Employees Information System Misuse: Insights from National culture and Criminological Theories

Yimer Mohammed, Tibebe Beshah
AAU,
yimoh_fast @yahoo.com

Merril Warkentin
Mississippi State University, USA.

Abstract

IS resources are expected to promote competitiveness and profitability, however, employees' misuse causes considerable security threats. To that, global organizations are investing evermore to defend their cyberspaces, but they are not able to fully protect them. Cultural factors contributed to influence employees' behaviours, but studies are lacking in Africa. So, developing a conceptual research model that comprising cultural dimensions and criminological theories will probably explain the factors that help to design socio-culturally appropriate countermeasures in Ethiopia.

Keywords
IS misuse behaviour, culture, security measure awareness, neutralization techniques, deterrence theory, positivist paradigm.

1. Introduction
Presently, Information Systems (InfoSys) applications and tools in and across organizations create tremendous potentials to easily access and practice in a variety of contexts, circumstances and conditions (Li and Siponen, 2011) to increase effectiveness and productivity. However, risks associated with InfoSys security problems from the use of Infosys resources pose considerable challenges and even result in "corporate liability", "loss of credibility", and "huge monetary damage" to many organizations (Bulgurcu et al. 2010), and become a worldwide phenomenon. That is the reason why organizations are investing a lot to try to deter and protect the problems using technical, administrative, procedural, physical controls and enforcing of InfoSys security policies worldwide (D'Arcy and Herath, 2011). Whatsoever the investment and effort offered, the problems are ever increasing and becoming more sever (Haeussinger and Kranz, 2013) due to the human behavioural factors (Montesdioca and Macada, 2015) that take considerable share towards InfoSys security threat incidences (Alnatheer, 2012).

Employee related deviant uses and practices of those resources are increasingly affecting organizations from time to time (D'Arcy and Herath, 2011; Barlow et al. 2013). In that regard, strong working procedures, policies and deterrence techniques are not guarantee to stop employees misuse intension (Alnatheer, 2012), because the culture of practicing InfoSys resources are ever-changing and becoming complex to manage them accordingly (Montesdioca and Macada, 2015). Moreover, employees are becoming potentially insiders as they have knowledge and privilege to access and practice InfoSys resources and by that means they may pose security risks (Colwill, 2009), because they are the "weakest link" to organizations (Ifinedo, 2012). That means, employees are both security assets and vulnerable InfoSys security weak-links, and as a result they can be both part of the problems and part of the solutions (Woretaw et al. 2019). InfoSys components including working procedures, workplace settings, places that offer InfoSys resources and working situation may also help employees to engage in InfoSys misuse behaviour (Maçada and Luciano 2010). So, investigating employees' psychology, including their beliefs, attitudes and perceptions towards creating InfoSys security positive cultures should be well- thought-out (Woretaw et al., 2019). InfoSys misuse credited to employees mostly comprise of important organizational InfoSys elements, including software, hardware, data, network, computer devices and services (Li and Siponen 2011).

Statistically, it was estimated that more than 50-70% of the security problems are attributed directly or indirectly to the internal employees' misuse behaviour (Barlow et al. 2013; Siponen and Vance 2010). Behavioural InfoSys security researchers have clearly indicated that employees' behavioural factors are greatly causing a chance of increasing InfoSys security threats such as "computer abuse" (Li and Siponen, 2011; Siponen and Vance, 2010), "violation of security policies" (Barlow et al., 2013; Siponen and Vance, 2010; Hinduja, 2007), personal use of organizational InfoSys networks (Cheng et al., 2014; Colwill, 2009), negligence and careless InfoSys practices (Barlow et al., 2013; Dols and Silvius, 2010; Shaw et al., 2010) and so on. In addition, personal as well as organizational factors are importantly influenced by national culture (Hofstede, 2011), since culture has a potential to change employees' attitude and loyalty (Hofstede, 2011), thereby influencing their InfoSys use and practice behaviours (Montesdioca and Macada, 2015). In addition to that, national culture can influence organizational culture (Hofstede, 2011), thereby influencing InfoSys security culture of individual employee. The sociocultural compositions that existed within organizational employees could also influence the adoption and implementation of InfoSys security policies and strategies (Alnatheer, 2012; Arage et al., 2015).

For example, according to (Alnatheer, 2012) culture specific awareness creation campaign could be an effective means of InfoSys threat reduction. So, investigating culture at national level could provide fundamental and wider insights when to explain behavioural InfoSys security matters (Dols and Silvius, 2010). Additionally, some suggested that criminological theories (including neutralization and deterrence) that are developed and tested in one culture might not work well with another culture (Siponen and Vance, 2010). To that end, the study of culture at national level would provide important directions to develop proactive InfoSys protection measures to minimize employees' related threat incidences (Colwill, 2009; Crossler et al. 2013), in African organizations. However, the study of national culture from the perspectives of African countries with respect to behavioural Infosys security issues, in general, and employees Infosys misuse intention, in particular, has been overlooked (Arage et al., 2015; Crossler et al. 2013).

