perceived Benefits and Collectivism

The eighth hypothesis proposed that "The higher the degree of collectivism, the stronger the impact of shame is on employees' intention to violate ISSP" and as can be seen from Figure 4.28 it is supported by the collected data. In part, this finding is substantiated by Hostede's (2011) cultural theory which stated that if people bypass rules in collective societies, then they feel ashamed while same action leads to guilty feeling in an individualistic society. If we bring this same reality into ISS, we incline to say that shame decreases employees' intention to violate their organization's ISSP and the strength of this relationship will get stronger and stronger for a more collective society than a less collective society.

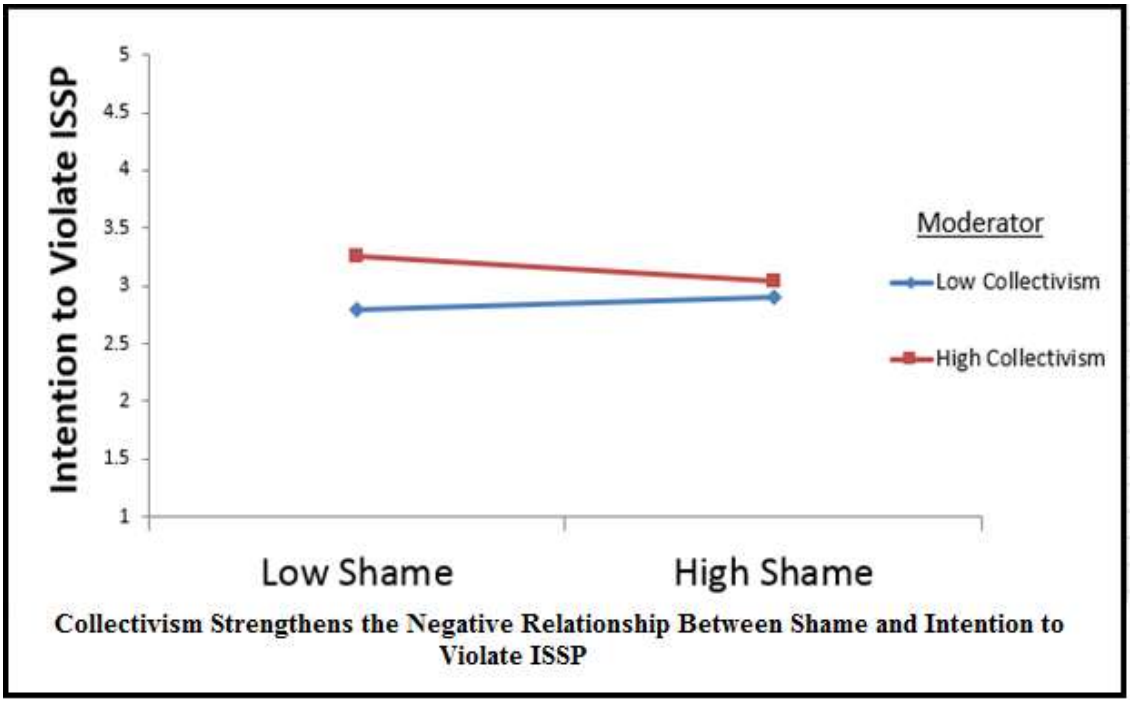

Figure: 4.28: Interaction Effect Between Shame and Collectivism

In the ninth hypothesis, we proposed that "The higher the degree of power distance, the stronger the impact of perceived benefits is on employees' intention to violate ISSP" and this hypothesis is found to be significant, but in the opposite direction to what has been hypothesized and hence it is not supported by the collected data (see Figure 4.29). Previous studies 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 then they will engage in such activities more often than low power distance societies. Unlike the above two studies, in our study the perceived benefit of violating ISSP is not monetary value, but time and this might in part influence the finding of our study because saving time is different from getting money and the two societies might 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 organization's ISSP also increase 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 organization ISSP.

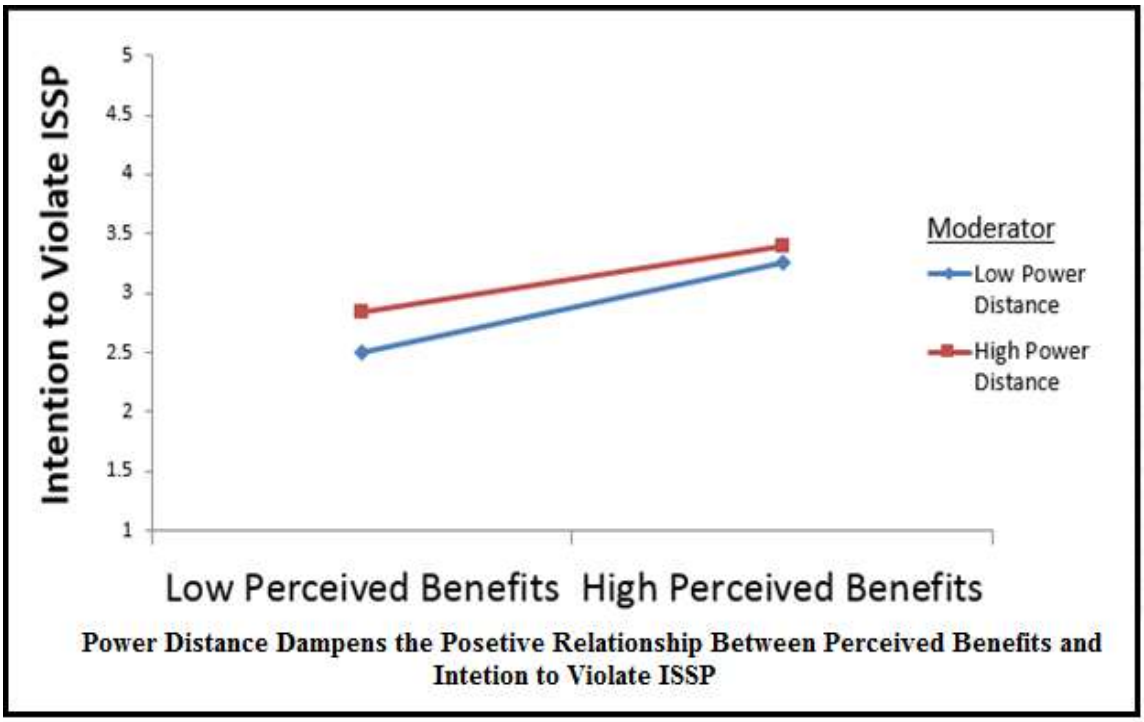

Figure: 4.29: Interaction Effect Between Perceived Benefits and Power Distance

In the tenth hypothesis, we proposed that "The higher the degree of power distance, the weaker the impact of formal sanctions is on employees' intention to violate ISSP" and as can be seen from Figure 4.30 the result is found to be significant but in the opposite direction from what has been proposed. Even though this result is consistent with some studies, the outputs from different studies show a mixed support. In this regards, 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 do. On the other hand, in an empirical work by Dols and Silvius (2010) it was reported that employees in high power distance society are found to be more obedient than low power distance people to their organization's rules given that they are ordered by their boss. In another study by Ifinedo (2009) in the area of IT security management it was reported that a government driven security regulation are more

successful in high power distance society than 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 regards, what might be implicit in the mind of our sample's respondents is that they feel they are expected/ordered by their boss to comply with their organization's ISSP.

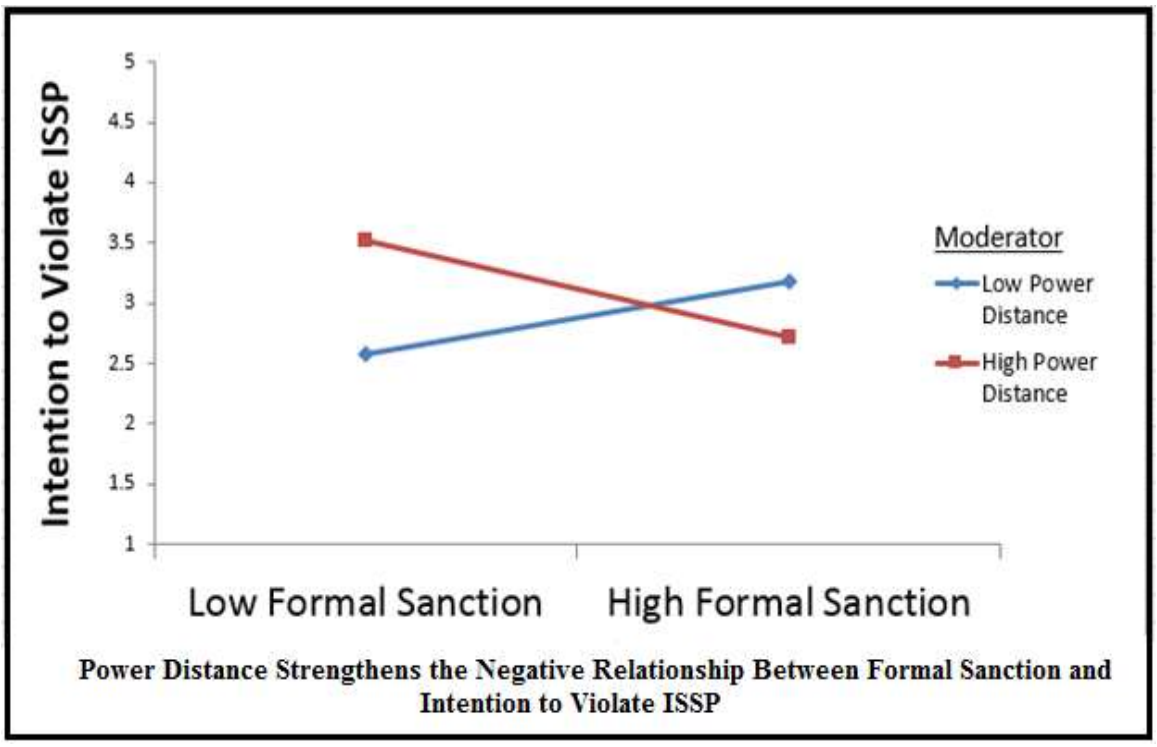

Figure: 4.30: Interaction Effect Between Formal Sanction and Power Distance

In the last hypothesis, we proposed that "The higher the degree of power distance, the weaker the impact of moral beliefs is on employees' intention to violate ISSP" and as can be seen from Figure 4.31 this hypothesis is supported. This finding is consistent with conceptual works in different disciplines. In this regards, in low power distance societies, there exists a participatory management style (Moore, 2003) and it is a good predictor of organizational citizenship behavior (OCB), which interns associated with a higher degree of compliance with rules by creating an environment where every individual feels belongingness and morally more tied up to the wellbeing of their company (Organ and Konovsky, 1998). This means as employees' moral beliefs increase, their intention to violate their organization's ISSP decrease

and this relationship is stronger for a lower power distance employees than their higher power distance counterparts. This idea is partly strengthened by Peterson et al. (2001) who stated that, even though the degree of influence varies, both individual's supervisors and people at home, do have an influence on individual's decisions concerning ethical dilemmas like noncompliance with the organization's rules (Peterson et al., 2001).

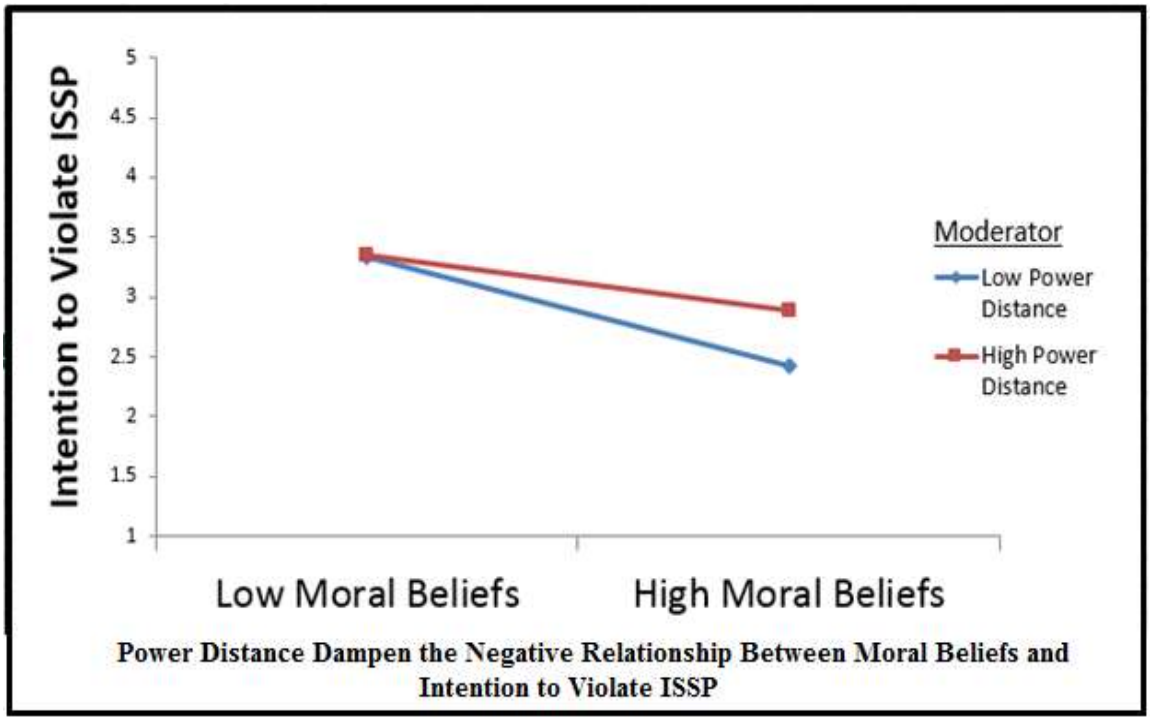

Figure 4.31: Interaction Effect Between Moral Beliefs and Power Distance

Finally, the effect of the five control variables (age, gender, CSSE, scenario type, and scenario realism) on employees' intention to violate their organization ISSP was also examined and as can be seen from Figure 4.24 one of them is found to be significant.

