1-2020

Cultural Influence and the Effective Use of Security Awareness in Congolese Organizations

Arnold Nzailu
Dakota State University

Insu Park
Dakota State University

Recommended Citation
Nzailu, A. (2020). Cultural Influence and the Effective Use of Security Awareness in Congolese Organizations. HICSS.

Cultural Influence and the Effective Use of Security Awareness in Congolese Organizations

Arnold Nzailu
Dakota State University
abnzailu@pluto.dsu.edu

Insu Park
Dakota State University
insu.park@dsu.edu

Abstract

In today's global economy, there is a growing need to apply technological advancements as well as training and awareness materials from western countries on information security programs in developing nations. To understand the underlying drivers of employees' effective use behaviors in relation to security awareness programs in organizations, this study examines the extrinsic and intrinsic motivation factors that influence employees located in developing nations. The results indicate that influencing employees' attitudes toward security is a better predictor of employees' effective use of security awareness programs than their intention to comply. Cultural effects has also proven to have an influence on employees' effective use of security awareness programs.

1. Introduction

In today's highly connected world, the protection of digital assets has become a priority for organizations and nation states. The cost of circumventing security measures has increased exponentially, thus making it more difficult for hackers to penetrate organizations' information systems. In response, hackers are adapting and taking advantage of "low-hanging fruit." Microsoft [1] explained that three of the low-hanging fruit routes most commonly employed by cyber attackers include social engineering, poorly secured cloud apps, and legitimate software platform features. Hackers are always looking for the path of least resistance in the security chain, and it is easier and less costly to social engineer a user into clicking a malicious link or opening a phishing email [1].

The identify theft resource center reported [2] that the total number of breaches in 2018 was 1,244, which decreased by 23% from the total number reported in 2017, which was 1,632 breaches. However, the reported number of consumer records containing sensitive personally identifiable information (PII) jumped significantly, with a 126% increase from 2017 (197,612,748 records exposed) to 2018 (446,515,334 records exposed). A breakdown of the reported breaches shows that humans played a sizable role through either accidental exposure, employee error, negligence, improper disposal, unauthorized access, or insider theft.

Mitnick and Simon [3, 4] explained that the best way to defeat human hacking is to implement an ongoing security awareness program. They suggest that the goal of a security awareness program must be to modify human behavior and attitude in the context of the protection of digital assets.

On the basis of research suggesting that behavioral models do not hold universally across cultures [5-7], we examine how individual culture may influence individual-level effective use of security awareness programs. The Democratic Republic of Congo (DRC) is ranked as the third most diverse country in the world, which leads us to argue that individual-level cultural values differ in degrees among individuals in DRC. Cultural values are incorporated into an extended model of technology acceptance in the form of independent variables and as moderators of key relationships.

Drawing from prior research about culture and information systems, we posit that national culture impacts individual values, which in turn influence the effective use of security awareness through technology acceptance.

2. Theoretical Background

In this section, we review the literature on culture and the cultural dimension, in addition to the effective use and acceptance of technology to develop the theoretical model and hypotheses.

2.1. Culture

Crossler et al. [8] argued that "one of the biggest issues and limitations of behavioral InfoSec research is that the majority of it has been conducted in western cultures, with occasional studies being conducted in

URI: https://hdl.handle.net/10125/63782
978-0-9981331-3-3

Asia and elsewhere. Most of the rest of the world has been overlooked; and little has been done to examine cross-cultural considerations involved with insider behavior, IT security compliance, hacking, security violations, and so forth."

Prior to Crossler et al. [8], Xunhua Guo and Nan Zhang [9] discussed how cultural issues have become an important topic in information systems research, particularly concerning user behavior during the adoption, diffusion, and infusion of new technologies and systems. Kruger, Flowerday, Drevin, and Steyn [10] suggested that cultural factors such as mother tongue and the area where a person grew up, among others, do have an impact on security awareness levels and should be taken into consideration when planning and developing the materials and processes of information security awareness programs.

Xunhua Guo and Nan Zhang [9] argued that when cultural issues are taken into account, Hofstede's well-known five dimensions model [11] provides the most influential theoretical framework. Due to its long-standing reputation and widespread use in the IS cross-cultural studies [12-14], this study has selected to use Hofstede's cultural theory. Hofstede defines culture as "the collective programming of the mind which distinguishes the members of one human group from another" [5]. Hofstede proposes four widely cited dimensions of national culture: individualism/collectivism, power distance, uncertainty avoidance, and masculinity/femininity.

Table 1 Culture Dimension

Dimensions	Definition
Individualism/ collectivism (IC)	Degree to which the individual emphasizes his/her own needs as opposed to the group needs and prefers to act as an individual rather than as a member of a group.
Power distance (PD)	Degree to which the individual accepts large differentials of power and inequality as normal. Power distance will condition the extent to which the employee accepts that his/her superiors have more power.
Uncertainty avoidance (UA)	Uncertainty avoidance is the level of risk accepted by the individual, which can be determined by his/her emphasis on rule obedience, ritual behavior, and labor mobility. This dimension examines the extent to which one feels threatened by ambiguous situations.
Masculinity/ femininity (MA_FE)	The degree to which an individual espouses gender inequalities. Individuals who espouse masculine values emphasize work goals such as earnings, advancement, competitiveness, performance, and assertiveness. On the other hand, individuals who espouse feminine values tend to emphasize personal goals such as a friendly atmosphere, comfortable work environment, quality of life, and warm personal relationships.

Our understanding of how culture influences technology adoption and ultimately the effective use of technology is very limited. Studies by Straub et al. [6, 15] and Rose et al. [16] have suggested that the TAM can be generalized to the Swiss and Arab cultures but not to the Japanese culture, thus implying that the theoretical relationships posited by TAM are valid for a small number of cultures other than that of the USA. Even though these studies have provided valuable insights into technology acceptance in different cultures, its ability to predict the effective use of security awareness program at an individual level cannot be assumed in such a diverse country as the DRC.