The following two research questions are developed in order to address some of the mentioned security issues: The first research question is: to what extent do neutralization techniques and rationality-based deterrent constructs influence employees' behaviour towards Infosys misuse in developing economy context? And to what extent people of different culture adopts Infosys security matters differently? The second one is: what are the potential factors that influence employees' behaviour to engage in InfoSys misuse intention?

This study, which is expected to be the first in this context, is therefore, proposed and hypothesized to investigate employees' InfoSys misuse behaviours to understand and explain their intentions on Infosys deviant use and practice behaviours. To that end, some theoretical lenses will be incorporated in the study process such as: national culture dimensions, neutralization techniques, deterrence constructs, theory of planned behaviour, and InfoSys security awareness. Besides, the study focuses more on three important InfoSys misuse behaviours such as: "personal use of organizational networks (e.g. Internet-access), "unauthorized access and data modification", and "personal use of computing devices" using suitable scenarios from extant studies.

2. Literature Review

2.1 Information Systems Security in the Horn of Africa

In today's workplace, InfoSys security problems are becoming ubiquitous worldwide. Countries of the world. Also cooperate one another to mitigate cybersecurity problems. For example, westerns support east African nations to mitigate the cybersecurity problems by giving greater emphasis on the need to combat terrorism and extremism in the region (Gagliardone and Sambuli, 2015). Besides, USA has exerted a lot of efforts in supporting the horn of Africa, especially on the regional readiness to prevent cybersecurity problems, even though, she has paid greater attention to her anti- terrorist strategy, rather than as parts of the coherent and concerted cybersecurity initiatives of the region (Gagliardone and Sambuli, 2015). In addition, international InfoSys security standards, including ISO27002 and ISO27001 are supposed to establish appropriate InfoSys security cultures and obeying those standards were also assumed to secure InfoSys resources across the global organizations, including African's (Woretaw et al. 2019). Even though, international standards and policies are suggested to manage InfoSys security incidences across countries, the problems are still increasing alarmingly worldwide (Yohannes et al. 2019). For instance, countries in the horn of Africa (such as Ethiopia and Kenya) have adopted international cyber security standards, including the European Convention on Cybercrime laws to protect their security problems, but both countries were not able to properly and fully prevent security threat incidences of their cyberspaces (Gagliardone

and Sambuli, 2015). In addition, it is very difficult to find organizations in Africa with effective and standardized InfoSys security policies and legislations that have been designed from the local perspectives (Arage et al. 2015). In such cases, every nation in Africa is encouraged to identify its own priorities when to implement or develop cybersecurity rules and policies to effectively defend own InfoSys security problems (African Union Commission and Council of Europe, 2018).

As an ample evidence, a case study conducted in the horn of Africa clearly revealed that three very close countries such as: Kenya, Ethiopia and Somalia have presented distinctive responses on cybersecurity problems and showing differing views on their digital cultures (Gagliardone and Sambuli, 2015). Consequently, the results of the study on such adjacent or neighboring countries produced higher differences on their security threat vulnerabilities from the perspectives of technical, social and political contexts (Gagliardone and Sambuli, 2015).

Some scholars have also clearly pointed out that countries in Africa often implemented InfoSys security policies, guidelines and other countermeasures that were mostly designed and adapted based on western cultures (Alnatheer, 2012, Arage et al. 2015). In addition, some also indicated that international policies and standards that were designed from the perspectives of western countries might not fit with African InfoSys security contexts (Arage et al. 2015; Bogale et al. 2019) mainly due to the socio- cultural diversities. Specific to Ethiopia (Yohannes et al. 2019) discovered that there is only limited studies on InfoSys security problems. According to (Arage et al. 2015), extant InfoSys security studies in Ethiopia were motivated to provide only technical solutions, even if the security losses of the country were mostly happened due to the human behavioural matters than technical faulty (Woretaw et al. 2019; Arage et al. 2015). For example, as of (Yilma, 2016), Ethiopian government was trying a lot to limit the distribution of politically affiliated problematic contents via the internet, but she was not capable of controlling security problems due to the lack of fully-fledged and context specific laws and policies. However, to show financial and non-financial losses of InfoSys security breaches in the country, there is a problem of getting the actual figures and resultant monetary losses due to the lack of empirical data on breach incidences (Arage et al. 2015).

Ethiopian government often blocked the access to internet, especially the use of social media networks aiming to limit politically affiliated contents of national cybersecurity threats (Yilma, 2016). In solving such important problems, the country was shutting down internet access privileges across the nation, but such access denials were also resulted in the loss of 9 million USD in 2016 alone (Yilma, 2016). In addition, the country's Revenue and Custom Authority experienced InfoSys security breach incidences by own employees and resulted in an estimated financial loss of ETB 13 million in the same year (Arage et al. 2016).

Ethiopian airline has also fired around 11 employees due to InfoSys security policy violations related malpractice behaviours (Arage et al. 2016). Even though, there are high InfoSys security problems in Africa as a whole, and in Ethiopia in particular, reports on treat incidences as well as InfoSys security studies are very rare, especially from the human behaviour perspectives Arage et al. 2015). In general, some extant scholarly evidences revealed that InfoSys security issues are at their infancy stage in Ethiopia in general and its banking sectors in particular (Woretaw et al. 2019). As a result, banks in Ethiopia are unable to create positive security cultures due to the lack of accurate evidences to create pertinent awareness and deliver effective training activities (Yohannes et al. 2019). As indicated in Bogale et al. 2019), contextual as well as socio-cultural InfoSys security policies and standards should be developed and implemented in order to enhance employees' level of InfoSys security understanding and awareness across organizations.