In this regard, we find out that employees' CSSE has a strong negative influence on employees' intention to violate their organizations' ISSP while the remaining variables (age, gender, scenario realism, and scenario type) are found to have insignificant influence. This means as employees' confidence and ability to understand and implement their organizational ISSP increases, then they will most probably respect the organizational rules and regulations

4.6. SUMMARY

In this chapter, firstly we showed the steps and procedures followed to conduct the instrument validation (pilot test). More specifically, we summarized the criteria used to test for validity and reliability test. In addition to this, we evaluated each and every constructs by constructing measurement model and we show how the full measurement model fit the collected data. In addition to this, we showed the result of the reliability test of the research constructs. Secondly, in the data analysis part, we accomplished tasks that assures the revalidation of the instruments by using the data collected from the main survey. Thirdly, we constructed the structural model to validate the hypotheses proposed in the first chapters. By constructing the structural model we showed the result of hypotheses testing, and finally we presented the discussion of the final results. In the next chapter, we made a discussion about the practical and theoretical implications of the research findings, moreover, we also finalized the chapter by giving a conclusion and recommendation remarks.

CHAPTER 5

CONTRIBUTIONS, DELIMITATIONS AND IMPLICATIONS

5.1. INTRODUCTION

In the previous chapter, we conducted data validation and data analysis activities followed by the discussion of the main findings of the research. In this chapter, we conduct a thorough discussion of the following topics: summarize the research questions that were stated in the first chapter and discuss the major steps followed to answer these research questions; outline the contribution of this study to research, theory and practice; discuss the main limitation of the study; discuss the implication of this study for future research; and finally we provide a concluding remark to the study.

5.2. RESEARCH QUESTIONS REVISITED

Even though the frequency and cost associated with ISS breaches caused by insiders increase from time to time, there has been unparalleled efforts to tackle this problem from behavioral perspectives (Arage et al., 2015). In the behavioral perspective, one of the important factors that has not been studied well for its impact on ISSP compliance is culture (Schiffman and Kanuk, 1997) and in African context there has been a very little knowledge, if any, about the exact impact of national culture on employees' ISSP compliance behavior. Even the findings of prior studies conducted in the western culture reported a mixed result (e.g. Doupnik and Tsakumis, 2004; Arage et al., 2016) on the impact of national culture dimensions on individuals 'ISSP compliance behavior, and more importantly, none of them measures culture at the individual level (Arage et al., 2016). In addition to this, many empirical studies that are conducted to investigate individuals' ISS behavior mainly use PMT and/or GDT theory and hence they were mainly focused on fear based strategy and provide only partial insight (Vance and Siponen, 2012). On the other hand, RCT includes additional constructs like perceived benefits and moral beliefs that provide a holistic view to the ISS problem (Li et al, 2010). In this regard, very few studies conducted in the western context (e.g. Vance and Siponen, 2012;

Li et al, 2010) use some of the constructs of RCT to investigate individuals' ISSP compliance behavior and their findings show inconsistent and even contradictory findings with previous studies around GDT (D'Arcy and Herath, 2011). Hence the applicability of the findings across different national culture has yet to be tested.

When examining those few previous studies that have investigated the impact of national culture and/or RCT constructs on individuals' ISSP compliance behavior in the context of economically developed countries, we noticed the following shortcomings: (1) to the best of our knowledge none of them (e.g. Dols and Silvius, 2010; Bjork and Jiang, 2006; D'Arcy et al., 2007) measure national culture at individual level and they did not empirically investigate the moderating influence of national culture in ISSP compliance area (2) construct of RCT like shame has rarely been investigated (with the exception of Vance and Siponen, 2010) for its impact on employees' ISSP compliance, and moreover all the constructs of RCT has never been investigated in African context, (3) none of the previous research investigated the moderating impact of national culture in the context of economically developing countries, particularly in Africa,(4) generally, the current research fall short of explaining the determinants of ISSP compliance in the context of developing economy countries.

Thus, to fill the gap left by previous studies we formulated the following research questions in the first chapter: (1) what is the influence of formal sanctions, perceived benefits, moral beliefs, and shame on employees' intention to violate their organization ISSP? (2) What is the moderating impact of national culture on the influence of formal sanctions, perceived benefits, moral beliefs, and shame on employees' intention to violate their organization ISSP?

In the upcoming subsections, we summarized how the two research questions were addressed by this study.

5.2.1. What is the influence of formal sanctions, perceived benefits, moral beliefs, and shame on employees' intention to violate their organization ISSP?

In addressing this research question, we conducted a detailed literature review about the constructs of the RCT. In this regard, we identified and discussed different research works that have been done concerning each of the RCT constructs and their relationship to the information security behavior of individuals (see Section 2.6). In this same section, we also discussed some of the limitations of the current studies around ISS. In this respect, our review shows that in the developing country context, little is known about the impact of formal sanctions, shame, perceived benefits, and moral beliefs on employees' intention to violate their organization ISSP. In addition to this, we justified the different methodological choice made for the study (see chapter 3). After conducting validity and reliability test on the survey instruments, the hypotheses were tested using a survey data collected from organizations that do have established ISSP (see chapter 4).

According to the empirical findings of the study, formal sanction, moral beliefs, and shame were found to have a very strong negative influence on employees' intention to violate their organization ISSP. This result is consistent with the research findings of prior studies in the field of IS and also criminology (e.g. Paternoster and Simpson, 1996; Pratt et al., 2006; D'Arcy et al., 2009; Siponen and Vance, 2010; Li et al., 2010; Vance and Siponen, 2012, Arage et al., 2015). In addition, the perceived benefit of noncompliance was found to encourage employees to violate their organization ISSP and this result is consistent with prior studies, such as: Siponen and Vance (2010), Li et al., 2010, Vance and Siponen (2012). Therefore, this study appropriately addresses the first research question posed at the beginning of this study.

5.2.2. What is the moderating impact of national culture on the influence of formal sanctions, perceived benefits, moral beliefs, and shame on employees' intention to violate their organization ISSP?

To answer this research question, first and foremost, we made a detailed overview of national culture (see section 2.7) and a brief analysis of the current literature about the influence of national culture on different types of IT related issues (see section 2.5.3). Particularly, we reviewed research works that mainly focus on how each of the national culture dimensions (power distance, masculine/feminine, uncertainty avoidance, and collectivism/individualism) are related to the information security behavior of individuals (see section 2.8 and section 2.9). Moreover, we also discussed the shortcomings of studies that investigate the impact of national culture on individuals ISS behavior (see section 2.8). In this regard, our review showed that there exists hardly any research that investigate the direct moderating impact of national culture dimensions on employees' intention to violate their organization ISSP.

In the third chapter, we discussed the philosophical position of the study and prepared the survey instruments related to the four dimensions of national culture, while in the fourth chapter we conduct validity and reliability test on the instruments. Finally, the hypotheses that proposed the moderating influence of national culture were tested using a survey data collected from organizations that do have established ISSP (see chapter 4). The output of the empirical test indicates that 8 out of 11 hypotheses were supported by the collected data. More specifically, the impact of moral beliefs, shame, and perceived benefits on employees' intention to violate their organization ISSP was found to be moderated by power distance, collectivism/individualism, and masculinity/uncertainty avoidance respectively (see Table 4.29). In this respect, our findings are consistent with prior studies that were conducted in different area, such as; Hofstede (2001, 2003, 2011) in the area of sociology; Timo (2009) in the area of ISS; Doupnik and Tsakumis (2004) in the area of finance.

On the other hand, based on the literature on IS and national culture, we have made our own justification regarding the three hypotheses that were not supported by the research findings (see section 4.5). In this regards, we also discussed (see section 4.5) the existence of some

prior studies in different areas (e.g. Husted (1999) in corruption, Tsakumis (2007) in tax evasion, Dols and Silvius (2010), and D'Arcy et al. (2007) in ISS) who reported similar findings to these three hypotheses. Thus, by following appropriate research procedures, we believe that this second research question is fully addressed by this study.

Generally, we believe that this study has identified some of the determinants of employees' intention to violate their organization ISSP and hence both of the research questions are sufficiently addressed.

5.3. CONTRIBUTION OF THE STUDY

In this study, we have identified, discussed, and tested decisive factors that are believed to have a direct or moderating impact on employees' intention to violate their organization ISSP. More specifically, we have made an extensive review of extant literature about the determinants of employees' ISSP compliance behavior, conceptualized them using appropriate theories, and finally tested them empirically in the Ethiopian context, which was neglected part of Sub-Saharan Africa in terms of mainstream IS research. The research model for this study was constructed based on the national culture and RCT. In terms of contribution, this study has got a strong contribution to research, practice, and theory. In the upcoming subsections we discussed these contributions in detail.

5.3.1. Contribution to Research and Theory

The contribution of this study to research and theory is discussed below:

First, our finding made it clear that examining the effect of deterrent countermeasures without considering the role of national culture dimensions is insufficient. A comprehensive view of employees' violation of ISSP need to combine deterrent countermeasures with national culture and this might partly explain the inconsistent findings of prior studies concerning the impact of deterrent countermeasures on ISSP violation. In this regards, to the best of our knowledge, this research is the first study to empirically investigate the moderating impact of national culture between RCT constructs and employees' intention to violate their

organization ISSP. There exists very few studies (e.g. D'Arcy and Herath, 2011; Dols and Silvius, 2010) that tried to bring the knowledge of national culture into the ISS area, but none of them empirically tests or explore the direct moderating influence of national culture. Hence, our study has made an original contribution in finding out the moderating role of national culture dimensions (i.e. power distance, collectivism/individualism, uncertainty avoidance, and masculine/feminine) on employees' intention to violate their organization ISSP. In addition to this, the finding of this study has also an important implication for studies in the ISS field by emphasizing that violation of ISSP is not only explained by fear of sanctions but also perceived benefits and moral beliefs.

Second, rather than directly taking the Hofstede's (1980, 1984, and 2001) values for the different cultural dimensions, this study directly measures national culture at the individual level. This procedure helps studies in the ISS to overcome one of the critics of Hofstede's (1980) cultural dimension. According to Wu (2006), the Hofstede's (1984) cultural data was collected before 30 years and as time changes people's cultural values also changes due to political, societal, and economic environments change. This might initiate researchers in the ISS field to revise their culture related studies by measuring national culture at individual level. To the best of our knowledge, there exists no research in the area of ISS that measures and use national culture at the individual level. This represents an original and important contribution to empirical research in area of ISS.

Third, this study contributes to the commutative theory building effort by bringing two traditionally separated theoretical streams: national culture and RCT. The result from the empirical test also proves that the combination of these two theories is appropriate and it provides additional insight into the problem of employees' violation of ISSP.

Fourth, this study is the first of its kind to include a components of RCT together with national cultural dimensions that has never been inculcated in previous RCT based ISS studies. For example, we provide a very important insight on how the impact of shame varies with different levels of national culture dimensions (i.e. collectivism vs. individualism) and this

will add some knowledge concerning important factors that has been overlooked by prior researchers. This might initiate future researchers to explore important variables that have been given less emphasis in the area of employees' ISSP compliance behavior.

5.3.2. Contribution to Practice

This study offers a number of contributions to ISS practice. Below is the detailed discussion of these contributions.

