11-14-2021

Examining the Effects of Cultural Dimensions on Deviant IS Use Behaviour in a Developing Economy Context

Yimer Mohammed

Merrill Warkentin

Tibebe Besha

Examining the Effects of Cultural Dimensions on Deviant IS Use Behaviour in a Developing Economy Context

Emerging Research Paper

Yimer Mohammed
Addis Ababa University
Yimoh_fast@yahoo.com

Merrill Warkentin
Mississippi State University
m.warkentin@msstate.edu

Tibebe Beshah
Addis Ababa University
Tibebe.Beshah@gmail.com

Abstract

Information System (IS) tools and applications create opportunities for a positive digital change to all individuals and organizations in the global workplace to improve competitiveness and quality of work life. Recent studies have shown that the most problematic areas in IS security incidences are people-related factors. In this regard, employees are causing IS security risks and vulnerabilities as they use those resources, especially by exercising their legitimate and lawful rights, mainly because people are the weakest link on IS security matters. On the one hand, the effects of organizational sanctions are not always effective due to socio-cultural variabilities, and so far they have not been able to fully defend employee related IS misuse or misconduct. On the other hand, the use of neutralization techniques supports individuals to justify their deviant actions, but differently to people in different socio-cultural bases. To examine such a problem, therefore, culture as a moderator, criminological constructs and level of employees' awareness to IS security as independent variables are employed to explain IS misuse intention in unison are proposed through a comprehensive conceptual research model. A positivist research paradigm using a cross-sectional quantitative survey data collection approach will be adapted to help empirically test the model. To validate the model and its constructs, the study will apply SEM-PLS data analysis techniques using Smart-PLS and SPSS with Amos. Finally, this study in progress discusses the potential practical and theoretical contributions and plans to provide scientific evidence based on its findings.

Keywords: IS misuse, National culture, Awareness, Neutralization Techniques, Deterrent theory

Introduction

Information System (IS) tools and applications create opportunities for a positive digital change to all individuals and organizations in the global workplace. These technologies are being used for a variety of objectives within the national, regional, and cultural boundaries and have been becoming increasingly ubiquitous worldwide (Shore & Venkatachalam, 1996: pp.19). Because such technologies are primarily used to increase productivity and quality of work life. Despite the importance of these technologies, which provide widespread economic and social welfare, such benefits can also be easily compromised by human-related factors (e.g. personal use or misuse or malpractice behaviors) (Charki et al., 2017). The proliferation of IS resources across the global workplace also poses new and emerging security threats (Charki et al., 2017), so that the failure to protect IS resources can greatly hurt everyone in many ways (Siponen & Vance, 2010). The above issues are most common when IS resources are used unwisely or negatively and affect individuals or organizations by triggering the financial and non-financial losses (Vaidyanathan & Berhanu, 2012). Due to the rapid growth of the digital economy around the world, data breaches are expected to increase in frequency, severity, and cost over time (Ponemon Institute, 2020). In particular, the frequency and cost of internal security threats are becoming more alarming (Ponemon institute, 2020), and the numbers and types of incidences are also gradually growing (D'Arcy & Herath, 2011). For example, the cost of insider threats was $8.76 million by 2018, whereas after a couple of years in 2020 the costs reached $11.45 million, which shows a 31% raise

(Ponemon institute, 2020) in magnitude worldwide. Even though there is a growing investment to strengthen IS security capabilities of businesses and countries, there are still huge data breach incidences (Crossler et al., 2013) here and there. Even if there are plenty of cybersecurity studies that have focused primarily on technical and physical security measures, research on human behaviours is unsatisfactory (Crossler et al., 2013). Additionally, studies have made it clear that technical solutions alone is powerless to bring the required level of IS protection to fully defend IS resources all over the world, including the Ethiopians (Yohannes et al., 2019; Arage et al., 2016). In so doing, to fully address IS security problems improving investment in all aspects of security countermeasures (i.e. the technical, physical and behavioural matters) should be well-thought-out (Bulgurcu et al., 2010), because investing in technical and physical security measures alone didn't bring an overall IS security solution. For example, according to Shropshire et al. (2015) the biggest threat to IS security incidences is not just the security environment (hackers, malware, etc.), but the careless or malicious practices of internal users, such as employees and trusted others. Recently, Insider Threat Intelligence Report also showed that humans are the most common cause of security incidents and accounts for about 90% of all IS security problems worldwide (2017). Others also clearly showed that 50-70% of security threats are directly or indirectly caused by human beings, mainly by employees who are legitimate and trusted workers (Siponen & Vance 2010), it is importantly because human beings are the weakest link in IS security lax behaviours (Bulgurcu et al., 2010; Siponen & Vance 2010). That is why IS security scholars have recently focused their attention more on human related IS security aspects, and employee-related IS misuse deserves considerable attention (e.g. Willison & Warkentin, 2013; Crossler et al., 2013).

