Association for Information Systems
AIS Electronic Library (AISeL)

MCIS 2016 Proceedings

Mediterranean Conference on Information Systems (MCIS)

2016

Investigating the Moderating Impact of National Culture in Information Systems Security Policy Violation: The Case of Italy and Ethiopia

Tilahun Muluneh Arage
Addis Ababa University, tilahunmuluneh2006@yahoo.com

France Belanger
Virginia Tech, belanger@vt.edu

Tibebe B. Tesema
Addis Ababa University, tibebe.beshah@gmail.com

Follow this and additional works at: http://aisel.aisnet.org/mcis2016

Recommended Citation

INVESTIGATING THE MODERATING IMPACT OF NATIONAL CULTURE IN INFORMATION SYSTEMS SECURITY POLICY VIOLATION: THE CASE OF ITALY AND ETHIOPIA

Research in Progress

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

France Belanger, Virginia Tech University, VA, USA, belanger@vt.edu

Tibebe B. Tesema, Addis Ababa University, Ethiopia, Tibebe.beshah@gmail.com

Abstract

Information systems security (ISS) has become one of the top agendas of companies located in the developed world. Despite this fact, there is an increasing trend in the types and frequency of ISS breaches. Most of the time researchers and practitioners focus on threat that are caused by external agents while most of the threats are originated from insiders. In addition to this, the majority of the investments and researches around ISS are limited to technically oriented solutions. It is now realized that the technical approach alone couldn't bring the required level of ISS, and this led ISS researchers to embark on socio-technical approaches. One of the critical social factors that has been given little emphasis is culture. Thus, this research investigates the impact of national culture on employees' ISS behaviour. Specifically, it answers the question "what is the moderating impact of national culture on the influence of ISS countermeasures on employees' intention to violate ISS policies?" We will develop and test an empirical ISS compliance model, using rational choice theory and national culture constructs. Survey will be used to collect data from Italy and Ethiopia.

Keywords: Information Systems Security, Information Systems Security Policy Violation Insiders, National Culture, Rational Choice Theory, Information Systems Security Countermeasures

1. Introduction

Despite the existence of IS security policies (ISSP), protecting the ISS (information systems security) becomes a moving target for most organizations around the world (Sommestad et al., 2013). Most of the time, the ISS specialists and researchers have been focusing on threat of external origins (Magklaras et al., 2006); however, it is now becoming more apparent that most of the ISS threats are originated from insiders (D'Arcy et al., 2009). Moreover, researchers like Magklaras et al. (2006) clearly stated that the internal incidents are here to stay and their mitigation should be a priority issue for IT professionals. More recently, practitioners and academics have started to realize that ISS cannot be achieved through only technological tools and effective organizational ISS should emphasis users' ISS behavior (Hamill et al., 2005). Since this is a new area, the knowledge of end users' ISS behavior and factors affecting this behavior are at an embryonic stage (Herath & Rao, 2009b). In this regards, one of the most significant factors to shape human ISS behavior is culture (Schiffman & Kanuk, 1997). To this end, our study will bring rational choice theory (RCT) and national culture together to give a more behavioral explanation to the ISS problem.

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

2. Background

ISS threats that are caused by insiders are not limited to developing countries; rather, it is a global problem. Hence, in the following paragraphs, we summarize important information related to insiders and ISS breaches from global and local (in Ethiopia) perspectives. In this research, insider is defined as "a person that has legitimately given the capability of accessing one or more components of IT infrastructure" (Magklaras et al., 2006, pp. 3). According to Mercury (2003), companies all over the world are losing more than US $2 trillion due to ISS breaches. Most of the breaches are caused by insiders (D'Arcy et al., 2007). Since insiders do have better access to the companies' secured information, they can bring catastrophic consequences to their company in terms of financial as well as non-financial aspects (D'Arcy et al., 2009). The Cyber Security Watch Survey (2010) annual report indicates more than US $2 billion in losses to organizations due to ISS breaches between 1997 and 2007. According to the report, companies might continue to suffer more losses in the future, given that

the overall types of attacks are doubled in the specified time period. More recently, the Cyber Security Watch Survey (2012) annual report indicates that insiders attack increased from 41% in 2004 to 53% in 2011. To make matters worse, insider abuse of company IS is the second most frequent (44%) ISS problem next to virus incident (49%) and well above outsiders (29%) (Richardson, 2008). Because only a fraction of ISS incidents is actually discovered, the figures from different reports and research might be lower than the actual facts (Hoffer & Straub, 1989; Whitman, 2003).