First and foremost, ISS managers and policy makers might get important insight into the moderating impact of each and every dimension of Ethiopian national culture on employees' intention to violate their organization ISSP. In Ethiopia the Information Network Security Agency (INSA) has the responsibility to develop and implement ISSP at national level. Unfortunately, the INSA has an ISSP directly copied from ISO 27002 and consequently organizations in Ethiopia are expected to use the ISO 27002 ISSP standards without any modification. Even though the literature indicates that culture do have a strong influence on the diffusing and the use of various kinds of practices, including IT related artifacts (Bjorck and Jiang, 2006), standards in the field of information security (e.g. ISO/IEC 27001, ISO/IEC 27002, BSI IT Baseline Protection Manual) largely neglects the impact of culture on information security (Timo, 2009). More specifically, Ifinedo (2009) reported that national culture has got a considerable influence in the successful implementation of varieties of practices brought from abroad (Ifinedo, 2009). In this regard, the findings of this study will have a paramount help to ISS policy makers at INSA in their attempt to adopt or modify the current ISSP. Generally, the following are some of the most important implications for ISS policy makers and managers:

- ✓ Since perceived benefit of noncompliance (e.g. Saving personal and work time) to organizational ISSP is found to have a very strong influence in initiating employees to violate their organizational ISSP, ISS managers need to prepare appropriate types of security education, training, and awareness programs that can convince employees not to compromise their organizational ISSP in exchange to any benefits like saving personal and work time. In this regards, since some

employees think that following organizational policies bring additional procedures to slow down work (Puhakainen, 2006), the security education, training, and awareness programs should work hard to change such attitude. More specifically, as perceived benefits of noncompliance increase, employees with a relatively lower uncertainty avoidance are found to engage in violation of their organizational ISSP more often than their higher uncertainty avoidance counterparts, and hence additional attention needs to be given to such employees. In addition to this, employees with a relatively higher score in masculinity are found to violate their organizational ISSP in exchange for some kinds of perceived benefits (i.e. saving work and personal time) and thus ISS managers need to take extra effort in controlling such employees. For example, organizations might focus on introducing a continuous and consistent training and awareness programs that communicating and convince employees not to compromise their organization ISSP for any reason.

- ✓ Since formal sanctions and shame were found to deter employees' violation of organizational ISSP, ISS managers are expected to invest the required amount of money and time to come up with the appropriate type of ISSP that consider the influence of such factors. Moreover, they need to make the implementation of the ISSP severe, certain and swift, so that they can be in a better position to protect their organization ISS. In parallel to this, it might be important to prepare different types of security education, training and awareness programs that emphasize the importance of respecting organizational ISSP and also stating the existence of severe penalties for violation of rules and this might increase employees' intention to voluntarily follow the organizational ISSP. At times when employees are found to violate ISSP, then ISS managers need to find out ways that announce rule breakers' activities in the organization so that they feel ashamed and deter themselves from further violation. In addition to this, by using different types of technologies ISS managers need to show their capacity and commitment in identifying ISS breach as soon as it occurs. This might increase employees' compliance intention by creating the feeling that the probability of being caught is

high if they violate the organization ISSP. Having said this, ISS managers need to know that, the impact of these variables might not be the same among employees with a relatively different cultural profile. For example, shame has a significant deterrent effect on employees with a relatively higher level of collectivism score, while it fails to have a deterrent impact on a relatively less collective employees. The implication of this for ISS managers is that disclosing an offender might work well in an organization where employees are more collective while this same mechanism might fail in a relatively less collective employees.

In addition to this, the findings of this study also indicate that, employees with a relatively higher power distance score are easily deterred by formal sanctions while this same counter measure leads to an increased violation of organizational ISSP in a relatively low power distance employees. This latter finding is the same as what Bjorck and Jiang (2006) reported "in a high power distance culture a mandated use of IT usage lead to a successful usage, while it leads to a rejection or refusal in low power distance culture". Thus, ISS managers need to know that formal sanctions might not produce the required level of compliance and even might resulted in unintended outcome if it is implemented unwisely without considering the power distance score of employees.

- ✓ A higher level of moral belief is found to reduce employees' intention to violate their organizational ISSP. This implies that ISS managers need to work hard in preparing different types of security education, training, and awareness programs that can convince employees how morally wrong it would be to violate their organizational ISSP. In this regards, Kohlberg (1984) proposed that through a well-prepared moral education programs, individuals will gradually but surely change their moral beliefs. More specifically, in organizations with a relatively higher level of power distance, ISS managers and supervisors are expected to show a high level of moral commitment to the organization rule and this intern might initiate subordinates to show a similar high level of moral commitment to the organization ISSP. This idea is partly strengthened by Peterson et al., (2001) who

stated that, even though the degree of influence varies, both individual's supervisors and people at home, do have an influence on individual's decisions concerning ethical dilemmas like noncompliance with organizational rules (Peterson et al., 2001).

- ✓ Generally, the above discussion clearly indicates that national culture is an important factor in the designing and implementation of successful ISSP, and hence ISS managers need to take into account the exact impact of each and every cultural dimension on the ISS behavior of their employees. In this respect, it will have a paramount importance if organizations prepare different types of cultural awareness programs to the ISS managers.

- ✓ As mentioned in the above paragraphs, having a successful security education, training, and awareness programs are the key to introduce employee different types of ISSP issues. One of the key mechanism to the successfulness of these programs is the use of scenario based training programs (Puhakainen, 2006). According to the author, this type of programs does have a proven power in communicating employees the level of harm the company might face when employees violate security rules. In this regards, organizations need to have a follow-up mechanism to understand the effectiveness of their security education, training, and awareness programs. Particularly, organizations can use feedback and evaluation mechanisms to understand the extent to which the security objectives are communicated and understood by employees and more importantly, it helps ISS managers to identify which mechanisms work well and which one need further improvement (Wilson and Hash, 2003).

Second, the findings of this study have also very important practical implication for companies that do have an outsourcing ambition for various kinds of service that involves IS. In this regards, this study offers an important information regarding the cultural makeup of Ethiopian employees and how does each and every dimension of national culture influence employees' compliance intention towards their organizational policies and procedures. This

information will put them in a better position to create and implement a standard and effective ISSP in their company.

Third, since the finding of our study indicate that CSSE has a negative influence on employees' intention to violate their organizational ISSP, organization should strive to improve their employees' confidence and ability to successfully understanding and implementing their organizational ISSP. In this respect, the contribution of different types of training and education programs would be invaluable.

5.4. DELIMITATION OF THE STUDY

Just like most empirical studies, this study has got its own limitations and 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 masculine. 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, 1984, and 2001) work. Since our research include the majority of national culture dimensions, we believe that the absence of one dimension doesn't has a considerable influence on the research finding.

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

The third limitation of this study might be the lack of a measure of the actual behavior of employees, and hence the use of intention as the dependent variable might raise the question "Whether intention indicates the actual behavior of employees?" Many researchers argue in

favor of using intention as the valuable approximation that provides a good explanation for behavior. The psychological theory of planned behavior suggests that people frequently behave as they predict (Ajzen, 1991). In this respect, researchers such as: Paternoster and Simpson (1996), Wenzel (2004), Pahnila, et al. (2007), Siponen and Vance (2010) use intention as a proxy to actual behavior in their study to predict employees' behavior in work place.

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. To reduce this limitation, we used a scenario method. According to Harrington (1996), since scenario describes others behavior in hypothetical case, respondents will not be intimidated to report their real intention to agree or disagree with what the scenario illustrate.

Fifth, in addition to the above limitations, since national culture is found to have a significant influence in IS studies (Leidner and Kayworth, 2006), it is important to note that the result of this study might 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 organizational ISSP and how national culture influence employees noncompliance behavior 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.

5.5. RECOMMENDATION FOR FUTURE STUDIES

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

First, researchers can repeat this same study in different countries so that they can test the generalizability of the findings of this study across different countries with similar national culture profile. As can be understood from the literature, studies in the area of ISS use the Hofstede's (1980, 1984, and 2001) cultural values without measuring culture at the individual level and their output show inconclusive findings concerning the impact of national culture dimensions across different countries with similar cultural makeup. Thus, we advise future researchers to conduct similar studies in a developing country context (a country with similar cultural makeup with Ethiopia) and see if the finding is generalizable to at least developing country context with similar cultural profile. Moreover, since ISSP is a new as well as sensitive area of research in developing countries, repeating this same study will help to secure matured knowledge of ISSP and national culture in developing country context.

Second, further studies are also needed to investigate the moderating influence of the collectivism cultural dimension between perceived benefits and intention to violate organizational ISSP. In contrary to our expectation, collectivism is found to dampen the positive relationship between the perceived benefits and intention to violate organizational ISSP. Different research outputs in IS reported that for the perceived benefit of being in harmony with friends, employees in a collective society might not expose their friends for violating the organization rules, and this might initiate employees to engage in violating of their organizational ISSP. In this regards, we do believe that the instrument used to measure perceived benefits need further research. In this study, the instruments that are used to measure the perceived benefits of noncompliance were 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 in a collective society overrides employees' intention to follow their organizational ISSP.

Third, 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 to enrich the knowledge around factors that contribute to the successfulness of organizational ISSP.

Fourth, even though the theory of Reasoned Action states that behavioral intention predicts actual behavior (Ajzen, 1991), future studies could be conducted by using the actual compliance behavior as the dependent variable. In this regards, 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 behavior 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 organizational security policies (e.g. lock their computer).

Fifth, this study used a quantitative research method, and we encourage future researchers to complement the survey method with additional interview so that the result can be further explained and triangulated.

5.6. CONCLUSION

As clearly discussed in this study, even though there exist a number of ISS standards around the world, protecting the ISS becomes a moving target for most organizations. To shed light on this problem (i.e. noncompliance), researchers in the area of ISS have been conducting a number of studies by using different theoretical lens (e.g. GDT, PMT, RCT) and based on their findings they reported on factors that might have a significant influence on improving employees' information security behavior. Most 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. In 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 behavior. 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 RCT (formal sanction, shame, perceived benefits, and moral beliefs) influence employees' intention to violate their organization 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 RCT constructs and employees' intention to violate their organization ISSP. Our proposed empirical model is sufficiently supported by the collected data. In this regards, we got a very important empirical evidence on factors that inhibit and also initiate employees to violate their organization ISSP. Moreover, the findings also show a strong evidence on the influence of contextual factors, national culture, on employees' information security behavior and consequently it highlighted the importance of taking some level of precaution when organizations introduce new policies or standards that are copied from abroad. ISSP 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 implication of our findings, we also highlighted the contribution of our study to research and theory. Based on the limitation of the study, we also recommend

opportunities for future researchers in the area of ISS to further enrich the existing knowledge around factors affecting employees' information security behavior.

When we summarized all the dissertation chapters in a nutshell, in the first chapter, we mainly identified and discussed important topics, such as: research gap, research questions, hypotheses, and objective of the research. In addition to this, we also gave some highlights of the research methodology used and the literature to be reviewed. While in the second chapter, we conducted a detailed literature review on the most important concepts of the study and also we substantiated our hypotheses with a detailed literature review. In the third chapter, a detailed discussion of the research methodology and the rationale behind each and every methodological decision was made. In addition to this, data preprocessing activities were also done. In the fourth chapter, we conducted validity and reliability tests followed by an empirical test on the research model by using survey data collected from different regions in Ethiopia. Moreover, we have also made a detailed discussion of the findings of the study. Finally, the fifth chapter conclude this study by discussing the contribution, delimitations, and implication of the study.

REFERENCCES

1. 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.
2. Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes, 50(2), 179-211.
3. Al-Awadi, M., & Renaud, K. (2007, July). Success factors in information security implementation in organizations. In IADIS International Conference e-Society.
4. Alexander, C. S., & Becker, H. J. (1978). The use of vignettes in survey research. Public opinion quarterly, 42(1), 93-104.
5. Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information security culture: a behaviour compliance conceptual framework. In Proceedings of the Eighth Australasian Conference on Information Security-Volume 105 (pp. 47-55). Australian Computer Society, Inc.
6. Alghazzawi, D. M., Hasan, S. H., & Trigui, M. S. (2014). Information Systems Threats and Vulnerabilities. International Journal of Computer Applications, 89(3).
7. Alreck, P. L., & Settle, R. B. (2004). The survey research handbook (3rd ed.). Boston, MA: McGraw-Hill.
8. 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. Psychometrical, 49(2), 155-173.
9. Arage, T., Belanger, F., & Beshah, T. (2015). Influence of National Culture on Employees' Compliance with Information Systems Security (ISS) Policies: Towards ISS Culture in Ethiopian Companies.
10. 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.
11. Armstrong, J. S., & Overton, T. S. (1977). Estimating nonresponse bias in mail surveys. Journal of marketing research, 396-402.
12. Bachman, R., Paternoster, R., & Ward, S. (1992). The rationality of sexual offending: Testing a deterrence/rational choice conception of sexual assault. Law and Society Review, 343-372.
13. Bagchi, K., & Udo, G. (2003). An analysis of the growth of computer and Internet security breaches. Communications of the Association for Information Systems, 12(1), 46.
14. Bailey, K. D. (1982). Methods of social research (2nd ed.). New York, NY: Free Press.