Examining human-related factors, therefore, would become more imperative (e.g. Bulgurcu et al., 2010); however, those efforts were scant to offer solid theoretical and practical foundations, particularly in Africa (Crossler et al., 2019). Some also supplemented that there are a dearth of empirical facts that help to understand the contextual and behavioural factors that affect employees' IS deviant behaviors (Willison & Warkentin, 2013), specially from the developing economy contexts (Crossler et al., 2013). Even though international standards and policies are suggested to prevent IS security threat incidences to all national boundaries, the problems are still alarmingly growing worldwide (Yohannes et al., 2019). For example, it is very difficult to find companies in Africa with effective and standardized security policies and laws designed from the perspectives of their own contexts (Arage et al., 2016). Moreover, truly effective IS security responses require more than just importing and implementing good practices and expertise that were designed elsewhere (Allen, 2021). In that regard, countries in the Horn of Africa (e.g. Ethiopia and Kenya) have adopted similar international cybersecurity standards, including the European Convention to Cybercrime, to protect their cyberspaces, however, both countries have not been able to fully protect themselves from cyberattacks (Gagliardon & Sambuli, 2015). Another piece of ample evidence in the same region revealed via a case study showed that three of the most bordering countries, such as Ethiopia, Kenya, and Somalia have responded cybersecurity challenges differently and expressed differing views on their digital cultures (Gagliardone & Sambuli, 2015). Having that in mind, regional and cultural factors should be taken into account while studying the significant influence of human behaviours in IS studies, including the IS security issues (e.g., Gupta et al., 2015, Vance et al., 2020), assuming that regional and cultural diversities are becoming the strongest ecological factors that can affect human behaviours more noticeably (Hofstede, 1984). Culture at national level is viewed as a set of stereotypical behaviours, promoting stereotypical personal attributions (Warkentin et al., 2015), so the direct application of national cultural values proposed by Hofstede to investigate IS-related behaviours has become tricky. It is because, Hofstede's national cultural metrics are derived from the average attitudinal tendencies of IBM staffs of the sampled countries, so it should be noted that significant disparities in these averages may exist within the population subcultural variations in a nation (McSweeney, 2002). Therefore, adopting cultural values in the above context may lead to misconceptions on the fact that all individuals in a country have the same IT use and practice behaviours is not always true (Warkentin et al., 2015). In addition, there are significant cultural differences among a particular population on individual parameters (Gupta et al., 2015; Vance et al., 2020), whereas individuals of different countries may also have similar cultural and personal characteristics (Warkentin et al., 2015). Having that in mind, the national-level culture assessment may overshadow the behavioural variability of individuals in a certain nation. In that regard, many argued that evaluating culture at an individual level or studying the cultural values that are espoused to individuals are becoming the focus of several scholars in IS disciplines today (Srite & Karahanna, 2006; Crossler et al., 2019; Chu et al., 2019).

So, the direct application of national cultural scores proposed by Hofstede is not fruitful, because the assumption that all people in a given nation have the same or similar cultural scores led to erroneous conclusions due to ecological fallacy (Srite & Karahanna, 2006; Chu et al., 2019). To that end, individual level espoused cultural dimensions measure are becoming an important research agenda of IS scholars. Espoused cultural dimensions are defined as the extent to which an individual accepted or embraced the values of the national culture (Srite & Karahanna 2006). For example, a country with multiple ethnic and linguistic bases (e.g. India) has a wide range of internal or in-group

variations amid its citizens on a variety of individual characteristics (Gupta et al., 2015). So, the above factors may work in a very similar context to other countries (Gupta et al., 2015), (e.g. Ethiopia) where multiple linguistic and subcultural societies live together (i.e. there are 86 different languages and dialects with diverse ethnic and linguistic bases). It is also greatly suggested that when a nation develops or implements standards and policies, it should first identify its national priorities and local contexts. However, there is still a lack of attention and evidence to address IS security challenges of Ethiopia, mainly from the socio-cultural and behavioral perspectives (Arage et al., 2016). For this reason, in light of the diverse subcultural groups in Ethiopia, this particular study pools important criminological constructs drawn from neutralization theory, extended deterrent theory, IS security awareness, and national culture dimensions as a moderator, which, to the best of our knowledge, have not yet been in unison applied to the contexts of IS security studies, including within the developing economy contexts. In so doing, this study will shed light on regional cybersecurity issues using a comprehensive theoretical research framework that will be empirically tested later on. So, this study seeks to address the questions: what is the impact of some criminological theories constructs to explain IS misuse intention? And to what extent does national culture moderate the relationship between neutralization theory, deterrent theory, and security awareness in unison to explain the misuse of employees' IS in the context of Ethiopia. Finally, this study is organized as follows: first, presenting the problems, developing a conceptual framework and hypotheses based on criminological theories perspectives, defining a method for conducting the study, and demonstrating the future possible contributions of the study and concluding the paper.

Ethiopia's Experience in Cybersecurity Challenges

It is unfortunate that only little attention has been paid to the rapidly growing cybersecurity problems in Africa (Arage et al., 2016). In addition, more than 96% of the cybersecurity incidents have not been reported and addressed in the continent (Allen, 2021). For instance, African businesses have lost an estimated monetary loss of $3.5 billion to cyber-related frauds and thefts in 2017 (Allen, 2021). When we come to Ethiopia where this study specifically focused on, Global Cybersecurity Index showed that Ethiopian cybersecurity capability has been 21st in Africa and 115th in the world by 2020, whereas three years back in 2017, it had been 14th in Africa and 98th in the whole world (ITU, 2020). The mentioned figures show that Ethiopia has lagged behind many African nations in terms of cybersecurity issues, mainly in technical, legal, and capacity-building aspects (ITU, 2020). Multiple organizations in Ethiopia often fail to monitor cybersecurity threats, collect digital forensic evidences, and are unable to prosecute crimes related to IS abuse (Allen, 2021). The national cybersecurity agency (i.e. INSA) pointed out that there is an increasing cyberattack incidences in the country. For example, insider threats in Ethiopian Revenues and Customs Authority (ERCA) caused about ETB13 million losses in 2016 (Arage et al., 2016). The country's airlines also fired 11 employees in violation of IS security policies (Arage et al., 2016). Others also pointed out that the banking sector employees lack security awareness (Yohannes et al., 2019), and unable to fully manage and understand security issues, and even lack e-banking adoption capabilities (Arage et al., 2016). In addition, Ethiopian broadcasting media announced that the national examination for grade 10 and 12 in the year 2016 were stolen by internal employees of the ministry of education staff members and disseminated across the country via social networking Medias by agents in foreign countries. As a result, the examination was canceled and the country lost multimillion dollars that were spent for the whole process of exam preparation, examination, re-examination, transportation, manpower wages, and other logistics in the process.