2.2. Technology Acceptance Model

The theory of reasoned action (TRA) [17], the theory of planned behavior (TPB) [18], and the technology acceptance model (TAM) [19] are the best known and most used models in IS to study the acceptance of technology. Of the three, the TAM is arguably the most widely accepted for use in technology acceptance studies. Through the years and in multiple studies, TAM has demonstrated that perceived ease of use influences perceived usefulness and, in turn, both beliefs influence behavioral intention to use a specific system. However, TAM did not incorporate the effect of the social environment on behavioral intention. Cooper et al. [20] argued that shared perceptions provide powerful cues for individuals regarding appropriate and desired behavior, in addition to performance expectations, within a contextual setting. Shared perceptions can be linked to culture; therefore, it can be inferred that technology adoption depends on an individual's attitudes, beliefs, and behavior, which are influenced by their cultural environment.

Researchers [21-25] have previously demonstrated that cultural values can influence the needs and motives for using a product, and attitude toward purchasing and using products. Following on from this line of thought, this study suggests that culture, as

proposed in our model, influences the effective use of security awareness.

2.3. Effective Use Theory

Burton-Jones and Grange [26] argued that despite the large body of existing research on when and why systems are used, very few studies have examined what effective system use involves and what drives it. They define effective use as increasing achievement of the goals of using the system. Burton-Jones and Grange draw on representation theory to derive a high-level framework of how effective use and performance evolve, as well as specific models of the nature and drivers of effective use. Andrew and Camille models explain the effective use of any information system. The authors state that this is not offered by traditional views, which tend to consider information systems simply as another tool rather than examining their unique characteristics. Their analysis suggests that users are more likely to take actions to improve effective use and performance when: (1) users are more knowledgeable, experienced, motivated, and supported; (2) systems and tasks are simple, flexible, familiar, and independent of other systems/tasks; and (3) users can take actions and rapidly see their consequences.

Furthermore, Burton-Jones and Grange [26] considered contexts in which users receive immediate feedback on performance, and contexts in which feedback is delayed, and found that users achieve more effective use and higher performance more quickly in the former context than the latter. They also pointed out the importance of actions that users take to improve effective use. They argued that users' learning and adaptation actions have immediate benefits for effective use, which in turn can change the user context by making users more knowledgeable and making the system more or less complex; this can affect the entire process of improving effective use and performance.

Other studies [27-29] have shown the effect of both intrinsic and extrinsic motivation as they relate to user behavior and usage intention by extending the TAM. The results of these studies consistently reveal that both intrinsic and extrinsic motivation factors influence user behavior and usage intention toward technology.

Our understanding of how effective use is influenced by the user's knowledge, experience, motivation, support, simplicity, and feeling of control over their actions helps to frame the research model presented in the following section by enabling us to group constructs into intrinsic or extrinsic motivation.

3. Research Model

The research model presented in Figure 1 integrates cultural values into an extended TAM to illustrate their impact on the effective use of security awareness.

3.1. Motivations

Intrinsic motivation refers to feelings associated with an action. In contrast, extrinsic motivations come from peer pressure and interactions with others in a group, the physical environment, or the ways in which the culture of an organization rewards and punishes certain activities [30]. From an intrinsic motivational (IM) perspective, employee behaviors arise from the employee's need to feel competent and self-determined in dealing with their working environment [31-33].

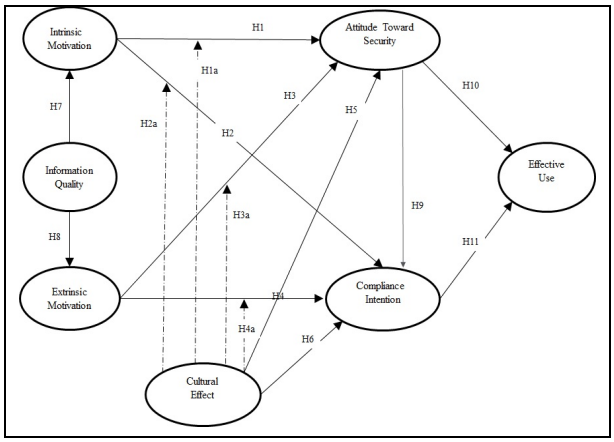

Figure 1 – Research Model

Researchers have found that employees with high confidence in their ability to provide a valuable contribution are more likely to accomplish specific tasks [34, 35]. For this study, the intrinsic motivation variable comprises self-efficacy, perceived usefulness, and perceived value. Self-efficacy is typically manifested in people believing that their knowledge can help to solve job-related problems and improve work efficacy [36, 37]. Perceived usefulness is considered to be the degree to which a person believes that using a particular system would enhance their job performance [38]. Finally, perceived value refers to the overall evaluation of the change related to a new information system implementation, based on the comparison of benefits and costs [39, 40].

While numerous empirical studies of technology acceptance and implementation focus on situations in which individuals have some discretion in adopting such technology, this study focuses on the mandatory aspect of adoption. This is because information security compliance in highly regulated industries, such as banking and telecommunications, are not

voluntary. Boss, Kirsch, Angermeier, Shingler and Boss [41] found that the acts of specifying policies and evaluating behaviors are effective at convincing individuals that security policies are mandatory. The perception of obligation is effective in motivating individuals to take security precautions; when these individuals believe that the management is watching, they will comply. Based on the above, this study removes ease of use from this extended version of TAM, as the study was conducted in organizations in which compliance with security guidelines are mandatory. In this situation, individuals do not have a choice of whether to comply, even if the security requirements are not easy to use.

This study posits that employees who have a positive perception of their organizations security awareness program, and who believe that they can contribute to their organization's performance by effectively using it, will develop a more positive attitude and intention to comply with the security requirements of their organization. Hence, the following hypotheses are proposed.

H1: Intrinsic motivation positively influences employees' attitudes toward the security awareness program.

H2: Intrinsic motivation positively influences employees' intentions to comply with the security awareness program.