15. Baron, Reuben M. and David A. Kenny (1986), "The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations," Journal of Personality and Social Psychology, 51 (6), 1173-1182.
16. Barsanti, C. (1999). Modern network complexity needs comprehensive security. Security, 36(7), 65-8.
17. Baskerville, R. (1991). Risk analysis: an interpretive feasibility tool in justifying information systems security. European Journal of Information Systems, 1(2), 121-130.
18. Bassili, J. N., & Scott, B. S. (1996). Response latency as a signal to question problems in survey research. Public Opinion Quarterly, 60(3), 390-399.
19. Bearden, W. O., Money, R. B., & Nevins, J. L. (2006). A measure of long-term orientation: Development and validation. Journal of the Academy of Marketing Science, 34(3), 456-467.
20. Beccaria, C. (1963). On crimes and punishments. New York: Macmillan.
21. Becker, G. S. (1968). Crime and Punishment: An Economic Approach. The Journal of Political Economy 76(1830482): 169–217.
22. Bell, E., & Bryman, A. (2007). The ethics of management research: an exploratory content analysis. British Journal of Management, 18(1), 63-77.
23. Bell, D. E., & La Padula, L. J. (1988). Secure computer system unified exposition and multics interpretation. Communications of the ACM, 1, 271-280.
24. Birch, D. G., & McEvoy, N. A. (1995). Structured risk analysis for information systems. Hard Money-Soft Outcomes, 29-51.
25. Bjorck, J., & Jiang, K. (2006). Information Security and National Culture (Doctoral dissertation, KTH Royal Institute of Technology, Stockholm, Sweden).
26. Blasi, A. (1980). Bridging moral cognition and moral action: A critical review of the literature. Psychological bulletin, 88(1), 1.
27. Boudreau, M. C., & Robey, D. (1996). Coping with contradictions in business process re-engineering. Information Technology & People, 9(4), 40-57.
28. Boudreau, M. C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: a state-of-the-art assessment. MIS quarterly, 1-16.
29. Brown, T. A. (2015). Confirmatory factor analysis for applied research. Guilford Publications
30. 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.
31. Bulmer, M. G. (1979). Principles of Statistics, Mineola, New York: Courier Dover Publications

32. Bultum, A. G. (2012). Adoption of Electronic Banking System in Ethiopian Banking Industry: Barriers and Driver. Available at SSRN 2058202.
33. Burn, J., Saxena, K. B. C., Ma, L., & Cheung, H. K. (1993). Critical issues of IS management in H a cultural comparison. Journal of Global Information Management (JGIM), 1(4), 28-30
34. Burrell, G., & Morgan, G. (1979). Sociological paradigms and organizational analysis (Vol. 248). London: Heinemann.
35. Byrne, B. (2001). Structural equation modelling with AMOS: Basic concepts, applications, and programming. Mahwah, NJ: Lawrence Erlbaum Associates.
36. Caelli, W., Longley, D., & Shain, M. (1991). Information security handbook. Stockton Press.
37. Cao, L. (2004). Major criminological theories: Concepts and measurements. Wadsworth/Thomson Learning.
38. Cardoso, A., & Ramos, I. (2012). Looking at the past to enrich the future: a reflection on Klein and Myers' quality criteria for interpretive research. Electronic journal of business research methods (EJBRM), 10(2), 77-88.
39. Cavusoglu, H., & Raghunathan, S. (2004). Economics of IT Security Management: Four Improvements to Current Security Practices. The Communications of the Association for Information Systems, 14(1), 37.
40. Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behaviour. Journal of Information Privacy and Security, 1(3), 18-41.
41. Chaula, J. A. (2006). A socio-technical analysis of information systems security assurance: A case study for effective assurance (Doctoral dissertation, Department of Computer and Systems Sciences
42. Chin, W.W 1998, 'The partial least squares approach to structural equation modelling,' in GA Marcoulides (ed.), Modern methods for business research, London, pp. 295–336
43. Choe, J. M. (2004). The consideration of cultural differences in the design of information systems. Information & Management, 41(5), 669-684.
44. Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719-731.
45. Chokhani, S. (1992). Trusted products evaluation. Communications of the ACM, 35(7), 64-76.
46. 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.
47. Chua, W. (1986) Radical developments in accounting thought. Accounting Review, 61, 601–632.

48. Clark, T., Eckhardt, G., & Hofstede, G. (2003). Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations across Nations, 2d ed.
49. Clarke, M. (2011). The Role of Self-Efficacy in Computer Security Behavior: Developing the Construct of Computer Security Self-Efficacy (CSSE).ProQuest LLC.
50. Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. MIS quarterly, 189-211.
51. Converse, J. M. & Presser, S. (1986). Survey Questions: Handcrafting the Standardised Questionnaire. SAGE Publications.
52. Cook, T. D., Campbell, D. T., & Day, A. (1979). Quasi-experimentation: Design & analysis issues for field settings (Vol. 351). Boston: Houghton Mifflin.
53. Courtney Jr, R. H. (1977, June). Security risk assessment in electronic data processing systems. In Proceedings of the June 13-16, 1977, national computer conference (pp. 97-104). ACM.
54. Creswell, J. W. (2009). Editorial: Mapping the field of mixed methods research. Journal of Mixed Methods Research, 3(2), 95-108.
55. Creswell, J. W. (2013). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.
56. Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. Computers and security, 32, 90-101.
57. Crotty, M. (1998). The Foundations of Social Research: Meaning and perspective in the research process. London, Sage Publications.
58. Cyber Security Watch Survey. (2010). 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/
59. Cyber Security Watch Survey. (2012). CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, September 2012. Available at URL: http://www.cert.org/insider_threat/
60. Cyber Security Watch Survey. (2014). CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, September 2012.Available at URL: http://www.cert.org/insider_threat/
61. Dagwell, R., & Weber, R. (1983). System designers' user models: a comparative study and methodological critique. Communications of the ACM,26(11), 987-997.

62. 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.
63. D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. Journal of business ethics, 89(1), 59-71.
64. D'Arcy, J., Lee, K., Hovav, A. (2007). A Cross-Cultural Analysis of Security Countermeasures Effectiveness. Second Pre-ICIS Workshop on Information Security and Privacy (WISP2007), December 8th, 2007. Montreal, Canada.
65. D'Arcy, J., & Hovav, A. (2004). The role of individual characteristics on the effectiveness of IS security countermeasures. AMCIS 2004 Proceedings, 176.
66. D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. Communications of the ACM, 50(10), 113-117.
67. 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.
68. Devamohan, A. (2008). E–Banking Problems and Prospects in Ethiopia. Available at URL: http://wA.Devamohan%20-%20E-banking.htm.
69. Dhillon, G. (1999). Managing and controlling computer misuse. Information Management & Computer Security, 7(4), 171-175.
70. Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal, 11(2), 127-153.
71. Dhillon, G., & Moores, S. (2001). Computer crimes: theorizing about the enemy within. Computers & Security, 20(8), 715-723.
72. Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. Information Systems Journal, 19(4), 391-412.
73. Dols, T., & Silvius, A. J. (2010). Exploring the Influence of National Cultures on Non-Compliance Behavior. Communications of the IIMA, 10(3), 11.
74. Dorfman, P. W., & Howell, J. P. (1988). Dimensions of national culture and effective leadership patterns: Hofstede revisited. Advances in international comparative management, 3(1), 127-150.
75. 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.

76. Eining, M. M., & Lee, G. M. (1997). Information ethics: An exploratory study from an international perspective. Journal of Information Systems, 11(1), 1-17.
77. Erdem, T., Swait, J., & Valenzuela, A. (2006). Brands as signals: A cross-country validation study. Journal of Marketing, 70(1), 34-49.
78. Ernest Chang, S., & Lin, C. S. (2007). Exploring organizational culture for information security management. Industrial Management & Data Systems,107(3), 438-458.
79. Ernst and Young. (2003). Global Information Security Survey. New York.
80. Ernst & Young (2008). Information Security Survey London, UK.
81. EthioNews, (2013). Ethiopian Airlines axes 11 employees for system abuse: available at URL : http://www.ethionews24.com/ethiopian-airlines-axes-11-employees-for-system-abuse-3
82. 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.
83. Field, A. (2009). Discovering statistics using SPSS. Sage publication
84. Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of marketing research, 39-50.
85. Fortune. (2012). The Ethiopian Revenue Authority Discover a wrong doing by employee. The Addis Fortune, Retrieved from http://addisfortune.net/articles/agency-frames-regulatory-stick-on-private-higher-education-institutions-at-fault/
86. Furrer, O., Liu, B. S. C., & Sudharshan, D. (2000). The relationships between culture and service quality perceptions basis for cross-cultural market segmentation and resource allocation. Journal of service research, 2(4), 355-371.
87. Gardachew, W. (2010). Electronic-Banking in Ethiopia-Practices, Opportunities and Challenges. Journal of internet Banking and commerce, 15(2), 2-8.
88. Garg, A., Curtis, J., & Halper, H. (2003). The financial impact of IT security breaches: what do investors think?. Information Systems Security, 12(1), 22-33.
89. Geertz, C. (1973). The interpretation of cultures: Selected essays (Vol. 5019). Basic books.
90. Gefen, D., Straub, D., & Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice. Communications of the association for information systems, 4(1), 7.
91. Gibbs, J. P. (1975). Crime, punishment, and deterrence (p. 58). New York: Elsevier.
92. Gottfredson, D. M., Wilkins, L. T., & Hoffman, P. B. (1978). Guidelines for parole and sentencing: A policy control method (pp. 25-33). Lexington, MA: Lexington Books.

93. Grasmick, H. G., & Bursik Jr, R. J. (1990). Conscience, significant others, and rational choice: Extending the deterrence model. Law and society review, 16(3), 837-861.
94. Greenberg, J. (2002). Who stole the money, and when? Individual and situational determinants of employee theft. Organizational Behavior and Human Decision Processes, 89(1), 985-1003.
95. Griffith, T. L., & Dougherty, D. J. (2001). Beyond socio-technical systems: introduction to the special issue. Journal of Engineering and Technology Management, 18(3), 207-218.
96. Guba, E. G. & Lincoln, Y. S. (2005). Paradigmatic controversies, contradictions, and emerging confluences', in NK Denzin and YS Lincoln (eds.). The Sage handbook of qualitative research, 3rd edn, Sage Publications, Thousand Oaks, 191–216
97. Hair, J. F., Babin, B. J., Anderson, R. E., and Tatham, R. L. (2006). Multivariate data analysis, 6.
98. Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2010). Multivariate data analysis (7th Eds.). NY: Pearson.
99. Hamill, J. T., Deckro, R. F., & Kloeber, J. M. (2005). Evaluating information assurance strategies. Decision Support Systems, 39(3), 463-484.
100. 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.
101. 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.
102. Hechter, M., & Kanazawa, S. (1997). Sociological rational choice theory. Annual review of sociology, 191-214.
103. 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.
104. Hentea, M. (2005). A perspective on achieving information security awareness. Informing Science: International Journal of an Emerging Trans discipline, 2, 169-178.
105. 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.
106. Herath, T., & Rao, H. R. (2009b). Encouraging information security behaviours in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47 (3), 154–165.
107. Higgins, G. E. (2005). Can Low Self-Control Help with the Understanding of the Software Piracy Problem? Deviant Behavior, 26 (1), 1-24.