Theoretical Grounding and Hypothesis development

IS security-related negative and positive human behaviours are investigated by adapting different theoretical lenses from behavioural or social science disciplines, including but not limited to PMT(protection Motivation Theory), TPB (Theory of Planned Behaviour), GDT(General Deterrence Theory), RCT(Rational Choice Theory), Agency Theory, and Activity Theory (Han et al., 2017). In order to offer more strong and comprehensive research contribution to IS problems, combining much related, but contending theoretical lenses and integrating them together could be an important first step (Lowry et al. 2019). However, integrating different theories into a single fresh conceptual model requires significant attention to ensure that the new combination is reasonable (Lowry et al. 2019). Here when combining different theories to develop an integrated research model two things should be considered: 1) possible proximity of those theoretical lenses to be combined, and 2) compatibility of their basic assumptions (Okhuysen & Bonardi, 2011). For example, several studies adapted neutralization techniques and deterrence constructs to evaluate, in particular, IS security negative behaviours (e.g. Siponen & Vance, 2010; Barlow et al., 2013) and these techniques were found to have positive and significant predictive powers. On the other hand, cultural values influence the overall belief systems and behaviors of individuals, including their attitudes and intentions (Hofstede, 1980) towards some actions. For instance, culture can influence the successful adoption and use of IS resources (Srite & Karahanna, 2006;

Leidner & Kayworth, 2006), because it has a profound effect on individuals' IS use and practice behaviors (Leidner & Kayworth, 2006), including the unauthorized use or act of IS security policy violations (Crossler et al., 2019; Chu et al., 2019). Here, this study focuses more on the effects of cultural dimension on the relationship between deterrent constructs, neutralization techniques, and IS security awareness to IS misuse intention. Using intention rather than attitude or actual behaviour in studying IS deviant behaviours is that attitude has a greater effect on intention (Bulgurcu et al., 2010) and intention is becoming a measure of a motivational state just prior to committing an act and a direct proxy to explain actual behaviours, so intention can be a suitable mediator to both of them (D'Arcy & Devaraj, 2012: pp.1096). According to D'Arcy & Devaraj (2012: pp.1096), IS technology misuse intention is defined as "a measured predisposition to engage in technology misuse". To this specific study, therefore, we define intention to IS resource misuse as: a measured predisposition of employees to engage in unauthorized and deviant uses and practices of computing resources in the workplace. As mentioned above, culture becomes a significant factor to determine individuals' differences in IS studies (Warkentin et al., 2015), by differentiating the members of one human group or society from the other (Hofstede, 1984), its values vary even within a sub-society (Srite & Karahanna 2006). Using the moderation effects of national cultural dimensions on the behavioural model is highly valuable to see its effects within the IS security theories, including this current research model. Adapting the moderating effects of individual-level culture assessment using Hofstede's cultural dimensions (e.g. Individualism/Collectivism (IND/COL), Power Distance (PD), Uncertainty Avoidance (UA) and Masculinity/Femininity (MAS/FEM)) have increasingly got incredible acceptance and applicability in IS studies (e.g. Srite & Karahanna 2006; Vance et al., 2020; Crossler et al., 2019). So, this study will adapt individual-level culture assessment and will be hypothesized accordingly.

Neutralization Theory

People use neutralization techniques to downplay the results of their illegitimate or abusive behaviors as a defense mechanism (Sykes & Matza, 1957). In addition, neutralization techniques have become a robust means of understanding individuals' intentions when violating social norms or offering a means of justifications in many contexts to reduce organizational sanction measures for deviant practices (Trinkle et al., 2021). Moreover, employees might seek to justify their deviant behaviours by denying responsibilities for their actions (Trinkle et al., 2021). However, all the techniques are not equally applicable for all contexts and perspectives, because different techniques work in a different way (i.e. some techniques might work well for general deviances, and some other techniques might be salient only for some other specific crimes) (Maruna & Copes, 2005). Since, all the techniques might not apply equally and significantly with all criminal actions (Maruna & Copes, 2005; Smallridge & Roberts, 2013), based on a broad literature survey only four techniques were selected to be adapted in this current study such as: appeal to higher loyalty, condemn the condemners, metaphor of the ledger, from Siponen & Vance (2010), and the claim of normalcy rationalization from (Hinduja, 2007). The techniques, then, will be hypothesized along with the effect of cultural moderation on the relationship between each technique with intention to misuse IS.

Condemn the Condemner

Condemn the Condemner refers to criminals shift the focus of attention towards the motivations or behaviors of the people expressing disapproval of their actions (Sykes & Matza, 1957). Using this technique employees criticize the authority holders to shift the focus from them to those who criticize them (Li & Cheng, 2013). Here, people may defend themselves by justifying that "Why focus on me? Everybody else is doing the same, including you, so don't point fingers at me" (McGregor, 2008: pp. 268). It also enables offenders to rationalize their actions by claiming that whom they condemn are pretenders and also likely engage in the behavior themselves (Sykes & Matza, 1957). In high PD culture, people accept that there is unequal distribution of power and ready to justify inequalities as the established or natural order of things (Hofstede, 1984, 2011), and as a result they are unlikely to condemn their managers or higher-ups. So, individuals from high PD culture are unable to shift the blame to higher authority persons (Hofstede, 1984, 2011). On the contrary, in low PD culture, people may think that everybody have same or similar power in front of the judge, thus, they may condemn the condemners easily. Having that in mind, PD moderates the relationship between Condemn the Condemner and intention to misuse IS. So, it can be hypothesized as: *H1: The use of condemn the condemners will positively influence employees' intention to misuse IS; H1a: The use of condemn the condemners will positively influence employees' intention to misuse IS resources; the effect is higher to low PD espoused culture than the high PD equivalent.*