In brief, employees of Ethiopian banking sectors failed to manage InfoSys security problems as well as unable to fully understand essential InfoSys security matters due to lack of proper awareness on various security concerns, including password management, virus related security issues, threat susceptibility, proper internet usage, backup skills, handling security incidences, encrypting corporate data transfer, proper sharing of files and computing devises to their coworkers, and so on Bogale et al. 2019). Recently, there is very fast internet penetration in Africa (African Union Commission and Council of Europe, 2018), so an integration of network resources in the workplace and defending them needs much work to fully protect them (Yohannes et al. 2019). However, employees not only lack high level InfoSys security awareness and understanding but banking employees in Ethiopia even lack fundamental knowledge to use ATM and E-payment systems (Yohannes et al. 2019). So, in general context specific behavioural studies might provide proper solutions for InfoSys security problems to Africans.

3. Theoretical Foundation

3.1 National culture

National culture is defined as a collective programming of the mind that differentiates one group of society from the other group or it is a collective thought or understanding towards socially constructed realities that can distinguish a member of one social group from the other (Hofstede, 1980). Culture is able to limit the nature and scope of individuals' actions and interactions, because it can directly affect the pattern of cognitive map or mental impetus of human society and guide the decision on their actions (Kaba and Osei- Bryson, 2013). Because national culture can influence individuals' attitude more than organizational culture (Plachkinova and Andrés, 2015), in that regard national culture is suggested to provide better understanding and proper insights of employees' Infosys security deviant behaviours (Siponen and Vance, 2010; Crossler et al. 2013; Plachkinova and Andrés, 2015). We present the four widely used Hofstede's cultural dimensions in the following sections, along with the hypotheses associated with each dimension.

3.1.1 By-laws and Policies

Individualism/ collectivism: Individualistic societies are less integrated, weakly tied and fragmented groups of people compared to collectivist society (Hofstede, 2011), where societal cohesiveness is very high. Collectivist societies are expected to protect their members in an exchange of unquestioning loyalty (Plachkinova and Andrés, 2015) and share even private properties to their group members. According to (Kaba and Osei-Bryson, 2013), strong social ties are very important, especially in Africa where people are more collectivist in nature. In most collectivist society, individual's opinions are the opinions of the group, because it is the group that provides structures, obligations, views, and safety to individuals (Kaba and Osei-Bryson, 2013). So, collectivists are not expected to respect InfoSys security policies and procedures if individuals from their social groups need them to share resources like organizational InfoSys tools and applications (Alshare and Lane, 2008). In that respect, for instance Ethiopia is a collectivist society but USA is individualist. So, it will be postulated as:

H1: Collectivism is more likely associated with employees' attitude towards InfoSys misuse behaviour, and the effect is higher in Ethiopia than in USA.

3.1.2 Power Distance (PD)

It is the extent to which large power inequalities are accepted as normal by the individual, therefore PD will condition the degree to which an employee believes that his/her superiors or higher-ups have more power (Srite and Karahanna, 2006, p. 682). In this respect, employees in high PD society are expected to respect organizational rules and regulations (Dols and Silvius, 2010; Crossler et al. 2013) may be fear of penalties from their superiors. However, unlike high PD societies whom they are expected to accept and practice new Infosys policies and procedures as directed (Dols and Silvius, 2010), the low PD societies may violate policies when they need (Crossler et al., 2013). According to (Hofstede, 1980), the people in many African countries have a high degree of hierarchical distance or power inequalities within their communities, so their perceptions of the superiors' power can greatly affect their decisions made in InfoSys misuse attitudes (Kaba and Osei-Bryson, 2013). With this in mind, using Hofstede's cultural scores, Ethiopians are generally, in comparison, higher than Americans in terms of PD values. Therefore, it will be hypothesized that:

H2: High PD is less likely to be associated with employees' attitude towards InfoSys misuse behaviour, and the effect is lesser in Ethiopia than in USA.

3.1.3 Feminine /masculine

It is the degree to which individuals espouse or embrace gender inequalities. People who are espoused to masculine culture emphasize work goals such as achievement, earnings, advancement, performance, competitiveness, and assertiveness, but people who are espoused to feminine culture emphasize more on personal goals such as a friendly atmosphere, relaxed work atmosphere, warm personal relationships, and quality of life (Srite and Karahanna, 2006, p. 682; Hofstede, 2011). In feminine culture, social relationships are more important. So, personal use of organizational internet access to chat with friends and families via social media networking may be tolerated (Dols and Silvius, 2010). In addition,

using organizational networks to watch movies may be permitted due to the need to maintain a relaxed work- life during working time, and company works may be done with families at home too (Dols and Silvius, 2010). So, in

the context of InfoSys security issues, InfoSys misuse may be more common in feminine culture than in masculine equivalents, because employees are prone to personal use of organizational internet access. On the contrary, societies with masculine culture is greatly concerned with attaining personal goals and productivity (Kaba and Osei-Bryson, 2013). So, people in masculine types of culture may not engage in InfoSys misuse practices to create smooth relationships with others. Using Hofstede's cultural score, Ethiopians are more feminine than the USA equivalents. So, it can be hypothesized as

H3: Femininity is positively associated with employees' attitude towards InfoSys misuse, the relationship is higher in Ethiopia than USA.