108. Hoffer, J. A., & Straub Jr, D. W. (1989). The 9 to 5 underground: are you policing computer crimes? MIT Sloan Management Review, 30(4), 35.
109. Hofstede, G. (1980). Culture's consequences: International differences in work- related values. Sage Publications, Beverly Hills, CA.
110. Hofstede, G. (1991). Cultures and organizations: Software of the mind. Intercultural cooperation and its importance for survival. London, McGraw-Hill.
111. Hofstede, G. (2000). The information age across cultures. Proceedings of 5th AIM conference: Information systems and organizational change, 43(4), 615-660.
112. Hofstede, G. (2001). Dimensions of national cultures in fifty countries and three regions. Explorations in cross-cultural psychology. Lisse, Netherlands: Swets& Zeitlinger.
113. Hofstede, G. (2011). Dimensional zing cultures: The Hofstede model in context. Online readings in psychology and culture, 2(1), 8.
114. Hofstede, G., & Bond, M. H. (1988). The Confucius connection: From cultural roots to economic growth. Organizational dynamics, 16(4), 5-21.
115. Hofstede, G. H., & Hofstede, G. (2001). Culture's consequences: Comparing values, behaviors, institutions and organizations across nations. Sage.
116. Hofstede, G. and G. J. Hofstede. (2005). Cultures and Organizations: Software of the Mind (second ed.) New York, Mcgraw-Hill.
117. Holgate, J. A., Williams, S. P., & Hardy, C. A. (2012). Information Security Governance: investigating diversity in critical infrastructure organizations.Proceedings of Bled eConference.
118. Holmes-Smith, P. (2010). An applied introductory course in structural equation modelling using AMOS', in SREAM.
119. Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), 615-660.
120. Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security–a neo-institutional perspective. The Journal of Strategic Information Systems, 16(2), 153-172.
121. Hussain, S. (1998). Technology transfer models across cultures: Brunei-Japan joint ventures. International Journal of Social Economics, 25(6/7/8), 1189-1198.
122. Husted, B. W. (1999). Wealth, culture, and corruption. Journal of International Business Studies, 30(2), 339-359.

123. Husted, B. W. (2000). The impact of national culture on software piracy. Journal of Business Ethics, 26(3), 197-211.
124. Ifinedo, P. (2009). Information technology security management concerns in global financial services institutions: is national culture a differentiator? Information Management & Computer Security, 17(5), 372-387.
125. Information Week. (2005). U.S. Information Security Research Report 2005. United Business Media, London.
126. Interpretation, T. N. (1990). NCSC-TG 005. National Computer Security Center.
127. ISO/IEC (2005). Information Technology — Security Techniques — Code of Practice for Information Security Management. Available at URL: http://www.iso27001security.com/html/27002.html. Accessed on August 2, 2013.
128. ISO/IEC (2009). Information Technology – Security Techniques – Information Security Management Measurements, ISO/IEC 27004, Geneva.
129. Jacobs, B. A. (2010). Deterrence and deterrability. Criminology, 48(2), 417-441.
130. Jansen, H., & Hak, T. (2005). The productivity of the three-step test-interview (TSTI) compared to an expert review of a self-administered questionnaire on alcohol consumption. Journal of Official Statistics: an international quarterly, 21(1), 103-120.
131. Johns, S. K., Smith, M., & Norman, C. S. (2002). How culture affects the use of information technology. In Accounting Forum, 27(1), 84-109.
132. Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. MIS quarterly, 34(4), 549-566.
133. Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. International journal of information management, 23(2), 139-154.
134. Kanuk, L., & Berenson, C. (1975). Mail surveys and response rates: A literature review. Journal of Marketing Research, 34(5), 440-453.
135. Karjalainen, M., Siponen, M. T., Puhakainen, P., & Sarker, S. (2013). One Size Does Not Fit All: Different Cultures Require Different Information Systems Security Interventions. In PACIS (p. 98).
136. Kassahun, A. (2012). The effect of Business Process Reengineering (BPR) on public sector organisation performance in a developing economy context. In PACIS, 23(3).
137. Keesing, R. M. (1974). Theories of culture. Annual review of anthropology, 8(2), 73-97.
138. Keil, M., Tan, B. C., Wei, K. K., Saarinen, T., Tuunainen, V., & Wassenaar, A. (2000). A cross-cultural study on escalation of commitment behaviour in software projects. MIS quarterly, 20(2), 299-325.

139. Kettinger, W. J., Lee, C. C., & Lee, S. (1995). Global measures of information service quality: a cross-national study. Decision sciences, 26(5), 569-588.
140. Kim, S. (2002). Participative management and job satisfaction: Lessons for management leadership. Public administration review, 62(2), 231-241.
141. King, P. M. and Mayhew, M. J., (2002). Moral judgement development in higher education: Insights from the Defining Issues Test. Journal of moral education, 31(3), pp.247-270.
142. Kirsch, L., & Boss, S. (2007). The last line of defence: motivating employees to follow corporate security guidelines. ICIS 2007 Proceedings, 103.
143. Kline, R. B. (2005). Principles and practice of structural equation modelling: methodology in social sciences, 2nd edn, Guilford Press, New York.
144. Kline, R. B. (2010). Principles and Practice of Structural Equation Modelling, 3rd edn Guilford Press. New York. USA.
145. Kohlberg, L. (1984). Essays on moral development: The psychology of moral development. New\ brk: Harper & Row.
146. Koskosas, I. V., & Paul, R. J. (2004, March). The interrelationship and effect of culture and risk communication in setting internet banking security goals. In Proceedings of the 6th international conference on Electronic commerce (pp. 341-350). ACM.
147. 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.
148. Kumar, P., Henikoff, S., & Ng, P. C. (2009). Predicting the effects of coding non-synonymous variants on protein function using the SIFT algorithm.Nature protocols, 4(7), 1073-1081.
149. Lafree, G., Ducan, L., & Piquero, A,. R. (2005). Testing a rational choice model of airline hijackings Criminology, 43(4), 340-361.
150. 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.
151. Lawshe, C. H. (1975). A quantitative approach to content validity. Personnel psychology, 28(4), 563-575.
152. Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. Information Management & Computer Security, 10(2), 57-63.

153. Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. Information & Management, 41(6), 707-718.

154. Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. Decision Support Systems, 50(2), 361-369.

155. Leidner, D. E., & Kayworth, T. (2006). Review: a review of culture in information systems research: toward a theory of information technology culture conflict. MIS quarterly, 30(2), 357-399.

156. Leonard, L. N., & Cronan, T. P. (2001). Illegal, inappropriate, and unethical behavior in an information technology context: A study to explain influences. Journal of the Association for Information Systems, 1(1), 12.

157. Leonard, L. N. K., T. P. Cronan, J. Kreie. (2004). What influences IT ethical behaviour intentions—Planned behavior, reasoned action, perceived importance, individual characteristics? Inform. Management, 42(1), 143–158.

158. Lewis, B. R., Templeton, G. F., & Byrd, T. A. (2005). A methodology for construct development in MIS research. European Journal of Information Systems, 14(4), 388-400.

159. Lewis-Beck, M., Bryman, A. E., & Liao, T. F. (2003). The Sage encyclopaedia of social science research methods. Sage Publications.

160. 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.

161. Linda, K., & Thomas D. (2008). Essentials of social research. McGraw-Hill Education (UK).

162. Linsky, A. S. (1975). Stimulating responses to mailed questionnaires: A review. Public Opinion Quarterly, 39(1), 82-101.

163. Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. MIS quarterly,10(2), 173-186.

164. MacCallum, R. C., Browne, M. W., & Sugawara, H. M. (1996). Power analysis and determination of sample size for covariance structure modeling. Psychological methods, 1(2), 130.

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

166. Magklaras, G. B., Furnell, S. M., & Brooke, P. J. (2006). Towards an insider threat prediction specification language. Information management & computer security, 14(4), 361-381.

167. Marakas, G., Johnson, R., & Clay, P. F. (2007). The Evolving Nature of the CSE Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time. Journal of the Association for Information Systems, 8(1), 2.
168. McCarthy, B. (2002). New economics of sociological criminology. Annual Review of Sociology, 19(3), 417-442.
169. McFadzean, E., Ezingeard, J. N., & Birchall, D. (2006). Anchoring information security governance research: sociological groundings and future directions. Journal of Information System Security, 2(3), 3-48.
170. McGrath, J. 1981. Dilemmatic: The study of research choices and dilemmas. American Behavioural Scientist, 25(2). 179-210.
171. McPhee, D. (2008). Information technology infrastructure library and security management overview. In Tipton, H.F. and Krause, K. (Eds), Information Security Management Handbook, Taylor & Francis, Boca Raton, FL.
172. Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. Communications of the ACM, 38(12), 65-74.
173. Moores, T. T. (2003). The effect of national culture and economic wealth on global software piracy rates. Communications of the ACM, 46(9), 207-215.
174. Morgan, G. A., & Griego, O. V. (1998). Easy use and interpretation of SPSS for Windows: Answering research questions with statistics. Psychology Press.
175. Morgan, G., & Smircich, L. (1980). The case for qualitative research. Academy of management review, 5(4), 491-500.
176. Myers, M. D. (1997). Qualitative research in information systems. MIS quarterly, 21(2), 241-242.
177. Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules & quest; an empirical study. European Journal of Information Systems, 18(2), 126-139.
178. Nagin, D. S., & Paternoster, R. (1993). Enduring individual differences and rational choice theories of crime. Law and Society Review, 12(4), 467-496.
179. Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815-825.
180. Njenga, K., & Brown, I. (2008). Collective Improvisation: Complementing Information Security Frameworks with Self-Policing. In ISSA (pp. 1-16).

181. Nunnally, J. C. (1978). Psychometric theory. McGraw-Hill (2and ed).New York.
182. Olson, K. (2010). Do non-response follow-ups improve or reduce data quality? a review of the existing literature. Journal of the Royal Statistical Society: Series A (Statistics in Society), 176(1), 129-145.
183. Organ, D. W., & Konovsky, M. (1989). Cognitive versus affective determinants of organizational citizenship behavior. Journal of applied psychology, 74(1), 157.
184. Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. Information systems research, 2(1), 1-28.
185. Palvia, P. C. (1998). Research issues in global information technology management. Information Resources Management Journal (IRMJ), 11(2), 27-36.
186. Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In System sciences, 2007. HICSS 2007. 40Th annual hawaii international conference on (pp. 156b-156b). IEEE.
187. Parker, D. B. (1976). Crime by computer (pp. xii-xii). New York: Scribner.
188. Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). Human factors and information security: individual, culture and security environment. 176(1), 129-145.
189. Paternoster, R., & Pogarsky, G. (2009). Rational choice, agency and thoughtfully reflective decision making: The short and long-term consequences of making good choices. Journal of Quantitative Criminology, 25(2), 103-127.
190. Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. Law and Society Review, 16(3), 549-583.
191. Pee, L. G., Woon, I. M., & Kankanhalli, A. (2008). Explaining non-work-related computing in the workplace: A comparison of alternative models. Information & Management, 45(2), 120-130.
192. Peterson, D., Rhoads, A., & Vaught, B. C. (2001). Ethical beliefs of business professionals: A study of gender, age and external factors. Journal of Business Ethics, 31(3), 225-232.
193. Pfleeger, C., & Pfleeger, S. L. (2003). Leveraging behavioral science to mitigate cyber security risk. Computers & security, 31(4), 597-611.
194. Phelps, D. C. (2005). Information system security: Self-efficacy and security effectiveness in Florida Libraries. 40Th annual hawaii international conference on (pp. 156b-156b). IEEE.

195. Pimchangthong, D., Plaisent, M., & Bernard, P. (2003). Key issues in information systems management: A comparative study of academics and practitioners in Thailand. Journal of Global Information Technology Management, 6(4), 27-44.
196. Pinch, T. (2008). Technology and institutions: living in a material world, theory and society, 37(5), 461-483.
197. Piquero, A. R., & Hickman, M. (1999). An empirical test of tittle's control balance theory. Criminology, 37(2), 319-342.
198. Piquero, A., & Tibbetts, S. (1996). Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: Toward a more complete model of rational offending. Justice quarterly, 13(3), 481-510.
199. Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. Journal of applied psychology, 88(5), 879.
200. Pogarsky, G. (2004). Projected offending and contemporaneous rule-violation: Implications for heterotypic continuity. Criminology, 42(1), 111-136.
201. Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2013). Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities. European Journal of Information Systems, 19(2), 181-195.
202. Puhakainen, P. (2006). Design theory for information security awareness. Journal of Global Information Technology Management, 6(4), 27-44.
203. Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. Information Systems Research, 20(1), 121-139.
204. Reed, S. K. (1977). Automatic Data Processing Risk Assessment. US Department of Commerce. National Technical Information Service.
205. Richardson, R., & Director, C. S. I. (2008). CSI computer crime and security survey. Computer Security Institute, 1, 1-30.
206. Salahuddin, M. A. (2011). Information security management: a case study of an information security culture (Doctoral dissertation, Queensland University of Technology).
207. Schafer, J. L. (1999). Multiple imputation: a primer. Statistical methods in medical research, 8(1), 3-15.
208. Schappe, S. P. (1998). The influence of job satisfaction, organizational commitment, and fairness perceptions on organizational citizenship behaviour. The Journal of Psychology, 132(3), 277-290.