Metaphor of the Ledger

This technique helps people to justify their deviant actions by showing their good deeds and names they had before help them to diminish their illegal actions (Klockars, 1974). In addition, offenders think that their former law abiding can be a credit for future deviances (Willison et al., 2018; Klockars, 1974), and by that means they try to minimize the resultant guilt or shame of their actions (Klockars, 1974). As discussed by Trinkle et al. (2021) if an employee is recognized as a hard worker in the organization and when he or she feels that the violation of IS laws and policies is

not so serious, he or she may engages in illegitimate or illegal uses and practices of IS resources by justifying the action. In that regard, an employee who misuses IS resources convince him/herself that the total positive image that he/she got from the workplace by the contributions in big projects compensate own IS misuse (Barlow et al., 2013; Siponen & Vance, 2010). With respect to cultural variable, power distance (PD) will condition the extent to which employee accepts the rational that superiors have more power (Srite & Karahanna, 2006: p. 682). In addition, PD culture is defined as the acceptance of inequalities in the existence of authority, wealth, status, and privilege (Hofstede, 1984). For instance, due to status and privilege differences, therefore, people in high PD culture obey the opinions and views of their higher-ups or senior staffs by assuming that they have bigger experience and expertise (Srite & Karahanna 2006), unlike the low PD societies where power is assumed to be equally distributed (Shore & Venkatachalam, 1996). People in high PD culture also perceive that personal use of IS tools by their higher-ups or experienced coworkers is more likely to be right than its usage by their equivalent peers (Alshare & Mousa, 2014). The metaphor of the ledger is positively related with individual's music piracy intentions (Smallridge & Roberts, 2013). Ordinary employees in high PD society, therefore, may think that to violate policies they have less power or acceptability to defend own deviances (Alshare & Mousa, 2014). Having that in mind, PD moderates the relationship between metaphor of the ledger and intention to misuse IS. So, this can be postulated as: *H2: The use of the Metaphor of the Ledger will positively influence employees' intention to misuse IS resources; H2a: The use of the Metaphor of the Ledger will positively influence employees' intention to misuse IS resources; the effect is higher within low PD espoused culture than the high PD counterparts.*

Appeal to Higher Loyalty

Offenders will use this technique to neutralize internal and external controls by claiming that their deviant behaviors are consistent with the moral obligations of a particular group of people (Maruna & Copes, 2005). So, offenders will justify their deviant actions as being parts of the higher-order value or ideal that are equal to or greater than self-interest (Li & Cheng, 2013) by claiming their actions as a long term social benefit and a greater good to the society (Siponen & Vance, 2010; Cheng et al., 2014). However, such people may not fully reject policies they are violating; rather, they justify that other norms are more important (Sykes & Matza, 1957), including satisfying the needs of their immediate in-groups (McGregor, 2008: pp.269). In short, using this technique, deviants claim as "I did it to protect, or take care of others" (McGregor, 2008). In a COL culture people depend more on one another, whereas people of individualistic society are not much inter-reliant. Boldly speaking, in a COL culture, individuals are highly integrated into their social groups or have cohesive in-groups and are firmly attached with families or friends, thereby protecting each other's in an exchange of absolute loyalty (Hofstede, 2011). As a member of a COL society, therefore, offenders believe that their policy violations are motivated to benefit the society as a member than for personal gains (Sykes & Matza, 1957; Chua & Holt, 2016). On the contrary, people from an IND culture are not much concerned about fulfilling the interests of others by violating policies and taking risks, contracting with this neutralization technique (Chua & Holt, 2016). Having that in mind, COL moderates the relationship between appeal to higher loyalty and intention to misuse IS. So, it can be postulated as: *H3: The use of appeal to higher loyalty will positively influence employees' intention to misuse IS resources; H3a: The use of appeal to higher loyalty will positively influence employees' intention to misuse IS resources; with higher influence in COL culture than in IND culture.*

Claim of Normalcy

This technique helps offenders to justify their deviant actions by stating that "how I act is nothing compared to others" (McGregor, 2008) or everybody is doing the same (Coleman, 1985). This technique was developed to explain employees' theft behaviors (Coleman, 1985), but later it was applied in predicting digital piracy (Hinduja, 2007) and becomes highly significant. Using this technique, deviants can minimize the guilt or shame of their wrongdoings by rationalizing that it is not a crime, rather it is in fact the norm in the society (Smallridge & Roberts, 2013). The claim of normalcy positively and significantly influenced individuals' digital piracy intentions (Smallridge & Roberts, 2013). Use of the claim of normalcy justification may be more prevalent within the society whom they are COL in nature and reliant on one another even for personal decisions. So, in COL culture, the norm of the society greatly influences an individual or a group, whereas, in IND culture the social norms will not have much effect on personal decisions (Srite & Karahanna, 2006). In a COL culture, therefore, people influence one another and if an action is the behaviour of most people, they are more likely to engage in that behaviour. If most employees violate policies and rules in a workplace, an employee from a COL society may behave like the many others (Hofstede, 2011), but, people from IND culture will not simply engage in deviances if they personally believe that it is illegal. Having that in mind, COL moderates the relationship between claim of normalcy and intention to misuse IS. So, it can be hypothesized as: *H4: The use of Claim of Normalcy will positively influence employees' intention to misuse IS resources; H4a: The use of Claim of Normalcy will positively influence employees' intention to misuse IS resources; the effect is stronger in COL espoused culture than in IND culture.*