The above discussion clearly shows how insiders pose great threats to their organizational ISS at a global perspective. When we come to countries in the developing economy, we find that there is a lack of research in the areas of ISS breaches in such countries (Salahuddin, 2011). Thus, it is difficult to find out the actual financial as well as non-financial losses attributed to ISS breaches caused by insiders. In the case of Ethiopia, according to Arage et al. (2015), Ethiopian Revenue and Custom Authority is one of the companies that suffer the consequence of an ISS breach caused by their own employees. The authors discussed that the noncompliance of an employee to his company ISS policy costs the company 13,000,000 Birr. In another incident of ISS breaches, the Ethiopian Airlines has terminated eleven employees working in different departments citing violation of the ISSP rules and procedures they were expected to abide by and abuse of the IS that they had privileged access to (Arage, et al., 2015).

As can be understood from the above information, the ISS breach problem is increasing at an alarming rate. To this end, some researchers in Europe and the USA try to address the noncompliance problem by giving some level of stress for both technical and social factors that might have an impact on reducing the current noncompliance problem. In this regards, we can mention the work of Dols & Silvius (2010) in Europe and the work of D'Arcy et al. (2007) in the USA that try to investigate the influence of national culture on employees' compliance with ISSP. But when we come to developing country context, it is very difficult to get research that try to shed light on the behavioral perspective of ISS. There is a particular lack of attention in the current IS literature about developing countries, and also how factors such as national and organizational culture relate to individual's attitudes towards ISS and its management (Salahuddin, 2011).

3. Theoretical Foundation

To study employees' ISS behavior, a number of theories have been used over the years. In this regards, theories such as: protection motivation theory (PMT) (e.g. Pahnila et al., 2007, Siponen et al., 2006), general deterrence theory (GDT) (e.g. Kankanhalli et al., 2003; D'Arcy & Hovav, 2007; D'Arcy et al., 2009; Straub, 1990), and agency theory (e.g. Herath & 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 is based on GDT and /or PMT, which are mainly fear based strategies; that is, fear of sanction and threat to organization ISS. This will only give a partial explanation to the problem of ISSP violation (Vance & Siponen, 2012). Thus, in order to have a better view on "why employees violate ISSP?" we need to use theories that go beyond this scope. In this regard, RCT goes beyond this limitation and includes perceived benefits and moral beliefs as additional determinants of ISS compliance. 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 decisions towards obeying or violating rules (Vance & Siponen, 2012). Therefore, we believe that use the RCT as one of our theoretical lenses is justified and also appropriate.
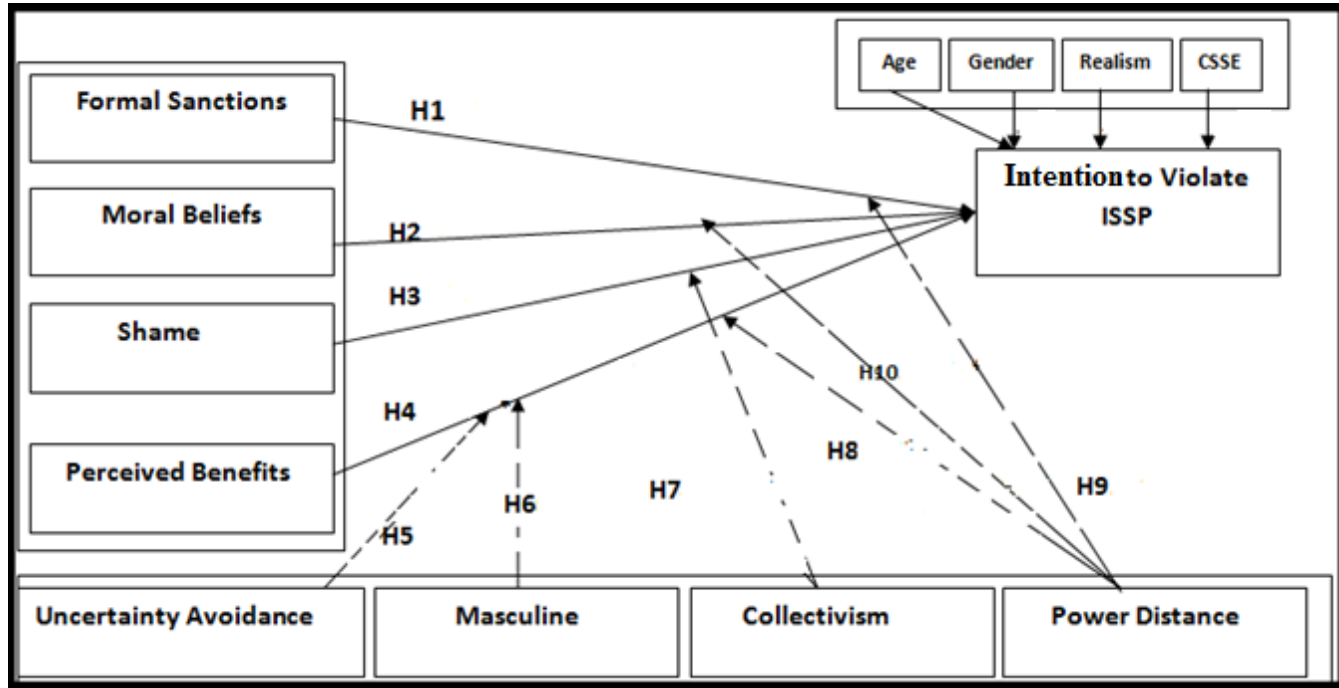
4. Research Model and Hypotheses