From the perspective of extrinsic motivation (EM), employee behaviors are motivated by external variables that are independent of the content of the activity itself [42]. For this study, the EM variable is composed of top management support, sanction, reward, and social pressure. Top management support is defined as the enthusiasm, support, personal involvement, and overall leadership offered by senior management with respect to a specific activity [43]. Reward is defined as the tangible or intangible compensation that an organization gives to an employee in return for compliance with the requirements of the information security policy [44]. Sanction is defined as the tangible or intangible penalties—such as demotion, loss of reputation, reprimand, monetary or nonmonetary penalties, and an unfavorable personal mention in oral or written assessment reports—incurred by an employee for noncompliance with the requirements of the information security policy [44]. Social pressure is defined as the social pressure perceived by an employee regarding compliance with the requirements of the information security policy, caused by the behavioral expectations of such important referents as executives, colleagues, and managers [44].

This study proposes that employees who have a positive perception of the external motivation factors—that is, management support for the security awareness program, organizational reward for complying with security guidelines, proportional sanction when an employee fails to comply with policy, and positive social pressure from colleagues—will develop a more positive attitude and intention to comply with the security requirements of their organizations. Hence, the following hypotheses are proposed.

H3: Extrinsic motivation positively influences employees' attitudes toward the security awareness program.

H4: Extrinsic motivation positively influences employees' intentions to comply with the security awareness program.

3.2. Cultural Effect

Srite and Karahanna [7] found that the effect of culture on individuals depends on the degree to which an individual is willing to become involved and engage with the values of their own culture. Their scales were found to have adequate psychometric properties and were successfully integrated with a model derived from TAM. This paper follows the same approach and measures culture at the individual level, thus enabling the moderating effects of culture within the developed model.

The general prediction is that users with higher PD values are more likely to be dependent on referent power in decision-making; that is, they would be more influenced by the views of others, particularly their superiors, in deciding whether to adopt technologies. Dinev et al. [45] compared samples from South Korea and the USA in the context of adopting protective (e.g. anti-virus) software and found that the relationship between SN and BI was significant for the South Korean sample (which had a high-PD culture) but not for the USA sample (low-PD culture). Like South Korea, the DRC is considered a high-PD culture, which can be seen in the hierarchical structure of its society.

A high-masculinity culture emphasizes work goals, while a low-masculinity culture encourages people to follow traditional standards that are more people-oriented than those with high masculinity values. A high-femininity culture is expected to be more influenced by interpersonal contact, while a high-masculinity culture would be expected to be more influenced by features that encourage the achievement of work goals. Srite and Karahanna [7] found the opposite effect, with a significant effect of PU on BI for a USA sample (which is a more feminine culture) but no significant effect for a Chinese sample (a more masculine culture). The DRC was originally considered a low-masculinity culture where people

cared for the wellbeing of their neighbors. However, the DRC has been through two decades of internal civil war that may have change its original position.

Srite and Karahanna [7] and Dinev et al. [45] supported the prediction that subjective norms such as social pressure have more influence in a high-UA context than in a low-UA context. While great uncertainty is a part of everyday life in the DRC, the people of the DRC are characterized as being high UA.

In individualistic societies, individuals focus on their own achievements and personal goals rather than the group to which they belong. In collectivistic societies, people prefer loyalty and group success to their own individual gain. Numerous researchers [45] have proved the relationship between SN and BI to be stronger in collectivist cultures than in individualistic cultures. Srite [7] found that while SN was a significant predictor of BI in a Chinese sample (which is a collectivist culture), there was no significant effect of SN on BI in the USA (an individualistic culture). The DRC is considered to be a collectivist society where decisions are made by families, clans, and tribes. Based on the discussion above, we postulate the following hypotheses:

H5: The cultural effect influences employees' attitudes toward the security awareness program.

H6: The cultural effect influences employees' intentions to comply with the security awareness program.

H1a: The cultural effect moderates the relationship between intrinsic motivation and employees' attitudes toward the security awareness program.

H2a: The cultural effect moderates the relationship between intrinsic motivation and employees' intentions to comply with the security awareness program.

H3a: The cultural effect moderates the relationship between extrinsic motivation and employees' attitudes toward the security awareness program.

H4a: The cultural effect moderates the relationship between extrinsic motivation and employees' intentions to comply with the security awareness program.

3.3. Information Quality

DeLone and McLean identified five information success features: system quality, use, user satisfaction, individual impact, and organizational impact. Prior research has developed numerous measures of information quality and has identified various constructs. Larcker and Lessig [46] introduced the notions of the perceived importance of information and the perceived usefulness of information. The perceived importance refers to factors related to the relevance, meaningfulness, importance, helpfulness, and significance of the presented information. Perceived usefulness refers to factors associated with concepts such as unambiguity, clarity, and readability. Meanwhile, Lee et al. [47] mapped 16 different dimensions of information quality, accessibility, completeness, and timeliness to four descriptive quadrants: sound, dependable, useful, and usable. Dickerson and Gentry [48] argued that innovation with substantial complexity requires skills that are more technical, and demands significant implementation and operational efforts, which decrease its chances of adoption. Thus, this study expects that if employees believe information provided by the security awareness program to be complete, accurate, and easy to apply, they will develop more positive attitudes toward the security awareness program of their organization. Hence, the following hypothesis is proposed.

H7: Information quality positively influences employees' intrinsic motivation.

H8: Information quality is positively associated with employees' extrinsic motivation.