3.1.4 Uncertainty Avoidance (UA)

It is the level of risk or unsure situation that is accepted to the individual, which can be credited by his/her emphasis on rule obedience, labour mobility, and ritual behaviour (Srite and Karahanna, 2006, p. 682). In short, this dimension examines the degree to which one feels threatened or unsecured by an ambiguous situation. Moreover, people in high UA culture need strict policies, guidelines, and rules to do their jobs very well (Crossler et al. 2013), it is because an employee from high UA culture is assumed to choose the right way of following policies and rules. On the other hand, an employee in low UA culture may ignore or neglect organizational rules and policies if he/she thinks that "it doesn't make sense" to him/her (Dols and Silvius, 2010). The people in low UA culture may not comply with organizational InfoSys security policies and procedures if they think that these policies and procedures are not necessary; however, people who are in the high UA culture respect policies and laws to avoid uncertain future risks or unintended consequences, because, people with high UA value have a strong sense of uncertainty or ambiguity aversion traditions (Kaba and Osei-Bryson, 2013). In addition, such people may also be weaker to report misuse behaviours of coworkers (Dols and Silvius, 2010). So, having strong policies and procedures are not a guarantee to secure InfoSys resources in a low UA culture than in a high UA culture (Crossler et al. 2013). Using Hofstede's cultural scores, in comparison, Ethiopia is higher in UA score than the USA equivalents. So, it can be postulated as:

H4: low UA is positively associated with employees' attitude towards InfoSys misuse the relationship is stronger in USA than Ethiopia.

3.2 Information System Security Awareness

InfoSys security awareness is proposed in improving employees' non-misuse practices as well as proper handling of InfoSys resources (Alshare and Lane, 2008), and can also produce strong organizational InfoSys security cultures, thereby reducing threat vulnerabilities (Maçada and Luciano, 2010). In addition, InfoSys security prevention awareness specific training, which is supposed to enhance employees' conscious and ethical use of InfoSys resources by making right decisions (Alshare and Lane, 2008) and can be a means of discouraging InfoSys misuse behaviours by informing them about the impacts of deviant practices (Tu and Yuan, 2014), thereby creating a positive attitude to dissuade themselves from misuse related behaviours (Barlow et al. 2013; Maçada and Luciano, 2010). So, employees' InfoSys security awareness will generate a better attitudinal behaviour to effectively defend such resources (Tu and Yuan, 2014). On the contrary, a lack of InfoSys security awareness may result in unintentionally releasing highly confidential information foolishly (Shaw et al., 2010). Moreover, security awareness is used to improve employees' policy compliance intentions positively (Haeussinger and Kranz, 2013) and reduce the intentions to misuse InfoSys resources. So, it is hypothesized as:

H5a: The better employees' InfoSys security awareness, the lower will be their attitude towards InfoSys misuse.
H5b: The better employees' InfoSys security awareness, the lower will be their intention towards InfoSys misuse.

3.2.1 Attitude towards Infosys Misuse Intention

Attitude, either positive or negative, will be changed into some forms of intentional behaviours and influences InfoSys security control measures of individuals (Tu and Yuan, 2014). Theory of Planned Bahaviour (TPB) states that intentional behaviour is importantly influenced by attitude to that behaviour (Ajzen, 1991), as a result, the actual or planned behaviours can be predicted via intention (Ajzen, 1991). For that, different studies have proved attitude as having a strong association with individuals' intention to comply with security policies (Bulgurcu et al., 2010; Ifinedo, 2012). This study, therefore, adopts the definition of employees' attitude as defined in (Ifinedo, 2012) as: "individual employees' positive or negative feelings towards engaging in a specified behaviour",
including InfoSys misuse attitude. Thus, it is hypothesized as:

H6: The higher employees' attitude towards InfoSys misuse, the more their intention to misuse InfoSys resources will be.

3.2.2 Deterrence Theory on Infosys Misuse Intention

Initially, general deterrence theory (GDT) in InfoSys security studies was proposed to explain how to prevent people from engaging in security deviant behaviour (Cheng et al. 2013). In this respect, multiple studies have revealed that deterrence theory by means of sanctions is widely investigated in order to devise techniques that are intended to deter or prevent individuals from engaging in InfoSys security deviant behaviours (Siponen and Vance, 2010; Cheng et al. 2014; Cheng et al. 2013; D'Arcy et al. 2009). Here, the certainty and severity of sanctions were both found to be a means of reducing employees' behavioural intention to engage in deviant behaviour (D'Arcy et al. 2009), including InfoSys misuse. To that end, this study uses three rationality-based deterrent constructs such as perceived detection certainty, perceived sanction severity, and perceived benefit that are important in InfoSys security studies (Cheng et al., 2014). More specifically, the higher the probability of detection certainty and the greater the severity of the sanction, the better employees are deterred from InfoSys misuse behaviour (Cheng et al., 2014; Cheng et al., 2013). For example, the perceived severity of sanction has a positive and strong association with InfoSys misuse intention (D'Arcy et al. 2009). Perceived benefits are all the assumed earnings that employees expect to have from personal use of InfoSys resources (Cheng et al. 2014). So, sanctions, as well as benefits of misusing organizational InfoSys resources, can influence individuals either to intentionally engage in or deter themselves from personally use InfoSys resources. As a result, it can be postulated as:

H7: The more certain the perceived detection of employees' InfoSys misuse, the lower the probability of their InfoSys misuse intention will be;
H8: The more severe the perceived sanction towards employees' organizational InfoSys misuse, the lower the probability of their InfoSys misuse intention will be;
H9: The higher the perceived benefits of using organizational InfoSys resources for personal reasons, the higher the probability of InfoSys misuse intention will be.
twenty countries producing 90% of the honey. Other by-products such as beeswax, propolis, pollen, royal jelly, broods, and venom are also produced and exported for economic gain (Aiyeloja, Popoola and Ogunjinmi, 2010).

3.2.3 Neutralization Theory on Infosys Misuse Intention

Neutralization techniques help employees to rationalize their misuse behaviours to reduce the perceived negative outcomes of own deviant behaviours (Colwill, 2009) in charge. Moreover, those techniques aid employees to free them from the feeling of shame and guilt by creating a "positive self-image" for their aberrant actions (Siponen and Vance, 2010). In the case of neutralization, individuals also use a priori rationalization techniques to convince themselves, and others, that their malpractices are easily justifiable and/or excusable (Colwill, 2009; Siponen and Vance, 2010; Hinduja, 2007; Cheng et al. 2014). So, InfoSys security policies and procedures are essential to be developed and implemented by considering employees' neutralization attitude and tendency (Siponen and Vance, 2010). Hence, neutralization techniques are recently getting greater attention and are widely used to understand InfoSys security negative behaviours of employees, and they are also highly associated with their intention to InfoSys security deviant behaviours. (Figure 1).

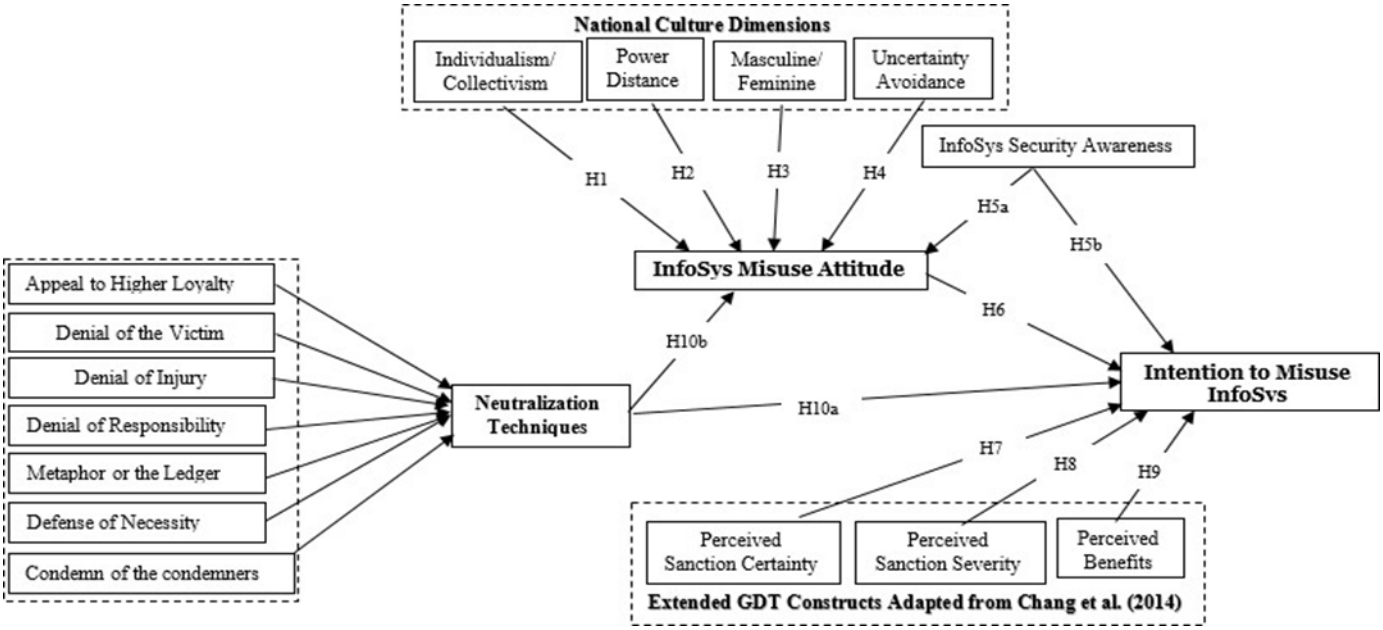

Figure 1. Proposed Research Model

4. Methods

The aim of the study is to address the research questions. Accordingly, the study methodology should align with answering the stated research questions by empirically testing the proposed research model. To that end, the study will follow the positivist research paradigm as a philosophy perspective because the research is designed in a manner to empirically test hypotheses as well as a theoretical research model designed as a result of gap assessment and literature survey. To that end, a cross- sectional quantitative survey will be utilized for data(Barlow et al. 2013; Siponen and Vance, 2010; Hinduja, 2007; Cheng et al. 2014).