Figure 1: The Proposed Research Model

Straub (1990) reported that Formal sanctions have a high impact on reducing IS abuse. In addition to this, considerable number of researchers (e.g. Tudor, 2000; Kankanhalli, 2003; Herath & Rao, 2009a; Siponen et al., 2007) tried to investigate whether the use of sanction reduce ISS problems or not, and found that these deterrent measures improve the security level and reduce the abuse level.

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

Criminological studies show that moral beliefs explain individuals intention to engage in a deviant behavior like corporate crime (Paternoster & Simpson, 1996), tax evasion (Wenzel, 2004), and sexual abuse (Bachman et al., 1992). With respect to ISS area, researchers (e.g. Li et al., 2010; Vance & Siponen, 2012) suggest that moral reasoning and individuals' values can be predictors of individuals' compliance with ISSP.

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

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

H3: Shame is negatively related to intention to violate ISSP

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

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

Since people in low uncertainty avoidance (UA) societies do not fear the risk of becoming jobless or making a wrong choice, they change jobs more often, with the intention of getting a better job, than those in high UA societies (Timo, 2009). With a similar logic, since ISSP violations might bring a

number of unknown consequences or threats to individuals, those in high UA societies are more likely to comply with ISSP, even if there are some benefits of violation

H5: The higher the degree of UA, the weaker the impact of perceived benefits on intention to violate ISSP

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

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

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

H7: The higher the degree of collectivism, the stronger the impact of shame on intention to violate ISSP

Countries with high power distance (PD) are found to be associated with a high level of tax evasion and corruption (Tsakumis, 2007; Husted, 1999). This could mean, if there exists any benefit of breaking the rule, then the high PD society might engage in illegal activity more than their low PD counterparts. Moreover, some empirical works show employees in high PD society break IT rules more often than low PD society (D'Arcy et al., 2007; Dols & Silvius, 2010). This means the fear of formal sanctions in high PD society is less strong than low PD society.

H8: The higher the degree of PD, the stronger the impact of perceived benefits on intention to violate ISSP

H9: The higher the degree of PD, the weaker the impact of formal sanctions on ISSP violation

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

H10: The higher the degree of PD, the weaker the impact of moral beliefs on intention to violate ISSP