209. Schatz, D. (2008). Setting priorities in your security program. In Tipton, H.F. and Krause, K. (Eds). Information Security Management Handbook, Taylor & Francis, Boca Raton, FL.
210. Schiffman, L.G. and L.L. Kanuk (1997). Consumer Behaviour, Sixth Edition. Englewood Cliffs, New Jersey: Prentice-Hall International, Inc.
211. Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. Computers & Security, 21(6), 526-531.
212. Scott, P. (2015). Executive Perspectives on Top Risks for 2015. EDPACS, 51(6), 8-11.
213. Shaw, E., Ruby, K., & Post, J. (1998). The insider threat to information systems: The psychology of the dangerous insider. Security Awareness Bulletin, 2(98), 1-10.
214. Sheatsley, P. B. (1983). Questionnaire construction and item writing. Handbook of survey research, 4(1), 195-230.
215. Shore, B., Venkatachalam, A. R., Solorzano, E., Burn, J. M., Hassan, S. Z., & Janczewski, L. J. (2001). Soft lifting and piracy: Behavior across cultures. Technology in Society, 23(4), 563-581.
216. Singleton, J., & Straits, B. C. (2005). Approaches to social research. New York, NY: Oxford University Press.
217. Siponen, M. T. (2000). A Conceptual Foundation for Organizational Information Security Awareness. Information Management and Computer Security, 8(1), pp. 31-41.
218. Siponen, M. T. (2001). Five dimensions of information security awareness. Computers and Society, 31(2), 24-29.
219. 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.
220. Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. MIS quarterly, 34(3), 487.
221. Siponen, M., Pahnila, S., & Mahmood, A. (2006). Factors influencing protection motivation and IS security policy compliance. In Innovations in Information Technology, 2006 (pp. 1-5). IEEE.
222. 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). Springer US.
223. 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.

224. Solutions, K. A. (2012). HIMSS Analytics Report: Security of Patient Data. Kroll Advisory Solutions, New York, NY.
225. 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.
226. 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.
227. Sondergaard, M. (1994). Hofstede's consequences: A study of reviews, citations and replications. Organization Studies, 15(3), 447-456.
228. Srite, M. (1999). The influence of national culture on the acceptance and use of information technologies: An empirical study. AMCIS 1999 Proceedings, 355.
229. Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers & Security, 24(2), 124-133.
230. Starkweather, J. (2013). Multivariate Outlier Detection with Mahalanobis Distance.
231. Straub Jr, D. W. (1990). Effective IS security: An empirical study. Information Systems Research, 1(3), 255-276.
232. Straub Jr, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: a field study. MIS quarterly, 45-60.
233. 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.
234. Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. MIS quarterly, 441-469.
235. Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. The Communications of the Association for Information Systems, 13(1), 63.
236. Suhr, D. (2006). The basics of structural equation modeling. Presented: Irvine, CA, SAS User Group of the Western Region of the United States (WUSS).
237. Tabachnick, B. G. (2001). Clearing Up Your Act: Screening Data Prior to Analysis, Tabachnick, BG & Fidell, LS (eds), Using Multivariate Statistics.
238. Taddesse, W., & Kidan, T. (2005). E-Payment: Challenges and Opportunities in Ethiopia. Journal of Internet Banking & Commerce, 12(2).
239. Tan, B. C., Smith, H. J., Keil, M., & Montealegre, R. (2003). Reporting bad news about software projects: Impact of organizational climate and information asymmetry in an

individualistic and a collectivistic culture. Engineering Management, IEEE Transactions on, 50(1), 64-77.

240. The Hofstede Center, (2013). Geert Hofstede National Culture Dimensions. Available at URL: http://geert-hofstede.com/ethiopia.html. Accessed on July11, 2013.

241. Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. Computers & Security, 24(6), 472-484.

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

243. Timo, D. G. (2009). Culture and Information Security, Outsourcing IT Services in China. (Master thesis, Berlin, Electrical Engineering and Technical University).

244. Tittle, C. R. (1980). Sanctions and social deviance: The question of deterrence. New York: Praeger.

245. Trevino, L. K. (1992). Experimental approaches to studying ethical-unethical behaviour in organizations. Busines's. Ethics Quarterly, 2(2), 121-136

246. Triandis, H. C. (1995). Individualism & collectivism. Westview press. London, UK.

247. Tsakumis, G. T. (2007). The influence of culture on accountants' application of financial reporting rules. Abacus, 43(1), 27-48.

248. 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.

249. Tudor, J. K. (2000). IS Security Architecture: An Integrated Approach to Security in the Organization, Boca Raton, FL: CRC Press.

250. Tushman, M. L., Newman, W. H., & Nadler, D. A. (1988). Executive leadership and organizational evolution: Managing incremental and discontinuous change. Journal of Internet Banking & Commerce, 12(2).

251. 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.

252. Vardi, Y. (2001). The effects of organizational and ethical climates on misconduct at work. Journal of Business Ethics, 29(4), 325-337.

253. Vardi, Y., & Wiener, Y. (1996). Misbehavior in organizations: A motivational framework. Organization science, 7(2), 151-165.

254. Verizon (2012). Data Breach Investigations Report, United States Secret Service, USA. Available at URL:www.verizon.com/enterprise/securityblog. Visited on January, 2014.
255. Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371-376.
256. Vreede, G. J. D., Jones, N., & Mgaya, R. J. (1998). Exploring the application and acceptance of group support systems in Africa. Journal of Management Information Systems, 15(3), 197-234.
257. Walsham, G. (2002). Cross-cultural software production and use: a structuration analysis. MIS quarterly, 24(1), 359-380.
258. Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. European Journal of Information Systems, 18(2), 101.
259. Weston, R. & Gore, PA (2006). A brief guide to structural equation modelling. The counseling psychologist. 34(5), 719- 720.
260. Wenzel, M. (2004). An analysis of norm processes in tax compliance. Journal of economic psychology, 25(2), 213-228.
261. Wheeler, M., and Venter, H. (2006). Change Management: A case study at the University of Pretoria. Proceedings of the Conference on Information Technology in Tertiary Education (CITTE) Pretoria, South Africa.
262. Whitman, M. and Mattord, H. (2008). Management of Information Security 2nd edn. , Thompson Course Technology, Boston, MA.
263. Whitman, M. (2003). Enemy at the gate: threats to information security. Communications of the ACM, 46(8), 91-95.
264. Whitman, M. E., Townsend, A. M., & Aalberts, R. J. (2001). Information systems security and the need for policy. In Information security management: Global challenges in the new millennium (pp. 9-18). IGI Global.
265. Willcocks, L., & Margetts, H. (1994). Risk assessment and information systems. European Journal of Information Systems, 3(2), 127-138.
266. Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. Information and organization, 16(4), 304-324.
267. Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: considering systems risk from a criminological perspective. European journal of information systems, 15(4), 403-414.

268. Willison, R., & Siponen, M. (2007, January). A critical assessment of IS security research between 1990-2004. In Proceedings of 15th European Conference on ISs, St. Gallen, Switzerland (pp. 1551-1559).

269. Wilson, M. & Hash, J. (2003). Computer Security: Building an Information Technology Security Awareness and Training Program. Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8933.

270. Wimbush, J. C., Shepard, J. M., & Markham, S. E. (1997). An empirical examination of the relationship between ethical climate and ethical behaviour from multiple levels of analysis. Journal of Business Ethics, 16(16), 1705-1716

271. Wong, K. K. (1977). Risk analysis and control: a guide for DP managers. NCC Publications.

272. Wood, P. B., Gove, W. R., Wilson, J. A., & Cochran, J. K. (1997). Nonsocial reinforcement and habitual criminal conduct: An extension of learning theory. Criminology, 35(2), 335-366.

273. Woretaw, A., & Lessa, L. (2012, June). Information Security Culture in the Banking Sector in Ethiopia. In 5th ICT 2012 Ethiopia Conference.

274. Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. Journal of the American Society for Information Science and Technology, 58(2), 212-222.

275. Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behaviour, 24(6), 2799-2816.

276. Wu, M. (2006). Hofstede's cultural dimensions 30 years later: A study of Taiwan and the United States. Intercultural Communication Studies, 15(1), 33.

277. Wyatt, G. (1990). Risk-taking and risk-avoiding behaviour: The impact of some dispositional and situational variables. The Journal of Psychology, 124(4), 437-447

278. Wybo, M. D., D. W. Straub. (1989). Protecting organizational information resources. Information Resources Management J. 2(4) 1–15.

279. Yigezu B. J. (2011). Information System Security Audit Readiness: A Case study on Ethiopian Government Organizations. (Master thesis, The Royal Institute of Technology, KTH , Department of Computer and Systems Sciences)

280. Young, K. (2010). Policies and procedures to manage employee Internet abuse. Computers in Human Behaviour, 26(6), 1467-1471.

281. Young, K. S., & Case, C. J. (2004). Internet abuse in the workplace: new trends in risk management. Cyber Psychology & Behaviour, 7(1), 105-111.

282. Zafar, H., & Clark, J. G. (2009). Current state of information security research in IS. Communications of the Association for Information Systems, 24(1), 34.
283. Zhang, Z., Wong, D. S., Xu, J., & Feng, D. (2006). Certificate less public-key signature: security model and efficient construction. In International Conference on Applied Cryptography and Network Security (pp. 293-308). Springer Berlin Heidelberg.
284. Zhi-Jun, W., Hai-Tao, Z., Ming-Hua, W., & Bao-Song, P. (2012). MSABMS-based approach of detecting LDoS attack. Computers & Security, 31(4), 402-417.

APPENDICES

Appendix 1: National Culture and ISS Literature.

Citation	Methodology and Measurement Of National Culture	Independent Variables	Dependent Variables *Moderating Variables*	Relevant Finding(s)
Taco Dols and A.J. Gilbert Silvius (2010)	Survey of big 5 accountancy firms in Belgium and Holland. Hofstede's cultural dimension used	National Culture (PD, IND, MAS, UAI)	Security Non Compliance Behavior	The study confirmed the influence of national culture. Four out of ten non-compliance behavior statements in the study showed a significant difference between the two countries/national cultures
Anat Hovav , John D'Arcy and Kyoungho Lee(2007)	Survey of computer using professionals from US and South Korea. They Use Hofstede Typology of culture.	Security Policies, SETA programs, Computer Monitoring	IS misuse intention. *National Culture.*	The result suggests that security policies have a greater deterrent effect on U.S. employees while the deterrent effectiveness of SETA programs and computer monitoring is stronger for south Korean employees.
Shore, Venkatachalam, Solorzano, Burn, Hassan, and Janczewski (2001)	Survey of students from New Zealand, Hong, Kong, Pakistan, and U.S. • Hofstede's culture Indices	Gender, usage, age, and experience	Attitudes toward intellectual property rights *National culture (IC, UA, PD, MF)*	Findings suggest that cross-cultural values influence attitudes toward intellectual property rights. Students from high power distance countries perceived less of an ethical issue with softlifting (copying software for personal use). Students from high masculinity and individualistic cultures perceived more of an ethical problem with software piracy violations while those from high UA countries did not.
Milberg, Burke, Smith, and Kallman (1995)	Survey of 900 IS audit and control respondents across 30 countries. Hofstede's cultural indices	National culture (UA, IC, PD)	Regulatory approaches to privacy, nature of privacy concerns	Found variance across nationalities of information privacy concerns. Study also identified significant differences in modes of government privacy

				regulation based upon cultural values. Countries exhibiting higher levels of UA and PD exhibited higher levels of government involvement in privacy regulation. Countries exhibiting higher levels of individualism exhibited lower levels of government privacy regulation.
Husted (2000)	Archival data analysis from Business Software Alliance (BSA) • Hofstede's culture indices	National culture (IC, UA, PD, MF)	Level of software Piracy	Results indicate that software piracy is less prevalent in more individualistic (as compared to collectivist) cultural settings.
Einings and Lee (1997)	Survey of Chinese and U.S. students • culture not explicitly measured	Attitudes toward ethical issues (privacy, access, property, and accuracy)	Assessment of IT related Ethical dilemmas *National culture*	Significant differences found between Chinese and U.S. students in how they assess certain information-related ethical dilemmas pertaining to privacy, access, property, and accuracy. Example: Chinese students placed more emphasis on relationships (as opposed to rules and regulations) in addressing certain ethical dilemmas.
Salahuddin M. Alfawaz (2011)	A case study method is used to investigates information security culture in the Saudi Arabia context. A conceptual framework for this study was constructed based on Peterson and Smith's (1997) model of national culture.	organizational and national cultural values	information security culture	The outcomes of the three case stud-ies demonstrate that some of the national, organizational and technological values have clear impacts on the development and deployment of organizations' information security culture.