Therefore, this study seeks to conceptualize the six neutralization techniques as suggested by (Siponen and Vance, 2010) such as denial of responsibility, denial of injury, appeal to higher loyalties, condemn the condemners, the metaphor of the ledger, the defence of necessity, and an additional technique called denial of the victim from (Cheng et al. 2014) will be included in order to investigate employees' InfoSys misuse intention with an assumption of the neutralization techniques as a second-order formative construct. So, it is hypothesized as:

H10a: Use of neutralization techniques positively affect Employees' intension to misuse organizational InfoSys resources;
H10b: Availability of diverse neutralization techniques positively shape employees' attitude to misuse organizational InfoSys resources;

Culture-based studies, moreover, are suggested to be conducted using a quantitative survey (Hofstede, 2011). The study is aimed at explaining the dependent variable (i.e. intention to misuse InfoSys) of interest using data of respondents from organizational employees. The pilot respondents will be selected randomly from the university lecturers who use computers as a working instrument in Ethiopia. However, the target population for the final survey will be all professional employees who are working in various organizations and have access to InfoSys resources in their day-to-day routines.

The sample population, therefore, incorporate randomly selected 1000 employees (i.e. 500 from the USA and 500 from Ethiopia) who are working in medium and large-scale organizations. Paper-edition types of data collection will be used for Ethiopian respondents, but the data from the USA will be collected through software tools (e.g. Qualtrics). Questionnaire instruments that will be adapted from extant studies will be operationalized for pretesting and pilot testing issues. To see how constructs and indicators work; pilot testing will be performed using 100 organizational employees.

A scenario-based approach will be employed for data collection activities, since scenario methods are widely applied and highly recommended in studying criminal, unethical and anti- social behaviours (Barlow et al. 2013; Siponen and Vance, 2010; D'Arcy et al. 2009), like this current one. The research model, as well as its constructs, will be validated and empirically tested using SEM-PLS analysis techniques. Finally, data analysis activities will be performed using Smart-PLS as well as SPSS with Amos software tools.

5. Expected Implications of the Study

5.1. Theoretical contributions

The study mainly focuses on comparing employees' use of organizational InfoSys resources and their attitude and intention to misuse those resources in the context of Africa (e.g. Ethiopia) and the westerns (e.g. USA). So, the study will shed light on how national culture, security awareness, and criminological theories are integrated to understand and determine InfoSys misuse intentions using a comparative analysis of data from two culturally different contexts. Since an actual behaviour is difficult to measure directly, especially using criminological theories in the case of deviant behaviour studies (Siponen and Vance, 2010), this study will try to operationalize intention to explain the actual human behaviours aptly. Finally, this study will illustrate how InfoSys misuse behaviours of employees vary across cultures.

5.2. Practical Implications

This study will also help to understand employees' InfoSys misuse behaviour in order to support the development and implementation of culturally as well as contextually appropriate behavioural InfoSys security protection measures. The study will also give an implication to managers and policymakers to understand how employees rationalize misuse behaviour, thereby, developing appropriate countermeasures to inhibit them from engaging in deviant behaviours. It also helps to understand employees' level of InfoSys security awareness, thereby conducting effective awareness campaigns anddeliver appropriate and secure use of InfoSys training.

The findings of this study will be applicable to countries having similar cultures to Ethiopia. Implications for employees are also to make them aware of the different InfoSys threat incidences and the impacts associated with deterrent countermeasures. It also helps companies of foreign origin while investing in Africa (e.g. Ethiopia) to develop and implement appropriate prevention measures to their InfoSys resources, thereby leading safe organizations. So, foreign investors can make cognizant decision-making activities when producing InfoSys policies in Ethiopia.

6. Conclusion

Even though this ongoing research includes an important comprehensive conceptual research model that can and should be tested to explain how the hypothesized relationships show employee IS misuse behaviour, there are no solid results to practically observe how effective the perceived relationships are. In addition, the output of this particular study may not be valid and applicable to countries with different socio- cultural settings as the planned respondents' context (i.e. Ethiopian and USA organizational employees). However, it provides an overall insights and understandings of the direct effects of cultural values on criminological theories, including neutralization theory and rational choice based deterrent constructs along with IS security countermeasure awareness to predict IS misuse intentions of employees. In this regard, this proposed study will be the first to examine employees' misuse of IS resources in an overlooked and neglected contexts of cultural disparities using a western traditions and the developing economy contexts.