3.4. Attitude Toward Security

The association between attitude and behavioral intentions has been considered in previous studies [49], which have shown that attitude toward complying with acceptable information system behaviors positively influences behavioral intentions [50-55]. Davis, Bagozzi, and Warshaw [56] used the TAM to explain why a user accepts or rejects information technology. The TAM provides understanding with which researchers can explain how external variables influence belief, attitude, and intention to use. According to the TAM, people's actual use of a technology system is influenced directly or indirectly by the user's behavioral intentions, attitude, perceived usefulness of the system, and perceived ease of use the system. Furthermore, attitude toward moral behavior has been investigated by Chang [57], who found that it significantly influences behavioral intentions. The TPB aims to explain all behaviors over which people can exert self-control. The model is based on behavioral intent, whereby behavioral achievement depends on both motivation (intention) and ability (behavioral control). Attitude has proven to be a significant predictor of employee behavioral intentions. In this study, attitude toward security refers to positive or negative evaluations of the security awareness program by an employee. Attitude refers to the degree to which a person has a favorable or unfavorable evaluation of the behavior of interest. This entails consideration of the outcomes of performing the behavior. Based on the above assertions regarding employee attitude toward security and behavioral intentions, the following hypotheses are proposed.

H9: Attitude toward security program positively influences employees' intentions to comply with the security awareness program.

H10: Attitude toward security program positively influences employees' effective use of the security awareness program.

3.5. Compliance Intention

Numerous studies have incorporated the subjective norm (SN) and found that it has a significant effect on intention in mandatory settings, but not in voluntary ones [58, 59]. Venkatesh, Brown, Maruping, and Bala [59] found that the effect of SN on behavioral intention was stronger in a mandatory setting and that SN was a significant determinant of PU. In the context of information security, SN has been identified as a significant predictor of behavioral intention to comply with or use protective security measures [50, 60, 61]. In this study, compliance with the security awareness program refers to the mandatory obligation of employees to adhere to the security requirements of their organization. Behavioral intention refers to the motivational factors that influence a given behavior, where the stronger the intention to perform the behavior, the more likely the behavior will be performed. Based on the above assertions regarding employee compliance with the security awareness program, the following hypotheses are proposed.

H11: Intention to comply with security guidelines positively influences employees' behavior toward effective use of the security awareness program.

4. Method

This research adopted a survey approach for data collection, which was conducted at a bank and a telecommunications company in the DRC. The subjects of the study are individuals employed in the selected organizations. The survey was administered using SurveyMonkey. No restriction was placed on who from the two organizations could take the surveys.

A questionnaire was developed that incorporates nominal and ordinal scales. Nominal scales were mainly used to determine the participants' demographic characteristics, such as age, gender, educational level, and experience. To allow participants to indicate the extent of their agreement or disagreement with specific statements or questions related to their attitudes and beliefs, a 7-point Likert scale was used. This permitted variety in the given answers, as participants in this study share many similarities in terms of their characteristics.

5. Data Analysis

Partial least squares (PLS), as implemented in SmartPLS version 3.0, is used for data analysis [62]. The PLS approach allows researchers to assess measurement model parameters and structural path coefficients simultaneously. This study primarily aims to carry out causal-predictive analysis, and PLS is effective for those early theory testing situations.

5.1. Missing Data

The total number of surveys downloaded from the host server was 715, of which 494 were from the telecommunications company and 221 from the bank. A total of 215 surveys (30.07% of the original 715) were eliminated because they were missing answers to all or nearly all demographic and scale items. Of these, 122 were telecommunications surveys and 43 were bank surveys. This left 500 surveys (322 from telecommunications participants and 178 from banking participants). The 500 remaining participants completed almost all of the demographic questions. However, 30.80% of these participants (n = 154) had skipped one or more scales on the survey. This study compared the demographic information of participants who completed the entire survey with participants who skipped one or more scales. The two groups differed significantly on four of the 10 demographic variables: age, $\chi2(5) = 13.22$, $p = 0.02$; position within the organization, $\chi2(3) = 13.09$, $p < 0.01$; company area in which the participants worked, $\chi2(5) = 11.56$, $p = 0.04$; and organization type (telecom or bank), $\chi2(1) = 12.28$, $p < 0.001$. Those who skipped one or more scales at higher rates than expected were in their 20s or 30s, employed in telecommunications, and worked as staff in the front office. These participants may have skipped sections of the survey for a variety of reasons, such as feeling less invested in the organization and its security, not being informed about the organization's security policy, or believing that security was not significant to their jobs. These and further reasons should be explored in future research, as this is beyond the scope of this research.

5.2. Reliability and Validity Assessment

This study adopted factors from different studies and built relationships between those variables. However, most of the items used to measure the constructs were developed and tested in different studies. Furthermore, some of these items are being studied for the first time in the security domain and in

the DRC context. Therefore, EFA was conducted as an essential first step in data analysis.

Initial assessments were conducted using SmartPLS 3.0. The guidelines of Hair et al. [63] were adopted to assess the factor loadings. Based on the guidelines, six items loaded less than 0.7 on an assigned factor and were deleted. The deletion of these six items had a positive effect on the content validity. Four (4) additional items were removed due to high collinearity. All of the formative indicators have a VIF of less than five, except for one indicator (IN_COLL2) of the cultural effect. This indicator was removed from the model and with it the collinearity problem.

Following the EFA analysis, construct reliability was calculated. Table 6 presents the results, which show that Cronbach's alpha values for all of the constructs in the research model were greater than 0.7, indicating that all constructs had adequate reliability assessment scores. The composite reliability of all of the reflective constructs were above the 0.7 threshold value, which demonstrated high levels of internal consistency reliability for all reflective constructs. Moreover, the AVE values for all reflective constructs were above 0.5, which means that the measure of all reflective constructs has a high level of convergent validity.

The discriminant validity was reviewed using the Fornell–Larcker criterion. The cross loadings were checked for discriminant validity and the square root of the AVE of each construct was found to be higher than the construct's highest correlation with any other construct in the model. Table 2 presents the results; the requirement for the Cronbach's alpha, composite reliability, and discriminant validity were met for each construct.