Rational Choice Theory Based Deterrent Constructs

General deterrent theory (GDT) is bases for the foundation in the rational decision-making processes of individuals. According to GDT, the perceived severity and certainty of sanction affect individuals' IS security policy related decisions (Bulgurcu *et al.*, 2010) based on cost-benefit tradeoffs (D'Arcy et al., 2009). So, the cost of crime take an account of different measures, such as legal sanctions, economic overheads, personal-social costs, and social disapprovals (Charki et al., 2017). Here, sanctions are effective means of reducing illegitimate IS uses (Li et al., 2010), but the deterrence effects of sanctions vary across samples and contexts (D'Arcy et al., 2009). Even though, some argued that formal sanctions were not effective to explain information security policy violation intentions (Siponen & Vance, 2010), others like D'Arcy & Devaraj (2012) found that sanction intimidations have a direct and indirect influence on IS technology misuse behaviours. Trinkle et al. (2021) argued that organizational sanctions play an important role in reducing the motives of employees in violating policies. Even though one of the key constructs of GDT is sanction celerity, studies showed that its measurement is very difficult to apply (Willison et al., 2018) and it also lacks theoretical power (D'Arcy & Herath, 2011: pp.645). So, we will not consider it in this study.

Perceived benefit

Perceived benefit is defined, here, as the overall expected optimal outcomes that employees may obtain when using IS resources personally (Li & Cheng, 2013; Cheng et al., 2014). Assuming benefits, criminals may try to calculate the costs and benefits before they actually engage in an action (Li & Cheng, 2013). A study in personal internet usage showed that perceived benefits are found to be positively associated with employees' intention to misuse workplace IS resources (Cheng et al., 2014; Li et al., 2010). Here, when people are afraid or uncertain about the costs of misusing IS resources they may restrain from doing so. So, the association between the perceived costs or benefits on IS misuse is moderated by uncertain future consequences. In case of people from high UA culture are unwilling to engage in abusive behaviours for fear of unintended or uncertain future outcomes (perhaps sanctions or risks). Uncertainty avoidance is the extent to which risk of an action is accepted by the individual and measures the degree to which one feels or perceives threatened by an ambiguous situation (Srite & Karahanna, 2006). However, individuals in low UA culture are more likely to take risks if they think that their actions meet certain personal goals. So, the perceived benefits of misusing workplace IS resources do not encourage those who come from high UA culture than low UA culture. So, perceived benefits are associated with intention to misuse IS and the relationship is moderated by UA culture. On the other hand, MAS/FEM is the extent to which gender inequalities are embraced and espoused by individuals, whereby this variable has the power to moderate the relationship between perceived benefits and IS misuse (Srite & Karahanna, 2006). In addition, individuals in the MAS culture place more emphasis on work goals, including assertiveness, earnings, and performance (Hofstede, 1984), but FEM culture has a tendency to engage in activities that meet personal pleasures and relationship goals, such as relaxed work environment, friendly atmosphere, quality of life and sincere relationship with others (Srite & Karahanna, 2006). So, people from FEM culture due to their perceived social goals may involve in IS misuse behaviours. In that regard, people in the FEM culture may simply engage in social interactions with friends or relatives using workplace internet connections to meet their gender roles. As a result, the benefits of personal use of workplace IS have a greater impact on FEM culture than the MAS one. So, can be hypothesizes as: *H5: The higher the Perceived benefits of using organizational IS resources for personal reasons, the higher will be the probability of employees' intention to misuse those resources; H5a: The influence of Perceived Benefit on intention to misuse organizational IS resources is highly moderated by FEM espoused culture than the MAS equivalent; H5b: The influence of Perceived Benefit on intention to misuse organizational IS resources is highly moderated by low UA espoused culture than high UA espoused culture.*

Perceived sanction certainty and Perceived sanction severity

The cost of employees' IS misuse is going to be calculated based on the likelihood of detection certainty and sanction severity (Cheng et al., 2014). The perceived certainty and severity of both formal and informal sanctions were adapted in IS security studies (D'Arcy & Herath, 2011; Cheng et al., 2014) even if there are some clear variations between the effects of the two variables across studies, both had significant influence on misuse intention (D'Arcy et al., 2009). However, perceived detection certainty has been highly correlated with intentional deviances (Cheng et al., 2014). On the other hand, perceived sanction severity negatively affected individual's intention to participate in IS misuse (D'Arcy et al., 2009) and positively linked with security policy compliance. It means, the higher the probability of detection certainty and the greater the severity of sanction, the better employees are deterred from IS misuse (Hovav & D'Arcy, 2012; Barlow et al., 3013). If people are not certain about the benefits as well as the sanctions related to the actions of their IS misuse, they may be profited or restrained from doing so. In this regard, the low UA culture is described by flexibility, need of fewer written rules, greater willingness to take conscious risks, but high UA culture is described by less willingness to take risks, needs explicit and more written rules (Hofstede, 1984, 2011; Hwang & Lee, 2012). So, UA insights moderate the relationship between perceived sanctions and IS misuse. Having that in

mind, in low UA culture people may likely take conscious risks, including sever or certain sanctions if there are perceived comparative advantages on their actions, whereas people in high UA culture, they are not willing to involve by taking risks. Thus, it is postulated as: *H6: The higher the perceived certainty of sanction on using organizational IS resources for personal reasons, the lower will be the probability of employees' intention to misuse those resources; H8: The higher the perceived severity of sanction on using organizational IS resources for personal reasons, the lower will be the probability of employees' intention to misuse those resources; H6a: The influence of Perceived Certainty of Sanction on intention to misuse organizational IS resources is highly moderated by low UA espoused culture than the high UA equivalent; H8a: The influence of Perceived Severity of Sanction on intention to misuse organizational IS resources is highly moderated by low UA espoused culture than the high UA equivalent.*

Awareness towards IS security behaviors

IS security awareness is viewed as one of the most important preconditions for security threat deterrence and plays a central role towards policy compliance (Bulgurcu et al. 2010). To comply with IS security policies and rules, employees should be aware of them (Hwang et al., 2019). Level of awareness and preventive measures may vary depending on the perceived severity and certainty of sanction (Hwang et al., 2019). IS security countermeasures, such as policies, education, training and awareness creation campions, have become essential components of security measures (Hovav & D'Arcy, 2012; Bulgurcu et al., 2010). Extant studies (e.g. Han et al., 2017; Bulgurcu et al., 2010) have proved that individuals' awareness of security measures significantly and positively influenced policy compliance.