5. Research Methodology

The underlying approach used here lies in the positivist paradigm. The choice for the positivist paradigm is done because of the fact that the purpose of the research is to develop and validate an empirical model. The research will utilize questionnaire-based data gathering technique. In addition to the traditional survey method, we will assess intention to violate ISSP and RCT constructs by using a scenario method. Scenario-based research is well suited to study issues that measure or involve ethical/unethical behavior (Pogarsky, 2004). We will use the Hofstede's (1980) model of cultural dimensions, because it has been rigorously validated in previous cross-cultural studies over time (Sondergaard, 1994). SEM based analysis will be used to evaluate the hypothesis. The research population includes companies located in Ethiopia and Italy. The reason to include two countries in the study is because our study is a cross cultural study and it is a must to take sample from multiple countries with varying cultures. According to Hofstede's(1980) cultural dimention (see Figure 2) the two countries

do have a considerable cultural difference. We plan to dispatch a considerable number of question-naires in both countries so that we can get enough responses for analysis. Anderson & Gerbing (1984) suggest that a sample size of 150 or more will be needed to obtain parameter estimates that have standard errors small enough to be of practical use. We will use previously validated instruments whenever possible. SPSS Amos software will be used to run different types of SEM based statistical analysis.
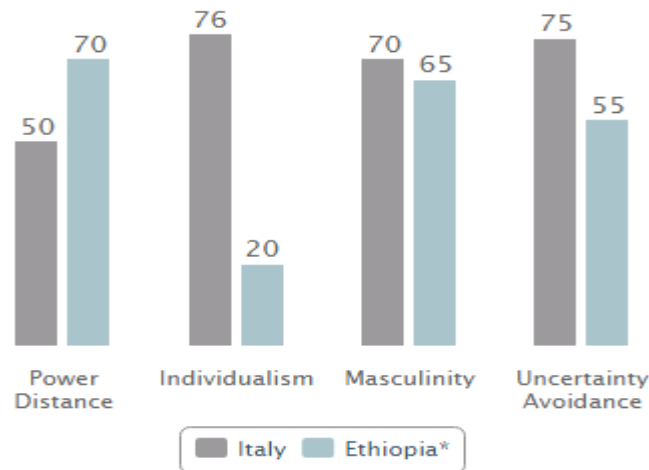

Figure 2: Comparison of the Cultural Dimension between Ethiopia and Italy

6. Contribution

Increasing numbers of researchers argue that, in order to better prepare to tackle the ISS problem, the human element needs to be well studied and addressed (Bjork & Jiang, 2006; D'Arcy et al., 2007; Timo, 2009). Thus, in this study we contribute in investigating national culture as one of the most important human related factors that is believed to have an impact on employees' ISSP compliance behavior. In this regards, some researchers indicate the importance of considering national culture in IT related issues. For example, a review of the existing literature by Dol & Silvius (2010) has clearly identified culture as one of the five factors that are considered to have an influence on employees' ISS policy compliance behavior. If we look at the ISS literatures, specifically in Africa, there is hardly any attempt to this end (Salahuddin, 2011), and this creates an opportunity for researchers to conduct research in this area. In this regards, this research will bring the knowledge of how national culture influence employees' intention towards ISSP violation and it gives insight on how to improve employees' ISS compliance. On the other hand, this research is the first study to see the ISS problem from the perspective of RCT and national culture perspective, and this will contribute to the cumulative theory building effort in the field of ISS. In addition to this, the output from this research can serve as an input for the development of ISSP and different types of ISS awareness and training programs by providing further understanding of factors that affect the successful implementation of ISSP. Moreover, this research output could also be an important input for companies that do have an outsourcing ambition of IT related services in Italy and Ethiopia. Knowing the impact of cultural dimensions on ISSP violation, service providers from abroad can identify and manage potential problems and risks (Timo, 2009).

7. Limitations

The output from this research might not be applicable for countries that do have different cultural dimensions. Since it is not possible to include organizations that do not have ISSP, the research population for the study is limited to employees who work only in companies that have a well-established ISSP. Even though culture can be studied at different label (national, organizational, and subunit level), this research is limited to national culture. National culture is more powerful than organizational culture in influencing employees' behavior (Robbins, 2005).

References

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

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

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

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

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34(3), 523-548.

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

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

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

D'Arcy, J. and Herath, T., 2011. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings.European Journal of Information Systems, 20(6), pp.643-658.

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

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

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

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

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

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

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

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

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

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

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

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

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.

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

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

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

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

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

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

Paternoster, R. and Simpson, S., 1996. Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. Law and Society Review, pp.549-583.

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

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

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

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

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

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

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

Sommestad, T., Ekstedt, M., & Holm, H. (2013). The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures. Systems Journal, IEEE, 7(3), 363-373.

Sondergaard, M.(1994). "Hofstede's consequences: A study of reviews, citation and replications," organization studies, 15(3), 447-456.

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

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

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

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

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

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