Table 2 Discriminant Validity

	ATT	IC	EUSA	INQ	MSUPP	PU	PUN	PVA	RE	SE	SP
ATT	0.91										
IC	0.71	0.90									
EUSA	0.33	0.31	0.90								
INQ	0.40	0.39	0.39	0.83							
MSUPP	0.39	0.38	0.45	0.60	0.76						
PU	0.54	0.56	0.23	0.40	0.35	0.84					
PUN	0.17	0.22	0.42	0.36	0.43	0.14	0.75				
PVA	0.54	0.60	0.37	0.52	0.42	0.66	0.27	0.73			
RE	-0.01	-0.13	0.17	0.14	0.16	-0.06	0.32	0.01	0.82		
SE	0.45	0.47	0.25	0.48	0.35	0.56	0.14	0.53	0.05	0.75	
SP	0.27	0.30	0.34	0.33	0.39	0.25	0.34	0.35	0.26	0.19	0.79
Reliability and validity											
Cronbach	0.90	0.93	0.94	0.92	0.90	0.79	0.74	0.82	0.88	0.85	0.79
CR	0.94	0.95	0.95	0.94	0.92	0.88	0.84	0.87	0.91	0.89	0.87
AVE	0.83	0.82	0.81	0.68	0.58	0.70	0.57	0.53	0.67	0.57	0.63

Attitude toward security (ATT), effective use (EUSA), compliance intention (IC), information quality (INQ), management support (MSUPP), punishment (PUN), perceived value (PVA), reward (RE), self-efficacy (SE), social pressure (SP), perceived usefulness (PU)

5.3. Model Testing

Having established that the theoretical model demonstrates adequate validity and reliability, a test of the structural model was conducted. A PLS approach to structural equation modeling was used to estimate the measurement model. Figure 2 shows the results of the model estimation, path coefficients, path significant level based on a two-tailed t-test, and the variance explained by the independent variables (R2). The PLS bootstrapping procedure provides the SRMR criterion, which has a value of less than 0.08; hence, the model meets the goodness of fit criteria.

The relationships between constructs were tested after supporting the validity and reliability of the measurement model. All hypothesized relationships and the moderating cultural effects were tested. Figure 2 presents the result of the model testing.

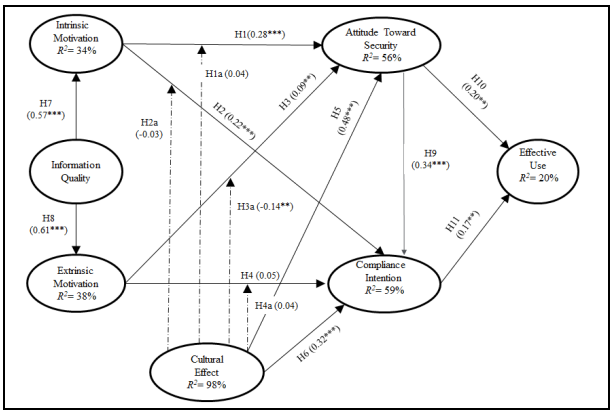

Figure 2 – Path Coefficient Results

Table 3 provides the indirect effects through which each construct and dimension affects the effective use.

Table 3 Indirect Effect

Indirect Effect	β	P value
MA_FE -> EUSA	0.01	0.39
PD -> EUSA	0.02	0.08
EM -> EUSA	0.03	0.03
IN_COLL -> EUSA	0.03	0.01
IM -> EUSA	0.11	0.00
INQ -> EUSA	0.09	0.00
UA -> EUSA	0.15	0.00
CUE -> EUSA	0.18	0.00

6. Discussion of Results

The research question that drove this study was "How do cultural values at the individual level influence the effective use of security awareness in organizations in the DRC?" The study answered this question by examining the effect of culture values on the relationship between employees' intrinsic and extrinsic motivations; the relationship between employees' intrinsic and extrinsic motivations with both attitude toward security and intention to comply with security guidelines; and finally the relationship between information quality, employee attitude, and compliance intention with employees' effective use of security awareness.

The results of this study show that individual culture positively influences the attitude of employees, which then influences their effective use of the security awareness program.

6.1. Cultural Effect

Cultural effects had a positive influence on employees' attitude toward security awareness (H5) and employees' compliance intention (H6). Cultural effects also had a negative moderating effect on the relationship between employees' extrinsic motivation and attitude toward security (H3a). The remaining moderating effect of culture on the various relationships were not significant.

The results in table 3 indicate that out of the four elements constituting cultural effects, only individualism/collectivism and uncertainty avoidance have a positive influence on employees' effective use of the security awareness program. These results imply that for the effective use of security awareness in the Congolese context, organizations must promote these two factors in their security programs. This result can also be seen in the way that participants answered the survey question. 80% of participants agreed that being loyal to the group (collectivism) is more important than individual gain, and 85% agreed that group success is more important than individual success. 94% of participants agreed with the statement "To me, it is important to have information on security requirements and instructions spelled out in detail so that employees always know what they are expected to do (uncertainty avoidance)." On the other hand, only 83% agreed that "To me, managers expect workers to closely follow information security awareness instructions and procedures." It should be troubling to management that almost 20% of employees doubt whether they are expected to follow the information security guidelines.

Four moderating effects were hypothesized in the study. It was found that in the Congolese context, cultural effects negatively influenced the relationship between extrinsic motivation and attitude toward security (H3a). The three remaining moderating effects were not statistically significant. Further investigation is required to determine which of the specific element(s) within cultural effects creates a negative moderating influence in the relationship.

6.2. Information Quality

Information quality had a positive influence on employees' intrinsic motivation (H7) and extrinsic motivation (H8), and an indirect positive effect on effective use of the security awareness program by employees. The participants agreed with all of the items on the information quality scale. However, the survey does reveal that many participants had doubts about the quality of the information on security awareness that they received. One in four were neutral toward or disagreed with the claim that information was clearly presented. Only two thirds agreed that the information on security awareness was up-to-date or personalized to their needs. Moreover, only half of the employees believed that security awareness information was easily accessible.