IS Security Countermeasure Awareness and Behavioral Intention

IS security countermeasures are important tools to defend workplace IS resources against potential security harms. In addition, IS security awareness is recommended in improving legitimate use of IS resources (Bulgurcu et al., 2010), create strong security cultures (Da Veiga, 2015), and possibly reduce vulnerabilities (D'Arcy et al., 2009). Having these in mind, IS security deterrence awareness, therefore, positively and significantly affects individuals' perceptions of the certainty and severity of workplace sanctions to IS misuse actions (D'Arcy et al., 2009). IS security awareness refers to individuals' knowledge and understanding about security issues (Haeussinger & Kranz, 2013) and frequently proved to influence intention to use IS and enhance policy compliance (Haeussinger & Kranz, 2013). According to GDT if punishments are certain and the resultant penalties are severe, then those who are planning to commit a crime will stop and think twice if they know that there will be penalties to violators (Vaidyanathan & Berhanu, 2012). IS security awareness significantly influenced individuals to engage either in misusing or safeguarding workplace IS resources (Bulgurcu et al., 2010). Moreover, IS security countermeasure awareness directly or indirectly improves compliance with security policy (Haeussinger & Kranz, 2013; Han et al., 2017) and reduce the IS misuse (Hovav &D'Arcy, 2012; D'Arcy et al., 2009). On the other hand, organizational sanctions discourage employees' illegitimate actions, including IS misuse (D'Arcy et al., 2009); however, this assumption works if and only if they know and understand IS deterrents and the resultant sanctions (Da Veiga, 2016). So, people who are aware of the certainty and severity of sanctions in connection to IS deviant behaviors (Vaidyanathan & Berhanu, 2012) can limit themselves and others from engaging in the behaviour. Besides, IS security deterrence awareness and perception have contextual and socio-cultural basis that have made disparities of results between individuals of different cultural or subcultural groups. According to Srite & Karahanna (2006) uncertainty towards system use behaviours could be reduced though an informational influence of peers and friends. In this regard, the level of awareness that people do have, maybe determined by the lowness or highness of UA cultural values. Individuals from low UA culture can easily discuss about risks or uncertainties (Hwang & Lee, 2012), so creating an awareness to them could be simpler. So, the more the awareness, the lower will be the uncertainty or ambiguity towards some behaviours, including IS security deviances. Here, people from low UA culture could easily determine the value placed on the target's capability (Hwang & Lee, 2012) if they have IS security awareness that enables them to rationally decide on the issues. In addition, creating an awareness to the people of low UA culture could be just to inform them about the issues, maybe the basic IS security, because they can discuss risks or uncertainties very well (Hwang & Lee, 2012). Conversely, in high UA culture people feel threatened by uncertain or unknown situations and need to have explicit rules and guideline for decision for actions. Here, informing people about sanction certainty and sanction severity on personal use of IS resources can increase the perceived risk of engaging in the action, especially in high UA culture than low UA culture. So, for uncertain future outcomes people in high UA culture require clear and precise awareness to engage in the action, whereas people of low UA culture may not be more concerned about clarity of sanction information to take risks. So it can be hypothesized as: *H7: The higher employees' level of IS security awareness towards possible IS use and practice behaviour, the lower will be their intention towards organizational IS misuse intention; H9: the higher the level of employees' awareness towards the risks of IS misuse, the healthier will be their perception on sanction certainty towards IS misuse intention; H10: the higher the level of employees' awareness towards the risks of IS misuse, the healthier will be their perception*

on sanction severity towards IS misuse intention; H7a: The influence of employees' IS security awareness on intention to misuse organizational IS is strongly moderated by high UA espoused culture than low UA espoused culture; H9a: The influence of employees' IS security awareness on the perceived certainty of organizational sanction is strongly moderated by high UA espoused culture than low UA espoused culture; H10a: The influence of employees' IS security awareness on the perceived severity of organizational sanction is strongly moderated by high UA espoused culture than low UA espoused culture.