Appendix 2: The Hypothetical Scenarios

Violation	Scenario
Password sharing	Jack is a low-level manager in a small company where he was recently hired. His company has a strong policy that each computer workstation must be password-protected and that passwords are not to be shared. However, Jack is on a business trip and one of his co-workers needs a file on his computer. Jack expects that sharing his password could save his company a lot of time. He also know that an employee was recently reprimanded for sharing his password. Jack shares his password with his co-worker.
Sharing customer information	Jack is working in a position that requires access to his company customers' personal information. His company's information security policy prohibit him from giving the customer's personal information detail 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 know that an employee was recently reprimanded for sending the data through unauthorized person. Jack gives the data to his friend so that he will send it to the main office.
Workstation logout	Jack is a middle-level manager in a medium-sized company where he was recently hired. His department uses an inventory procurement software application program to make inventory purchases. To ensure that only authorized individuals make inventory purchases, the company has a firm policy that employees must log out or lock their computer when not in use. However, to make work more convenient, Jack's manager directs him to leave his user account logged-in for other employees to freely use. Jack expects that keeping his user account logged-in could save him company time. He also knows that keeping the computer logged-in is a common practice in the industry and an employee recently was reprimanded for leaving the computer logged-in. Jack leaves the computer logged-in when he is finished

Appendix 3: Mean Score for Each of the Constructs in the Main Survey

Constructs	**Mean**
Formal Sanction	4.02
Shame	4.11
Moral Beliefs	3.15
Masculinity	2.50
Perceived Benefit	2.20
Collectivism	3.10
Uncertainty Avoidance	2.30
Power Distance	3.10
CSSE	2.07
Intention to Violate ISSP	2.30

Appendix 4: The Initial Measurement Items and Their Sources

Constructs	Item Code	Item	Source
Intention	Int	What is the chance that you would do what [the scenario character] did in the described scenario?	Paternoster and Simpson (1996)
Power Distance 1	PD1	People in higher positions should make most decisions without consulting people in lower positions	Yoo, Donthu and Lenartowicz (2012)
Power Distance 2	PD2	People in higher positions should not ask the opinions of people in lower positions too frequently.	Yoo, Donthu and Lenartowicz (2012)
Power Distance 3	PD3	People in higher positions should avoid social interaction with people in lower positions.	Yoo, Donthu and Lenartowicz (2012)
Power Distance 4	PD4*	People in lower positions should not disagree with decisions by people in higher positions.	Yoo, Donthu and Lenartowicz (2012)
Power Distance 5	PD5	People in higher positions should not delegate important tasks to people in lower positions.	Yoo, Donthu and Lenartowicz (2012)
Uncertainty Avoidance 1	UA1	People should avoid making changes because things could get worse	Srite, M. (1999)
Uncertainty Avoidance 2	UA2	Change should be avoided when its outcomes are uncertain	Srite, M. (1999)
Uncertainty Avoidance 3	UA3	It is better to work in an organization with specific rules and regulations as opposed to a more flexible organization	Srite, M. (1999)
Uncertainty Avoidance 4	UA4	I would prefer a bad situation that I know about to an uncertain situation which might be better	Srite, M. (1999)
Uncertainty Avoidance 5	UA5*	Providing opportunities to be innovative is more important than requiring standardized work procedures	Srite, M. (1999)
Uncertainty Avoidance 6	UA6*	It is important that people take initiative in their work rather than always following step-by-step instructions	Srite, M. (1999)
Collectivism 1	CL1	Individuals should sacrifice self-interest for the group.	Yoo, Donthu and Lenartowicz (2012)
Collectivism 2	CL2	Individuals should stick with the group even through difficulties	Yoo, Donthu and Lenartowicz (2012)
Collectivism 3	CL3	Group welfare is more important than individual rewards.	Yoo, Donthu and Lenartowicz (2012)

Collectivism 4	CL4	Group success is more important than individual success	Yoo, Donthu and Lenartowicz (2012)
Collectivism 5	CL5*	Individuals should only pursue their goals after considering the welfare of the group.	Yoo, Donthu and Lenartowicz (2012)
Collectivism 6	CL6*	Group loyalty should be encouraged even if individual goals suffer.	Yoo, Donthu and Lenartowicz (2012)
Masculinity 1	MS1	It is more important for men to have a professional career than it is for women.	Yoo, Donthu and Lenartowicz (2012)
Masculinity 2	MS2	Men usually solve problems with logical analysis; women usually solve problems with intuition	Yoo, Donthu and Lenartowicz (2012)
Masculinity 3	MS3	Solving difficult problems usually requires an active, forcible approach, which is typical of men	Yoo, Donthu and Lenartowicz (2012)
Masculinity 4	MS4	There are some jobs that a man can always do better than a woman.	Yoo, Donthu and Lenartowicz (2012)
Moral Beliefs 1	MB1	I feel that the scenario character acted wrongly by violating company IT security policy	Derived from Vance and Siponen (2012)
Moral Beliefs 2	MB2	How morally wrong would it be to do what the person did in the scenario?	Vance and Siponen (2012)
Moral Beliefs 3	MB3	It is moral wrong to violate company information systems security policies?	Derived from Vance and Siponen(2012)
Perceived Benefits 1	PB1	If I would do what the scenario character did, I would save time.	Vance and Siponen (2012)
Perceived Benefits 2	PB2	If I would do what the scenario character did, I would save work time	Vance and Siponen (2012)
Perceived Benefits 3	PB3	Noncompliance with the information security policies saves work time.	Vance and Siponen (2012)
Perceived Benefits 4	PB4	Noncompliance with the information security measure saves employees' time	Vance and Siponen (2012)
Certainty of Shame 1	SC1	How likely is it that you would be ashamed if co-workers knew that you had violated company information security policy?	Vance and Siponen(2012)
Certainty of Shame 2	SC2	How likely is it that you would be ashamed if others knew that you had violated the company information security policy?	Vance and Siponen(2012)

Certainty of Shame 3	SC3	How likely is it that you would be ashamed if managers knew that you had violated the company information security policy?	Vance and Siponen(2012)
Severity of Shame 1	SS1	How much of a problem would it be if you felt ashamed that co-workers knew you had violated the company information security policy?	Vance and Siponen(2012)
Severity of Shame 2	SS2*	How much of a problem would it be if you felt ashamed that others knew you had violated the company information security policy?	Vance and Siponen(2012)
Severity of Shame 3	SS3*	How much of a problem would it be if you felt ashamed that managers knew you had violated the company information security policy?	Vance and Siponen(2012)
Computer security self-efficacy 1	CSSE 1	I would feel comfortable following most of the information security policies on my own	Herath and Rao(2009a)
Computer security self-efficacy 2	CSSE 2	If I wanted to, I could easily follow information systems security policies on my own	Herath and Rao(2009a)
Computer security self-efficacy 3	CSSE 3	I would be able to follow most of the information systems security policies even if there was no one around to help me	Herath and Rao(2009a)
Formal sanctions—certainty 1	FSC1	What is the likelihood you would receive sanctions if you violated the company information security policy?	Derived from Vance and Siponen(2012)
Formal sanctions—certainty 2	FSC2	What is the likelihood that you would be formally sanctioned if management learned that you had violated company information security policy?	Derived from Vance and Siponen(2012)
Formal sanctions—certainty 3	FSC3	What is the likelihood that you would be formally reprimanded if management learned you had violated company information security policy?	Derived from Vance and Siponen(2012)
Formal sanctions—severity 1	FSS1	How much of a problem would it be if you received severe sanctions if you violated the company information security policy?	Vance and Siponen(2012)
Formal sanctions—severity 2	FSS2	How much of a problem would it create in your life if you were formally sanctioned for doing what [the scenario character] did?	Derived from Vance and Siponen(2012)
Formal sanctions—severity 3	FSS3	How much of a problem would it create in your life if you were formally reprimanded for doing what [the scenario character] did?	Derived from Vance and Siponen(2012)

*Note: * refers to items removed based on the result of instrument validation test*

Appendix 5: The Research Instruments

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 labeled 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 organization's information systems security policies on my own.					
2	If I wanted to, I could easily follow my organization's information systems security policies on my own.					
3	I would be able to follow most of my organization's information systems security policies even if there was no one around to help me.					
4	People in higher organizational positions should make most decisions without consulting people in lower positions.					
5	People in higher organizational positions should not ask the opinions of people in lower positions too frequently.					
6	People in higher organizational positions should avoid social interaction with people in lower positions.					
7	People in lower organization positions should not disagree with decisions by people in higher positions.					
8	People in higher organizational 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 organization with specific rules and regulations as opposed to a more flexible organization.					

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 Standardized 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	Noncompliance with an organization's information systems security policies saves work time					
26	Noncompliance with an organization'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 details of 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 (criticized) for sending data through an unauthorized 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 labeled 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 (criticized) for doing what Jack did?					

Section Three

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**
35	How likely would you 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 (criticized) 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 would you 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 would you 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)

45. Please indicate your gender ___ Female ___ Male
46. How realistic is the given scenario?
    ___Non-realistic _____Somewhat realistic ____Realistic
47. What is your highest completed education certification?
    ___ High school certificate
    ___diploma
    ___ Bachelor's degree
    ___ Master's degree
    ___ Doctoral degree
    ___Other, please specify _____
48. What is your age? _____ years
49. Years of computer usage:
    ___ ≥ 10years ___ ≥ 5 years ___ ≥ 2 years ___< 2 year
50. What is your current employment status?
    _____Student ____Employee _____Retired _____Other

Appendix 6: An Informed Consent Form for the Participants

Consent Form

ADDIS ABABA UNIVERSITY IT DOCTORAL PROGRAM

Informed Consent for Participants in Research Projects

Title of Project: Information Systems Security Policy Violation

Investigators:

TilahunMuluneh	Dr. France Belanger	Dr. TibebeBeshah
Ph.D. Candidate	Professor and Byrd Research Fellow	Coordinator,IT Ph.D. Program(IS track)
Lecturer at Addis Ababa University	ACIS Department, Virginia	School of information Systems, AAU
Tilahunmuluneh@yahoo.com	TechBelanger@vt.edu	Tibebe.Beshah@gmail.com
(+251)911935006	(1)540-231-6720	(+251)911457318

I. Purpose of this Research/Project
Thank you for participating in this survey. Your participation will help us better understand how people make decisions to Violate/comply with Information Systems Security Policies (ISSP).

II. Procedures
As a participant in this research project, your assistance will be needed to answer a survey.

III. Risks
There are no personal risks associated with participating in this study.

IV. Benefits
No promise or guarantee of benefits is made to encourage you to participate in this study. If you would like a copy of the results of this study, please let the researchers know and it will be provided to you at the conclusion of the research.

V. Extent of Anonymity and Confidentiality
No personally identifiable information is being collected from you and all information you provide will be combined with the other data and analyzed, and reported in the aggregate. Responses will be kept confidential at all times, and only the members of the research team will have access to the data. Participation is completely voluntary.

VI. Compensation
There is no compensation for participating in this research.

VII. Freedom to Withdraw
You are free to withdraw from this study at any point in time. If you choose to no longer participate there will be no repercussions to you.