The results show that INQ positively influences all items of both intrinsic and extrinsic motivation. Its highest influence was on MSUPP, followed by PVA, PU, SE, PUN, SP, and finally RE. This result suggests that in the Congolese context INQ is a very important construct that information security professionals must take into account in order to gain management support; this is essential to guarantee a successful information security program.

6.3. Motivation

Intrinsic motivation had a positive influence on employees' attitude toward security awareness (H1) and compliance intention (H2). Extrinsic motivation had a positive influence on employees' attitude toward security awareness (H3), but it did not have a significant influence on employees' compliance intention (H4). As shown in Table 6, both intrinsic motivation and extrinsic motivation have an indirect positive effect on the effective use of security awareness.

6.3.1. Intrinsic Motivation

Intrinsic motivation—self-efficacy, perceived usefulness, and perceived value—had an positive effect on employees' attitude toward security and their intention to comply. The results in table 3 indicate that intrinsic motivation also has a positive indirect effect on employees' effective use of the security awareness

program. Hence, for employees of an organization to have a favorable attitude toward information security, the intention to comply with security guidelines and effectively use the security awareness program in the Congolese context, the implemented security awareness programs must satisfy employees' need for knowledge about security (perceived value). Furthermore, employees must feel that the programs have perceived usefulness; that is, they must believe that the programs will help them to effectively reduce security threats. Finally, employees must feel that they have the ability to understand and implement the organization's security programs (self-efficacy).

6.3.2. Extrinsic Motivation

Extrinsic motivation - top management support, sanction, reward, and social pressure - had a positive effect on employees' attitude toward security but it did not influence the employees' intention to comply with security awareness guidelines. The results in table 3 indicate that extrinsic motivation also has a positive indirect effect on employees' effective use of the security awareness program. Hence, for employees of an organization to have a favorable attitude toward information security and effectively use the security awareness program in the Congolese context, the implemented security awareness programs must consider management support and level of support as top priority. The result also implies that cybersecurity program manager must not make punishment the main motivator to change attitude neither should they use reward for the same purpose as they both exhibited limited effect on both attitude and intention to comply.

6.4. Attitude Toward Security

Employees' attitude toward security had both a positive influence on their effective use of the security awareness program (H10) and their intention to comply with security guidelines (H9). The vast majority of participants seemed to have a positive attitude toward security. The data shows that over 90% of participants agreed that security awareness was relevant, useful, and necessary. Only 1% did not believe that security awareness was useful, and just 4% did not agree that it was important or necessary. More surprisingly, in response to the statement "To me, the security awareness program is beneficial," none of the participants chose strongly agree or agree. Almost 47% chose slightly agree and 44.80% chose neutral.

Despite the moderately significant relationship between attitude toward security awareness and the effective use of security awareness, the model only explained 20% of the variance in effective use. This could be partly caused by a lukewarm attitude toward security awareness. Therefore, if an organization would like to increase the effective use of its security awareness program, it must begin by working on its employees' attitude toward security. There is a need to shift the attitude from neutral to a more positive one.

6.5. Compliance Intention

Employees' compliance intention had a slightly less influence on employees' effective use of the security awareness program (H11) than attitude toward security. The intention to comply shows a similar pattern to attitude toward security. This result can also be seen in the way that participants answered the survey questions. Like attitude, intent to comply may not be strong. While over 90% of participants agreed with the statements "I intend to protect information resources according to the requirements of the security awareness programs of my organization" and "I intend to carry out my responsibilities prescribed in the security awareness programs of my organization when I use information resources," no one strongly agreed with them. Moreover, no participant chose agree or strongly agree in response to the statement "I intend to comply with the requirements of the security awareness programs of my organization." Only 44.80% chose slightly agree and 47.11% chose neutral. As in the case of attitude, this may be partly attributed to a lukewarm attitude toward security awareness. Therefore, if an organization in the Congolese context would like to increase the effective use of its security awareness program, it must work on its employees' intention to comply with security guidelines by improving INQ, EM and IM.

7. Theoretical and practical Contribution

Given the trend of globalization in business and the sharing of security awareness processes and guidelines, it has become particularly important to understand how local and individual culture influences the effective use of security awareness. While much of the previous literature concentrated on the deterrent effect of sanctions, or incentives to encourage desirable employee behavior, no studies have addressed the problem of employees' effective use of security awareness programs with a focus on the individual cultural dimension.

To our knowledge, this study is the first to develop a model to investigate the influence of employees' culture on the effective use of security awareness programs. This study contributes to behavioral aspects

of the body of knowledge on information security by presenting empirical support that employees' culture, intrinsic motivation, extrinsic motivation, information quality, and attitude toward security awareness programs are important factors to consider in order to predict employees' decisions on the effective use of security awareness program. Collectivism and uncertainty avoidance are positively associated with the effective use of security awareness programs, while masculinity/femininity and power distance did not.

This study presents empirical evidence that employees' intention to comply with security awareness guidelines is not a good predictor of their effective use of a security awareness program. Both intrinsic and extrinsic factors considered in this study are positively associated with the effective use of security awareness programs.

Furthermore, the study confirms that top management support is a positive factor to help increase the effective use of security awareness in the Congolese context. According to the findings, top management must work on increasing employees' intrinsic motivation and attitude in relation to security awareness guidelines and must follow through with both reward and punishment. Finally, organizations should create a culture where each employee makes their peers accountable for following the security awareness program guidelines.

8. Conclusion and Limitations

The objective of the study was to illustrate how cultural values at the individual level of analysis may influence the effective use of a security awareness program, using a proposed model with constructs from TAMs. This study provides a general framework and sets the stage for future research on the effective use of security awareness and the role of culture in information security in general.

Although no statistically significant bias was found for this study, we identify at least two limitations to the research effort. First, the usage measurements were self-reported, which could lead to a bias in reporting; we believe that when people are asked about their security-related behavior, they are unlikely to answer with complete honestly. Second, although the variables in the study explain the variation in effective use, other variables that may also influence effective use, such as computer skills, were left out.