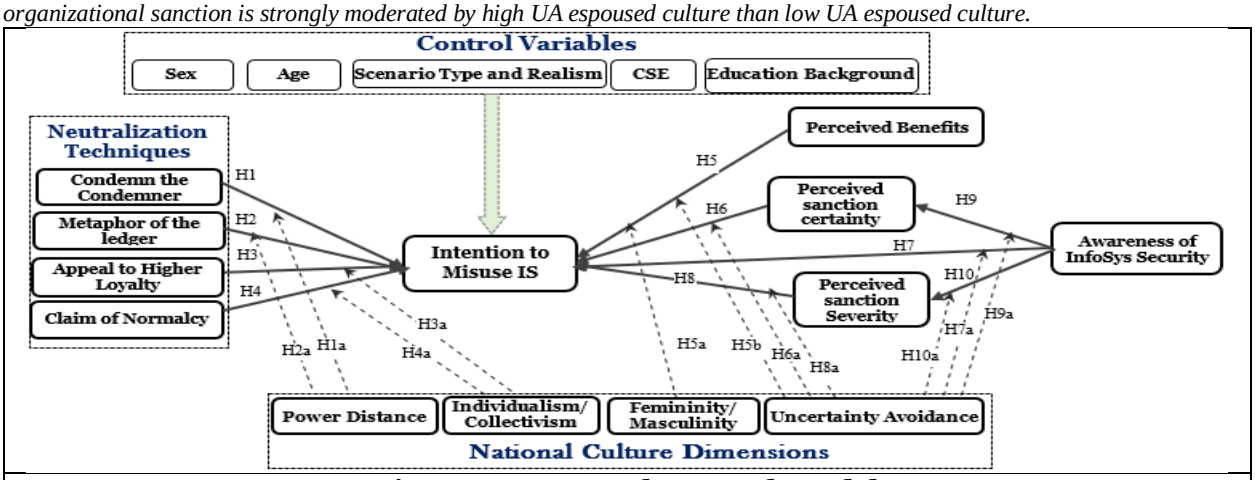

Figure1: Conceptual Research Model

Study Methodology

The aim of this study is to address the research questions because the study methodology should align with answering the questions on hand. To that end, the research model, which is constructed based on the research question as a result of the empirical literature review, will be tested empirically. Cultural studies are mostly conducted by a positivist paradigm and cross-sectional quantitative survey (Hofstede, 2011) because culture is traditionally understood as a system of values designed by cultural dimensions (Hofstede, 1984). This research is proposed to predict the dependent variable (i.e. IS misuse intention) by adapting existing questionnaire instruments. The target population to this study will be all professional employees who have access to organizational IS resources in their day to day routines. Here, behavioural factors, including employees' attitude, intention, and motivation are not easily provable by means of different than self-reporting (Podsakoff & Organ, 1986). So, paper-based questionnaires with a hands-on random distribution is planned for employees to self-report their feelings and perceptions. To that end, we will adapt scenario-based data collection approach, because scenario-based method provides a less threatening way of measuring IS misuse intentions, because scenario methods are highly applicable and recommended in studying criminal or unethical behaviors (e.g. Siponen & Vance, 2010). To that, this study is designed to understand employees IS misuse intention, the scenario method, therefore, will be more salient. To empirically test the model, Smart-PLS and SPSS with Amos will be employed. To see how constructs work; the pilot test will be performed using 100 university staffs. As a choice and clarity of questions, instrument translation and back translation will be performed for idea consistency.

Potential Contribution

Theoretical contribution

In short, study of national culture with criminological theories will probably support organizations to protect their IS resources by developing cultural and context-specific security policies and deterrent countermeasures. The study mainly focuses more on employees' intentional misuse of IS resources in Ethiopia. In this context, there is no study in the extant literatures that is conducted to show the moderating influence of national culture between the mentioned criminological theories and IS security awareness on IS misuse intention. Studies are lacking by integrating different theoretical lenses in this context, so this study is the first to stretch the theoretical underpinning in IS security studies. The study will shed light on how culture dimensions, IS security awareness and criminological theories are integrated to understand and determine employees' IS misuse intention.

Practical Implication

This study is intended to shed light on IS security studies with implications for scholars, managers, and IS users of Ethiopian organizations. This study will help to realize employees' IS misconduct in support of cultural and contextual relevant behavioral development and implementation, such as security policies, standards, protective procedures, and

code of conduct. It also provides implications for managers and policymakers on how to develop appropriate policies and practices that may curb future use of employees' neutralization techniques and increase an awareness of effective deterrence countermeasures. Moreover, the study helps managers deliver effective awareness-raising campaigns to their employees. Implications for employees are to make them aware of the different threats and influences associated with deterrent countermeasures, including sanctions. It also assists foreign investors in developing and implementing appropriate IS measures when investing in Ethiopia. The study also applies to countries with similar cultures to Ethiopia.

Conclusion

Even though this ongoing research includes an important comprehensive conceptual research model that can and should be tested to evaluate how the hypothesized relationships explain employee IS misuse behaviour, there are no concrete findings to see 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 organizational employees). However, it provides an overall insights and understandings of the moderating effects of espoused 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 context of the developing economy.

References

Allen, N. 2021. "Africa's Evolving Cyber Threats, African Center for Strategic Studies," Washington DC.

Alshare, K., & Mousa, A. 2014. "The moderating effect of espoused cultural dimensions on consumer's intention to use mobile payment devices," Proceedings of 35th International Conference on IS. Auckland, New Zealand.

Arage, T. M., Belnger, F. & Tesema, T. B. 2016. "Investigating the Moderating Impact of National Culture in IS Security Policy Violation: The Case of Italy and Ethiopia," MCIS 2016 Proceedings. 56. Paphos, Cyprus.

Barlow J. B., Warkentin, M., Ormond, D. & Dennis, A. R. 2013. "Don't make excuses! Discouraging neutralization to reduce IT policy violation," Computers & Security, (39: B), pp.145–159.

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), pp.523-548.

Charki, M. H., Josserand, E., & Boukef, N. 2017. "The paradoxical effects of legal intervention over unethical information technology use: A RCT perspective," Journal of Strategic Information Systems, (26), pp. 58–76.

Cheng, L., Li, W., Zhai,Q. & Smyth, R. 2014. "Understanding personal use of the Internet at work: An integrated model of neutralization techniques & GDT," Computers in Human Behavior, (38), pp.220–228.

Chua, Y. T. & Holt, T. J. 2016. "A Cross-National Examination of the Techniques of Neutralization to Account for Hacking Behaviors," Victims & Offenders, (11), pp.534–555.

Coleman, J. W. 1985. "The Criminal Elite: The Sociology of White-Collar Crime," New York: St. Martin.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. 2013. "Future directions for behavioral information security Research," Computers & Security, (32), pp.90-101.