References

Abdelkader, A., Elshorbagy, A., Tuninetti, M., Laio, F., Ridolfi, L., Fahmy, H., and Hoekstra, A.Y., National Water, Food, and Trade Modeling Framework: The Case of Egypt, *Science of the Total Environment*, vol. 639, pp. 485–496, 2018.

Alkaisi, A., Mossad, R. and Sharifian-Barforoush, A., A Review of the Water Desalination Systems Integrated with Renewable Energy, *Energy Procedia*, vol. 110, no. December 2016, pp. 268–274, 2017.

African Union Commission and Council of Europe. Cyber Security and Cybercrime Policies for African Diplomats. Concept Document, 12-13, April-2018, Addis Ababa, Ethiopia, 2018.

Ajzen, I. The Theory of Planned Behavior, Organizational Behavior and Human Decision Processes, 50, 179-211, 1990.

Alnatheer, M. A. Understanding and Measuring Information Security Culture in Developing Countries: Case of

Saudi Arabia. PhD Thesis 2012, Queensland University of Technology, Australia.

Alshare, K. A., and Lane, P. L. A Conceptual Model for Explaining Violations of the Information Security Policy (ISP): A Cross Cultural Perspective. Proceedings Americas Conference on Information Systems (AMCIS), 1-1-2008.

Alahmad, M., Prediction of Performance of Sea Water Reverse Osmosis Units, *Desalination*, vol. 261, no. 1–2, pp. 131–137, 2010.

Compliance with Information Systems Security (ISS) Policies: Towards ISS Culture in Ethiopian Companies. Twenty-first Americas Conference on Information Systems, Puerto Rico.

Arage, T. M., Belnger, F., and Tesema, T. B, Investigating the Moderating Impact of National Culture in Information Systems Security Policy Violation: The Case of Italy and Ethiopia. MCIS 2016 Proceedings, Paper 56, Paphos, Cyprus, http://aisel.aisnet.org/mcis2016/56.

Barlow J. B., Warkentin, M., Ormond, D., and Dennis,

A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. Computers and Security, 39, B, 145–159.

Baawain, M., Choudri, B.S., Ahmed, M., and Purnama, A., *Recent Progress in Desalination, Environmental and Marine Outfall Systems*, Springer International Publishing, 2015.

Bashitialshaaer, R., Solar-Energy Innovative and Sustainable Solution for Freshwater and Food Production for Lake Titicaca Islands, *European Journal of Engineering Research and Science*, vol. 5, no. 4, pp. 436–442, 2020.

Baawain, M., Choudri, B.S., Ahmed, M., and Purnama, A., *Recent Progress in Desalination, Environmental and Marine Outfall Systems*, Springer International Publishing, 2015.

Bashitialshaaer, R., Solar-Energy Innovative and Sustainable Solution for Freshwater and Food Production for Lake Titicaca Islands, *European Journal of Engineering Research and Science*, vol. 5, no. 4, pp. 436–442, 2020.

Bogale, M., Lessa, L., and Negash, S. , Building an Information Security Awareness Program for a Bank: Case from Ethiopia. Twenty-fifth Americas Conference on Information Systems (ACIS), Cancun, 2019.

Cheng, L., Li, W., Zhai, Q., and Smyth, R, Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. Computers in Human Behavior, vol. 38, pp. 220–228, 2014.

Colwill, C. Human factors in information security: The insider threat Who can you trust these days?". Information Security Technical Report, vol. 14, pp.186-196, 2009.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hud, Q., Warkentin, M., and Baskerville, RFuture directions for behavioral and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. European information security Research. Computers and Security, vol. 32, pp. 90-101, 2013.

D'Arcy, J., and Herath, T. A review Journal of Information Systems, vol. 20, pp. 643–658. 2011.

D'Arcy, J., Hovav, A., and Galleta, D. F., User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research, vol. 20, no. 1, pp. 79-98. 2009

Dols, T., and Silvius, G. Exploring the Influence of National Cultures on Non- Compliance Behaviour", Communications of the IIMA, Vol. 10, No. 3, Art. 2. 2010,

Eke, J., Yusuf, A., Giwa, A. and Sodiq, A., The Global Status of Desalination: An Assessment of Current Desalination Technologies, Plants and Capacity, *Desalination*, vol. 495, no. 9, pp. 114633, 2020.

El-Nashar, W.Y., and Elyamany, A.H., Managing Risks of the Grand Ethiopian Renaissance Dam on Egypt, *Ain Shams Engineering Journal*, vol. 9, no. 4, pp. 2383–2388, 2018.

Eke, J., Yusuf, A., Giwa, A. and Sodiq, A., The Global Status of Desalination: An Assessment of Current Desalination Technologies, Plants and Capacity, *Desalination*, vol. 495, pp. 114633, 2020.

El-Nashar, W.Y., and Elyamany, A.H., Managing Risks of the Grand Ethiopian Renaissance Dam on Egypt, *Ain Shams Engineering Journal*, vol. 9, no. 4, pp. 2383–2388, 2018.

Goh, P. S., Lau, W. J., Othman, M. H.D. and Ismail, A. F., Membrane Fouling in Desalination and Its Mitigation Strategies, *Desalination*, vol. 425, no. October 2017, pp. 130–155, 2018.