9. References

[1] A. Agrawal, D. Fantham, D. Ghosh, D. Kelley, E. Florio, E. Avena, E. Douglas, F.T. Seng, J. Trull, J. Borenstein, K. Selvaraj, K. Kaplinska, K. Laidler, M. Duncan, M. Simos, P. Henry, P. Pandey, R. Pliskin, R. Mcgee, S. Kathuria, S. Wacker, T. Ganacharya, V. Grebennikov, Y. Zohar, Microsoft Security Intelligence Report, In: M. Corporation (Ed.) Microsoft Security Intelligence Report, Microsoft Corporation, 2019.

[2] I.T.R. Center, 2018 End-Of-Year Data Breach Report, End-Of-Year Data Breach Report, Identity Theft Resource Center, 2018.

[3] K.D. Mitnick, W.L. Simon, The Art Of Deception: Controlling The Human Element Of Security, John Wiley & Sons2011.

[4] K.D. Mitnick, W.L. Simon, The Art Of Intrusion: The Real Stories Behind The Exploits Of Hackers, Intruders And Deceivers, John Wiley & Sons2009.

[5] G. Hofstede, Culture And Organizations, International Studies Of Management & Organization, 10 (1980) 15-41.

[6] D. Straub, M. Keil, W. Brenner, Testing The Technology Acceptance Model Across Cultures: A Three Country Study, Information & Management, 33 (1997) 1-11.

[7] M. Srite, E. Karahanna, The Role Of Espoused National Cultural Values In Technology Acceptance, Mis Quarterly, Doi (2006) 679-704.

[8] R.E. Crossler, A.C. Johnston, P.B. Lowry, Q. Hu, M. Warkentin, R. Baskerville, Future Directions For Behavioral Information Security Research, Computers & Security, 32 (2013) 90-101.

[9] X. Guo, N. Zhang, User Attitude Towards Mandatory Use Of Information Systems: A Chinese Cultural Perspective, International Comparisons Of Information Communication Technologies: Advancing Applications, Igi Global2012, Pp. 1-18.

[10] H.A. Kruger, S. Flowerday, L. Drevin, T. Steyn, An Assessment Of The Role Of Cultural Factors In Information Security Awareness, Information Security South Africa (Issa), 2011, Ieee, 2011, Pp. 1-7.

[11] G. Hofstede, M.F. Peterson, Culture: National Values And Organizational Practices, Handbook Of Organizational Culture And Climate, 3 (2000) 401-416.

[12] R. Davison, M. Martinsons, Guest Editorial Cultural Issues And It Management: Past And Present, Ieee Transactions On Engineering Management, 50 (2003) 3-7.

[13] D.P. Ford, C.E. Connelly, D.B. Meister, Information Systems Research And Hofstede's Culture's Consequences: An Uneasy And Incomplete Partnership, Ieee Transactions On Engineering Management, 50 (2003) 8-25.

[14] M. Gallivan, M. Srite, Information Technology And Culture: Identifying Fragmentary And Holistic

Perspectives Of Culture, Information And Organization, 15 (2005) 295-338.
[15] D.W. Straub, K.D. Loch, C.E. Hill, Transfer Of Information Technology To The Arab World: A Test Of Cultural Influence Modeling, Advanced Topics In Global Information Management, 2 (2003) 141-172.
[16] G. Rose, D. Straub, Predicting General It Use: Applying Tam To The Arabic World, Journal Of Global Information Management (Jgim), 6 (1998) 39-46.
[17] I. Ajzen, M. Fishbein, Understanding Attitudes And Predicting Social Behaviour, Doi (1980).
[18] I. Ajzen, The Theory Of Planned Behavior, Organizational Behavior And Human Decision Processes, 50 (1991) 179-211.
[19] F. Davis, Technology Acceptance Model, York University, Par, 1 (1986).
[20] B. Cooper, J. Wang, T. Bartram, F.L. Cooke, Well-Being-Oriented Human Resource Management Practices And Employee Performance In The Chinese Banking Sector: The Role Of Social Climate And Resilience, Human Resource Management, 58 (2019) 85-97.
[21] A. Turró, D. Urbano, M. Peris-Ortiz, Culture And Innovation: The Moderating Effect Of Cultural Values On Corporate Entrepreneurship, Technological Forecasting And Social Change, 88 (2014) 360-369.
[22] J.J. Kacen, J.A. Lee, The Influence Of Culture On Consumer Impulsive Buying Behavior, Journal Of Consumer Psychology, 12 (2002) 163-176.
[23] T.-F. Kummer, J.M. Leimeister, M. Bick, On The Importance Of National Culture For The Design Of Information Systems, Business & Information Systems Engineering, 4 (2012) 317-330.
[24] S. Jackson, Organizational Culture And Information Systems Adoption: A Three-Perspective Approach, Information And Organization, 21 (2011) 57-83.
[25] V. Venkatesh, X. Zhang, Unified Theory Of Acceptance And Use Of Technology: Us Vs. China, Journal Of Global Information Technology Management, 13 (2010) 5-27.
[26] A. Burton-Jones, C. Grange, From Use To Effective Use: A Representation Theory Perspective, Information Systems Research, 24 (2012) 632-658.
[27] R.-A. Shang, Y.-C. Chen, L. Shen, Extrinsic Versus Intrinsic Motivations For Consumers To Shop On-Line, Information & Management, 42 (2005) 401-413.
[28] T.S. Teo, V.K. Lim, R.Y. Lai, Intrinsic And Extrinsic Motivation In Internet Usage, Omega, 27 (1999) 25-37.
[29] M.H. Fagan, S. Neill, B.R. Wooldridge, Exploring The Intention To Use Computers: An Empirical Investigation Of The Role Of Intrinsic Motivation, Extrinsic Motivation, And Perceived Ease Of Use, Journal Of Computer Information Systems, 48 (2008) 31-37.
[30] J. Grenny, K. Patterson, D. Maxfield, R. Mcmillan, A. Switzler, Influencer: The Power To Change Anything, Mcgraw-Hill Professional2013.
[31] R.M. Ryan, E.L. Deci, Intrinsic And Extrinsic Motivations: Classic Definitions And New Directions, Contemporary Educational Psychology, 25 (2000) 54-67.
[32] E.L. Deci, R.M. Ryan, Intrinsic Motivation, Wiley Online Library1975.
[33] E. Deci, R.M. Ryan, Intrinsic Motivation And Self-Determination In Human Behavior, Springer Science & Business Media1985.
[34] G.W. Bock, Y.-G. Kim, Breaking The Myths Of Rewards: An Exploratory Study Of Attitudes About Knowledge Sharing, Information Resources Management Journal (Irmj), 15 (2002) 14-21.
[35] D. Constant, S. Kiesler, L. Sproull, What's Mine Is Ours, Or Is It? A Study Of Attitudes About Information Sharing, Information Systems Research, 5 (1994) 400-421.
[36] D. Constant, L. Sproull, S. Kiesler, The Kindness Of Strangers: The Usefulness Of Electronic Weak Ties For Technical Advice, Organization Science, 7 (1996) 119-135.
[37] F. Luthans, Positive Organizational Behavior: Developing And Managing Psychological Strengths, The Academy Of Management Executive, 16 (2002) 57-72.
[38] C. Cook, F. Heath, R.L. Thompson, A Meta-Analysis Of Response Rates In Web-Or Internet-Based Surveys, Educational And Psychological Measurement, 60 (2000) 821-836.
[39] H.-W. Kim, A. Kankanhalli, Investigating User Resistance To Information Systems Implementation: A Status Quo Bias Perspective, Mis Quarterly, 33 (2009) 567-582.
[40] H.-W. Kim, H.C. Chan, S. Gupta, Value-Based Adoption Of Mobile Internet: An Empirical Investigation, Decision Support Systems, 43 (2007) 111-126.
[41] S.R. Boss, L.J. Kirsch, I. Angermeier, R.A. Shingler, R.W. Boss, If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, And Information Security, European Journal Of Information Systems, 18 (2009) 151-164.
[42] D.-G. Ko, Antecedents Of Knowledge Transfer From Consultants To Clients In Enterprise System Implementations, Mis Quarterly, 29 (2005) 59-85.
[43] J. Karimi, T.M. Somers, A. Bhattacherjee, The Role Of Information Systems Resources In Erp Capability Building And Business Process Outcomes,