VIII. Subject's Responsibilities
You have the following responsibilities: answer the survey questions.

Appendix 7: Mahalanobis D^2 Distance Matrix for All Variables

Case number	Mahalanobis d-squared	D^2/DF (df=33)	Case number	Mahalanobis d-squared	D^2/DF (df=33)	Case number	Mahalanobis d-squared	D^2/DF (df=33)
114	62	2	18	41	1	16	37	1
32	58	2	58	41	1	25	37	1
108	56	2	157	41	1	113	36	1
65	53	2	171	41	1	137	36	1
150	52	2	125	41	1	26	36	1
5	51	2	20	41	1	27	36	1
1	50	2	187	41	1	52	36	1
51	50	2	8	40	1	116	36	1
133	49	1	200	40	1	90	36	1
131	49	1	34	40	1	79	36	1
185	48	1	118	40	1	129	36	1
119	48	1	41	40	1	190	36	1
198	47	1	199	40	1	31	35	1
155	47	1	33	40	1	191	35	1
126	47	1	102	39	1	61	35	1
161	46	1	71	39	1	134	35	1
100	46	1	127	39	1	202	35	1
72	46	1	142	39	1	176	35	1
170	45	1	3	39	1	177	35	1
110	44	1	204	39	1	49	35	1
178	44	1	195	39	1	54	34	1
179	44	1	103	38	1	172	34	1
101	43	1	87	38	1	132	34	1
43	43	1	91	38	1	56	34	1
104	43	1	120	38	1	146	34	1
2	43	1	188	37	1	115	34	1
149	43	1	35	37	1	117	33	1
160	43	1	9	37	1	136	33	1
107	42	1	124	37	1	7	33	1
24	42	1	141	37	1	162	33	1
154	42	1	50	37	1	78	33	1
80	42	1	166	37	1	164	33	1
19	42	1	88	37	1	37	33	1
75	42	1	73	37	1	83	25	1
30	33	1	76	29	1	46	25	1
109	33	1	175	29	1	47	25	1

111	33	1	4	29	1	165	25	1
189	33	1	42	29	1	152	24	1
194	33	1	14	29	1	44	24	1
174	32	1	151	29	1	93	24	1
140	32	1	208	29	1	158	24	1
63	32	1	121	29	1	197	23	1
15	32	1	28	29	1	67	23	1
59	32	1	62	28	1	130	23	1
173	32	1	201	28	1	96	23	1
181	32	1	169	28	1	167	22	1
45	32	1	6	28	1	168	22	1
138	32	1	17	28	1	64	22	1
186	32	1	70	28	1	68	22	1
57	32	1	147	28	1	39	22	1
145	31	1	156	28	1	66	22	1
99	31	1	203	28	1	206	21	1
182	31	1	192	28	1	163	21	1
148	31	1	38	28	1	29	20	1
74	31	1	106	28	1	10	20	1
95	31	1	180	27	1	139	20	1
11	31	1	144	27	1	48	20	1
105	30	1	40	27	1	81	19	1
85	30	1	209	26	1	53	19	1
55	30	1	60	26	1	205	19	1
12	30	1	207	26	1	128	19	1
77	30	1	94	26	1	112	19	1
86	30	1	82	26	1	143	18	1
22	30	1	193	26	1	36	18	1
196	30	1	122	26	1	123	18	1
153	30	1	23	26	1	135	18	1
89	30	1	92	26	1	13	18	1
184	30	1	97	25	1	84	13	0
69	18	1	210	16	0	159	13	0
21	17	1	183	15	0	98	11	0

Appendix 8: Test of Normality for All Variables

Variables	Skewness[1]	Kurtosis[1]	Variables	Skewness[1]	Kurtosis[1]
CSSE1	-1.82	-0.33	*PB2*	0.43	-1.39
CSSE2	0.27	-1.26	*INT*	2.39	0.21
CSSE3	-0.85	-1.32	*MB1*	-1.8	-0.34
PD1	2.42	0.67	*MB2*	0.17	-1.16
PD2	0.35	-1.4	*MB3*	-0.75	-1.22
PD3	2.45	0.81	*PB3*	-1.6	0.02
PD5	1.34	0.15	*PB4*	-2.42	0.28
UA1	2.25	0.79	*FSS1*	-2.24	0.24
UA2	2.33	0.32	*FSS2*	-2.23	-0.02
UA3	-0.04	-0.45	*FSS3*	-2.21	-.03
UA4	0.84	-0.59	*SC1*	-2.35	-0.48
CL1	-0.66	-0.38	*SS1*	-1.5	-0.97
CL2	-2.7	1.67	*SC2*	-2.32	0.85
CL3	-1.83	-0.61	*SC3*	-2.11	0.35
CL4	-0.67	0.02	*FSC1*	-1.82	1.43
MS1	2.49	-0.52	*FSC2*	-2.02	0.01
MS2	0.69	-0.61	*FSC3*	-1.63	-0.49
MS3	2.11	0.13	*SS3*	-2.36	-0.53
MS4	-0.27	-1.88			
PB1	1.87	0.03			

[1] Standard error for skewness is .343 and standard error of kurtosis is .674 .

The skewness and kurtosis values are critical ratios (Zskewness and Zkurtosis values) i.e. after each skewness and kurtosis value was divided by their respective standard error value.

Appendix 9: Test for Common Method Bias:-Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	9.902	22.505	22.505	9.902	22.505	22.505
2	4.077	9.266	31.771			
3	3.279	7.452	39.224			
4	2.757	6.265	45.489			
5	2.415	5.488	50.977			
6	2.270	5.159	56.136			
7	2.195	4.988	61.124			
8	1.877	4.266	65.390			
9	1.600	3.637	69.027			
10	1.484	3.372	72.399			
11	1.220	2.774	75.172			
12	1.078	2.450	77.622			
13	.952	2.163	79.785			
14	.893	2.029	81.813			
15	.875	1.988	83.801			
16	.774	1.759	85.560			
17	.747	1.699	87.258			
18	.640	1.454	88.712			
19	.556	1.264	89.977			
20	.529	1.201	91.178			
21	.484	1.099	92.277			
22	.452	1.026	93.303			
23	.419	.952	94.255			
24	.378	.860	95.115			
25	.296	.672	95.787			
26	.294	.669	96.456			
27	.243	.552	97.008			
28	.230	.523	97.531			
29	.179	.406	97.937			
30	.155	.353	98.290			

Appendix 10: The Recruitment Document

Invitation For Participation

Greetings [name],

We are currently working on a research project that is concerned with employees' information systems security policy violation behavior.

As part of this research project, we would like you to take a survey, which asks you various questions related to your information security policy violation behavior. However, none of the questions should allow us to identify any participant individually. We are interested in aggregate results.

Your participation will help us to better understand determinants of employee information security policy violation. Your participation is completely voluntary. If you would like a copy of the results of this study, please let the researchers know and it will be provided to you at the conclusion of the research.

If you have any questions please let me know.

Thanks,

Appendix 11: The Final Measurement Items and Their Sources

Constructs	Item Code	Item	Source
Intention	Int	What is the chance that you would do what [the scenario character] did in the described scenario?	Paternoster and Simpson (1996)
Power Distance 1	PD1	People in higher positions should make most decisions without consulting people in lower positions	Yoo, Donthu and Lenartowicz (2012)
Power Distance 2	PD2	People in higher positions should not ask the opinions of people in lower positions too frequently.	Yoo, Donthu and Lenartowicz (2012)
Power Distance 3	PD3	People in higher positions should avoid social interaction with people in lower positions.	Yoo, Donthu and Lenartowicz (2012)
Power Distance 5	PD5	People in higher positions should not delegate important tasks to people in lower positions.	Yoo, Donthu and Lenartowicz (2012)
Uncertainty Avoidance 1	UA1	People should avoid making changes because things could get worse	Srite, M. (1999)
Uncertainty Avoidance 2	UA2	Change should be avoided when its outcomes are uncertain	Srite, M. (1999)
Uncertainty Avoidance 3	UA3	It is better to work in an organization with specific rules and regulations as opposed to a more flexible organization	Srite, M. (1999)
Uncertainty Avoidance 4	UA4	I would prefer a bad situation that I know about to an uncertain situation which might be better	Srite, M. (1999)
Collectivism 1	CL1	Individuals should sacrifice self-interest for the group.	Yoo, Donthu and Lenartowicz (2012)
Collectivism 2	CL2	Individuals should stick with the group even through difficulties	Yoo, Donthu and Lenartowicz (2012)

Collectivism 3	CL3	Group welfare is more important than individual rewards.	Yoo, Donthu and Lenartowicz (2012)
Collectivism 4	CL4	Group success is more important than individual success	Yoo, Donthu and Lenartowicz (2012)
Masculinity 1	MS1	It is more important for men to have a professional career than it is for women.	Yoo, Donthu and Lenartowicz (2012)
Masculinity 2	MS2	Men usually solve problems with logical analysis; women usually solve problems with intuition	Yoo, Donthu and Lenartowicz (2012)
Masculinity 3	MS3	Solving difficult problems usually requires an active, forcible approach, which is typical of men	Yoo, Donthu and Lenartowicz (2012)
Masculinity 4	MS4	There are some jobs that a man can always do better than a woman.	Yoo, Donthu and Lenartowicz (2012)
Moral Beliefs 1	MB1	I feel that the [scenario] character acted wrongly by violating company IT security policy	Derived from Vance and Siponen (2012)
Moral Beliefs 2	MB2	How morally wrong would it be to do what the person did in the scenario?	Vance and Siponen (2012)
Moral Beliefs 3	MB3	It is moral wrong to violate company information systems security policies?	Derived from Vance and Siponen(2012)
Perceived Benefits 1	PB1	If I would do what [the scenario character] did, I would save time.	Vance and Siponen (2012)
Perceived Benefits 2	PB2	If I would do what [would do what [the scenario character] did, I would save work time	Vance and Siponen (2012)
Perceived Benefits 3	PB3	Noncompliance with the information security policies saves work time.	Vance and Siponen (2012)

Perceived Benefits 4	PB4	Noncompliance with the information security measure saves employees' time	Vance and Siponen (2012)
Certainty of Shame 1	SC1	How likely is it that you would be ashamed if co-workers knew that you had violated company information security policy?	Vance and Siponen(2012)
Certainty of Shame 2	SC2	How likely is it that you would be ashamed if others knew that you had violated the company information security policy?	Vance and Siponen(2012)
Certainty of Shame 3	SC3	How likely is it that you would be ashamed if managers knew that you had violated the company information security policy?	Vance and Siponen(2012)
Severity of Shame 1	SS1	How much of a problem would it be if you felt ashamed that co-workers knew you had violated the company information security policy?	Vance and Siponen(2012)
Computer Security Self-efficacy 1	CSSE1	I would feel comfortable following most of the information security policies on my own	Herath and Rao(2009a)
Computer Security Self-efficacy 2	CSSE2	If I wanted to, I could easily follow information systems security policies on my own	Herath and Rao(2009a)
Computer Security Self-efficacy 3	CSSE3	I would be able to follow most of the information systems security policies even if there was no one around to help me	Herath and Rao(2009a)
Formal sanctions—certainty 1	FSC1	What is the likelihood you would receive sanctions if you violated the company information security policy?	Derived from Vance and Siponen(2012)
Formal sanctions—certainty 2	FSC2	What is the likelihood that you would be formally sanctioned if management learned that you had violated company information security policy?	Derived from Vance and Siponen(2012)
Formal sanctions—certainty 3	FSC3	What is the likelihood that you would be formally reprimanded if management learned you had violated company information security policy?	Derived from Vance and Siponen(2012)
Formal sanctions—severity 1	FSS1	How much of a problem would it be if you received severe sanctions if you violated the company information security policy?	Vance and Siponen(2012)

Formal sanctions—severity 2	FSS2	How much of a problem would it create in your life if you were formally sanctioned for doing what [the scenario character] did?	Derived from Vance and Siponen(2012)
Formal sanctions—severity 3	FSS3	How much of a problem would it create in your life if you were formally reprimanded for doing what [the scenario character] did?	Derived from Vance & Siponen(2012)

Appendix 12: The Unstandardized Estimate, Standard Error (S.E.), Critical Ration (C.R.), SMC, and P value for each of the constructs Items.

Construct	Item	Unstandardized Estimate	S.E.	C.R.	SMC	P
Power Distance	PD1	0.942	0.105	8.947	0.62	***
	PD2	1.062	0.119	8.947	0.69	***
	PD3	0.933	0.123	7.569	0.53	***
	PD5	1.3	0.133	9.799	0.85	***
Collectivism/ Individualism	CL4	1.344	0.125	10.752	0.63	***
	CL3	1.105	0.084	13.114	0.8	***
	CL2	0.847	0.075	11.286	0.64	***
	CL1	0.744	0.069	10.752	0.49	***
Uncertainty Avoidance	UA4	0.943	0.107	8.782	0.62	***
	UA3	0.806	0.101	7.947	0.53	***
	UA2	0.714	0.095	7.551	0.49	***
	UA1	1.4	0.185	7.551	0.8	***
Masculine/ Feminine	MS4	1.43	0.264	5.426	0.5	***
	MS3	1.43	0.248	5.775	0.84	***
	MS2	0.699	0.121	5.775	0.35	***
	MS1	0.94	0.186	5.052	0.41	***
Perceived Benefits	PB4	1.009	0.067	15.083	0.9	***
	PB3	0.991	0.066	15.083	0.8	***
	PB2	0.875	0.069	12.731	0.77	***
	PB1	0.775	0.078	9.891	0.59	***
Moral Beliefs	MB3	1.087	0.085	12.803	0.79	***
	MB2	1.07	0.087	12.357	0.8	***
	MB1	1.163	0.092	12.646	0.82	***
Shame	SC3	0.896	0.097	9.27	0.63	***
	SS1	0.84	0.068	12.439	0.67	***
	SC1	1.292	0.109	11.813	0.86	***
	SC2	1.19	0.096	12.439	0.93	***
Formal Sanction	FSS1	1.176	0.178	6.625	0.54	***
	FSC2	1.485	0.192	7.726	0.78	***
	FSC1	1.17	0.18	6.499	0.52	***
	FSC3	0.855	0.13	6.565	0.48	***
	FSS2	1.046	0.177	5.908	0.42	***
	FSS3	1.17	0.178	6.565	0.53	***
CSSE	CSSE1	1.128	0.126	8.952	0.83	***
	CSSE2	0.886	0.099	8.95	0.69	***
	CSSE3	1.004	0.107	.422	0.78	***