D'Arcy, J. & Herath, T. 2011. "A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings," European Journal of Information Systems, (2011), pp.1–16.

D'Arcy, J., Hovav, A., & Galleta, D.F. 2009. "User awareness of security countermeasures and its impact on information systems misuse: Deterrence approach," Information Systems Research, (20:1), pp.79-98.

Da Veiga, A., & Martins, N. 2015. "Improving the information security culture through monitoring and implementation actions illustrated through a case study," Computers & Security, (49), pp.162-176.

Gagliardone, I. & Sambuli, N. 2015. "Cyber Security and Cyber Resilience in East Africa," Global Commission on Internet Governance, Paper Series: No. 15, May 2015.

Gupta, G., Zaidi, S. K., Udo, G. J., & Bagchi, K. K. 2015. "The Effect of Espoused Culture on Acceptance of Online Tax Filing Services in an Emerging Economy," Advances in Business Research, (6), pp.14-31.

Haeussinger, F. J. & Kranz J. J. 2013. "Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior," 34th International Conference on IS, Milan, Italy, pp. 1-16.

Han, J.Y., Kim, Y. J., & Kim, H. 2017. "An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective," Computers & Security, (66), pp. 52-65.

Hinduja, S. 2007. "Neutralization theory and online software piracy: An empirical analysis," Ethics and Information Technology, (9:3), pp.187–204.

Hofstede, G. 1984. "Culture's Consequences: International Differences in Work-Related Values," Beverly Hills, CA: SAGE Publications.

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

Hovav, A., & D'Arcy, J. 2012. "Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the US &South Korea," Information & Management, (49:2), pp.99–110.

Hwang, I., Wakefield, R., Kim, S., & Kim, T. 2019. "Security Awareness: The First Step in Information Security Compliance Behavior," Journal of Computer Information Systems, DOI: 10.1080/08874417.2019.1650676.

Hwang, Y., & Lee, K. C. 2012. "Investigating the moderating role of uncertainty avoidance cultural values on multidimensional online trust," Information & Management, (49), pp.171–176.

Klockars, C. B. 1974. "The Professional Fence", New York (NY), Free Press.

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), pp.357-399.

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), pp. 635-45.

Li, W. & Cheng, L. 2013. "Effects of Neutralization Techniques and Rational Choice Theory on Internet Abuse in the Workplace," Dalian University of Technology, PACIS 2013 Proceedings, AIS Library. Paper 169.

Lowry, B. P., Zhang, J., Moody, D. G., Chatterjee, S., Wang, C., & Wu, T. 2019. "Proposing an integrative theory to address the sociotechnical nature of cyber-harassment in light of technology-based opportunism," Journal of Management Information System.

Maruna, S. & Copes, H. 2005. "What Have We Learned from Five Decades of Neutralization Research?," The University of Chicago press, pp,221-320.

McGregor, S. L. T. 2008. "Conceptualizing immoral and unethical consumption using neutralization theory," *Family &Consumer Sciences Research Journal, (36*:3), pp.261–276.

McSweeney, B. 2002. "Hofstede's model of national cultural differences and their consequences: A triumph of faith – a failure of analysis," Human Relations, (55:1), pp.89–118.

Okhuysen, G., & Bonardi, J. P. 2011. "The Challenges of Building Theory by Combining Lenses," Academy of Management Review (36:1), pp. 6-11.

Podsakoff, P. M., & Organ, D. W. 1986. "Self-reports in organizational research: Problems and prospects," *Journal of Management, (12:*4), pp.531–544.

Ponemon Institute. 2020. 2020 Cost of Insider Threats Global Report.

Shore, B. &Venkatachalam, A. R. 1996. "Role of national culture in the transfer of information technology," Journal of Strategic Information Systems, (5:1), pp.19-35.

Siponen, M. & Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," MIS Quarterly, (34:3), pp.487-502.

Smallridge, J. L. & Roberts, J. R. 2013. "Crime Specific Neutralizations: An Empirical Examination of Four Types of Digital Piracy," International Journal of Cyber Criminology, (7:2), pp.125-140.

Srite, M. & Karahanna, E. 2006. "The role of espoused national cultural values in technology acceptance," MIS Quarterly, (30:3), pp.679–704.

Sykes, G. M., & Matza, D. 1957. "Techniques of neutralization: A theory of delinquency," American Sociological Review, (22:6), pp.664-670.

Trinkle, B. S., Warkentin, M., Malimage, K., & Raddatz, N. 2021. "High-Risk Deviant Decisions: Does Neutralization Still Play a Role?," Journal of the Association for Information Systems, (22:3), pp.797-826.

Vaidyanathan, G. & Berhanu, N. 2012. "Impact of Security Countermeasures in Organizational Information Convergence: A Theoretical Model," Issues in Information Systems, (13:2), pp.21-25.

Vance, A., Siponen, M. T. & Straub, D.W. 2020. "Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures," Information & Management, *(57:4).*

Warkentin, M., Charles-Pauvers, B., & Chau P. Y. K. 2015. "Cross-cultural IS research: perspectives from Eastern and Western traditions," European Journal of Information Systems, (24), pp.229–233.

Willison, R. & Warkentin, M. 2013. "Beyond deterrence: An expanded view of employee computer abuse," MIS Quarterly, (37), pp.1-20.

Willison, R., Lowry, P. B., & Paternoster, R. 2018. "A Tale of Two Deterrents: Considering the Role of Absolute and Restrictive Deterrence to Inspire New Directions in Behavioral and Organizational Security Research," Journal of the Association for Information Systems, (19:12), pp.1187-1216.

Yohannes, T., Lessa, L. & Negash, S. 2019. "Information Security Incident Response Management in an Ethiopian Bank: A Gap Analysis," Twenty-fifth Americas Conference on Information Systems, Cancun.