Journal Of Management Information Systems, 24 (2007) 221-260.
[44] B. Bulgurcu, H. Cavusoglu, I. Banbasat, Information Security Policy Compliance: An Empirical Study Of Rationality-Based Beliefs And Information Security Awareness, MIS Quarterly, 34 (2010) 523-A527.
[45] T. Dinev, J. Goo, Q. Hu, K. Nam, User behaviour towards protective information technologies: the role of national cultural differences, Information Systems Journal, 19 (2009) 391-412.
[46] D.F. Larcker, V.P. Lessig, Perceived usefulness of information: A psychometric examination, Decision Sciences, 11 (1980) 121-134.
[47] Y.W. Lee, D.M. Strong, B.K. Kahn, R.Y. Wang, AIMQ: a methodology for information quality assessment, Information & management, 40 (2002) 133-146.
[48] M. Dee Dickerson, J.W. Gentry, Characteristics of adopters and non-adopters of home computers, Journal of Consumer research, 10 (1983) 225-235.
[49] V. Venkatesh, M.G. Morris, G.B. Davis, F.D. Davis, User acceptance of information technology: Toward a unified view, MIS quarterly, DOI (2003) 425-478.
[50] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, MIS quarterly, 34 (2010) 523-548.
[51] T. Herath, H.R. Rao, Protection motivation and deterrence: a framework for security policy compliance in organisations, European Journal of Information Systems, 18 (2009) 106-125.
[52] L. Myyry, M. Siponen, S. Pahnila, T. Vartiainen, A. Vance, What levels of moral reasoning and values explain adherence to information security rules? An empirical study, European Journal of Information Systems, 18 (2009) 126-139.
[53] S. Pahnila, M. Siponen, A. Mahmood, Employees' behavior towards IS security policy compliance, System sciences, 2007. HICSS 2007. 40Th annual hawaii international conference on, IEEE, 2007, pp. 156b-156b.
[54] S. Pahnila, M. Siponen, A. Mahmood, Which factors explain employees' adherence to information security policies? An empirical study, PACIS 2007 Proceedings, DOI (2007) 73.
[55] M. Siponen, M.A. Mahmood, S. Pahnila, Employees' adherence to information security policies: An exploratory field study, Information & management, 51 (2014) 217-224.
[56] F.D. Davis, R.P. Bagozzi, P.R. Warshaw, User acceptance of computer technology: a comparison of two theoretical models, Management science, 35 (1989) 982-1003.
[57] M.K. Chang, Predicting unethical behavior: a comparison of the theory of reasoned action and the theory of planned behavior, Journal of business ethics, 17 (1998) 1825-1834.
[58] J. Hartwick, H. Barki, Explaining the role of user participation in information system use, Management science, 40 (1994) 440-465.
[59] V. Venkatesh, H. Bala, Technology acceptance model 3 and a research agenda on interventions, Decision sciences, 39 (2008) 273-315.
[60] C.L. Anderson, R. Agarwal, Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions, MIS quarterly, 34 (2010) 613-643.
[61] T. Dinev, Q. Hu, The centrality of awareness in the formation of user behavioral intention toward protective information technologies, Journal of the Association for Information Systems, 8 (2007) 386.
[62] C.M. Ringle, S. Wende, J.-M. Becker, SmartPLS 3. Boenningstedt: SmartPLS GmbH, 2015.
[63] J.F. Hair Jr, G.T.M. Hult, C. Ringle, M. Sarstedt, A primer on partial least squares structural equation modeling (PLS-SEM), Sage Publications2016.