Gagliardone, I., and Sambuli, N., Cyber Security and Cyber Resilience in East Africa. Published by the Centre for International Governance Innovation and Chatham House, Global Commission on Internet Governance, Paper Series: No. 15 , 2015.

Goh, P. S., Lau, W. J., Othman, M. H.D. and Ismail, A. F., Membrane Fouling in Desalination and Its Mitigation Strategies, *Desalination*, vol. 425, no. October 2017, pp. 130–155, 2018.

Haile, G.G., Tang, Q., Li, W., Liu, X. and Zhang, X., Drought: Progress in Broadening Its Understanding, *WIREs Water*, vol. 7, no. 2, pp. 1–25, 2020.

Hesamian, G. and Akbari, M.G., A Robust Multiple Regression Model Based on Fuzzy Random Variables, *Journal*

of Computational and Applied Mathematics, vol. 388, pp. 113270, 2021.

Huber, P.J., *Robust Statistics*, John Wiley and Sons, 1981.

Haile, G.G., Tang, Q., Li, W., Liu, X. and Zhang, X., Drought: Progress in Broadening Its Understanding, *WIREs Water*, vol. 7, no. 2, pp. 1–25, 2020.

Hesamian, G. and Akbari, M.G., A Robust Multiple Regression Model Based on Fuzzy Random Variables, *Journal of Computational and Applied Mathematics*, vol. 388, pp. 113270, 2021.

Haeussinger, F. J., and Kranz J. J. (2013). Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior. Thirty Fourth International Conference on Information Systems, Milan 2013.

Hinduja, S. (2007). Neutralization theory and online software piracy: An empirical analysis. Ethics and Information Technology, 9, 187–204, Springer 2007, DOI 10.1007/s10676-007- 9143-5.

Hofstede, G,Culture's Consequences: International Differences in Work-Related Values. Beverly Hills, CA: SAGE Publications.,1980.

Hofstede, G. Dimensionalizing Cultures: The Hofstede Model in Context, Online Readings in Psychology and Culture. Universities of Maastricht and Tilburg, Netherland. 2011

Ifinedo, P., Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. Computers and Security, 31, 83-95, 2012.

Jang, Y., Kim, H. S., Lee, J. H., Ham, S. Y., Park, J. H. and Park, H. D., Development of a New Method to Evaluate Critical Flux and System Reliability Based on Particle Properties in a Membrane Bioreactor, *Chemosphere*, vol. 280, no. April, pp. 130763, 2021.

Jeong, K., Park, M. and Chong, T. H., Numerical Model-Based Analysis of Energy-Efficient Reverse Osmosis (EERO) Process: Performance Simulation and Optimization, *Desalination*, vol. 453, no. November 2018, pp. 10–21, 2019.

Jerry L. Hintze, *User's Guide III. Regression and Curve Fitting,* NCSS Statistical System, 2007.

Joseph, A. and Damodaran, V., Dynamic Simulation of the Reverse Osmosis Process for Seawater Using LabVIEW and an Analysis of the Process Performance, *Computers and Chemical Engineering*, vol. 121, pp. 294–305, 2019.

Joseph, A. and Damodaran, V., Event-Driven Enabled Regression Aided Multi-Loop Control for SEC Minimisation in SWRO Desalination Considering Salinity Variation, *ISA Transactions*, vol. 119, pp. 221–241, 2021.

Kaba B., and Osei-Bryson, K., Examining influence of national culture on individuals' attitude and use of information and communication technology: Assessment of moderating effect of culture through cross countries study. International Journal of Information Management, vol. 33, pp. 441–452. 2013

Kim, Y. M., Kim, S. J., Kim, Y. S., Lee, S., Kim, I.S. and Kim, H.J., Overview of Systems Engineering Approaches for a Large-Scale Seawater Desalination Plant with a Reverse Osmosis Network, *Desalination*, vol. 238, no. 1–3, pp. 312–332, 2009.

Kolluri, S.S, Esfahani, I.J, Garikiparthy, P.S.N. and Yoo, C.K., Evaluation of Multivariate Statistical Analyses for Monitoring and Prediction of Processes in an Seawater Reverse Osmosis Desalination Plant, *Korean Journal of Chemical Engineering*, vol. 32, no. 8, pp. 1486–1497, 2015.

Li, Y., and Siponen, M. , A Call for Research on Home Users' Information Security Behavior. Pacific Asia Conference on Information Systems (PACIS) 9 July 2011, PACIS Proceedings, Association for Information Systems. 2011

Maalouf, S., Rosso, D. and Yeh, W.W.G., Optimal Planning and Design of Seawater RO Brine Outfalls under Environmental Uncertainty, *Desalination*, vol. 333, no. 1, pp. 134–145, 2014.

Maronna, R.A., Martin, R.D., Yohai, V.J., and Salibian-Barrera, M., *Robust Statistics: Theory and Methods*, 2nd edition John Wiley and Sons, 2006.

Qasim, M., Badrelzaman, M., Darwish, N.N., and Darwish, N.A., Reverse Osmosis Desalination: A State-of-the-Art Review, *Desalination*, vol. 459, no. February, pp. 59–104, 2019.