HUMAN FACTOR IN CYBER SECURITY: LINK BETWEEN ATTITUDE TOWARDS SECURITY AND INTENTION TO PERFORM SECURITY RELATED BEHAVIOR

Doriane Micaela ANDEME BIKORO
Catholic University of Central Africa
Cameroon
dorianebikoro@gmail.com

Samuel FOSSO WAMBA
Toulouse Business School
France
s.fosso-wamba@tbs.education.fr

Jean Robert KALA KAMDJOUG
Catholic University of Central Africa
Cameroon
jrkala@gmail.com

ABSTRACT

Information systems security has always been oriented towards external threats such as hackers and viruses; this makes organizations open to internal violations. Human factors in the context of information system security have begun to take center stage, especially with failures in security technologies to protect businesses. This paper presents the human factors in cyber security, presenting in particular the link between attitude towards security and intention to perform security related behavior. To effectively contribute to the link between these two fundamental notions, this study is based on the Unified Theory of Acceptance and Utilization of Technology and the Health Belief Model, which highlighted a specific research model. A model that highlights various individual perceptions that influence cyber security practices. To bring this model to life, we used a mixed method of research. The first phase consisted of a quantitative approach that made it possible to administer the research questionnaire in four public and parapublic administrative establishments. And the second phase took place by conducting semi-structured interviews with ten employees from various public and parapublic administrative establishments. The analysis of the data collected was done by the "XLSTAT" software in its 2017 version and "SmartPLS" in its 2015 version for the quantitative component; and a content analysis for the qualitative aspect. These results confirmed the hypotheses resulting from the research model and presented the theoretical and practical implications for this study. The particularity of this work in the field of behavioral aspects of security in the field of research and development.

KEYWORDS

Human behavior, cyber security, attitude, intention, Cameroon.

1 INTRODUCTION

The recent May 13, 2017 computer attacks that rocked many global companies confirmed that the need for cyber security is growing. This is due to the strong reliance of organizations on information and communication technologies (ICTs) (Arabo 2015, de Bruijn and Janssen 2017). Today's society has become a real cyber society that relies on information and communication technologies (ICT) in its day-to-day lives, making the need for cyber security essential (Conklin and White 2006, de Bruijn and Janssen 2017). Information in an organization is always considered one of its most important assets; especially since with the propagation of the Internet, the data exchanged on line growth day by day. This is perfectly in line with Microsoft's projections when it states that by 2020, the number of Internet users will be around 4 billion. This number means an increase of more than 50% compared to the current number (Wheeler 2016, WSJ 2017). The security of this information is thus much more essential; especially since we are in an era where the world is more connected and richer in information (Spears and Barki 2010, Wall, Lowry et al. 2015). This is in agreement with Cyber security Ventures, which guesses worldwide information robbery at around $ 429 million (securityventures 2016, ANDEME BIKORO, KAMDJOUG et al. 2017). Security concerns are ubiquitous because of the ease of access to information (Abubakar, Chiroma et al. 2015, Wall, Lowry et al. 2015). Reason for managing information security has proven to be a key concern for many organizations; this is in the strategic domain (Wheeler 2016, Kolkowska, Karlsson et al. 2017). This is a global aim to secure the information resources of the organization(Spears and Barki 2010, Kolkowska, Karlsson et al. 2017). Because of its military and practicalbirth, information security is often referred to as a set of methods aimed at maintaining security in a computer system (Kolkowska, Karlsson et al. 2017). Outside, in terms of governance of societies, this concept encompasses both the management of practical and theoretical information (Henshel, Cains et al. 2015, Kolkowska,

Karlsson et al. 2017). The human factor in information security has been particularly highlighted when the use of asset securing technologies has failed to protect organizations from cyber attacks(Henshel, Cains et al. 2015, Evans, Maglaras et al. 2016). For instance, the Global inspection on Information Security 2015 (securityventures 2016)showed that employees account for 35% of all business-related security breaches (Kolkowska, Karlsson et al. 2017). Recent estimates show that at least half of Information systems are more linked to the human aspect than to the technical aspect(Spears and Barki 2010). These estimates support the usual beliefs that structural efforts to manage the security of information systems are based on technological vulnerabilities encompassing the technical side to the detriment of other sources of vulnerability that take into account people, policies, processes and culture (Spears and Barki 2010). Recent surveys thus support our above-mentioned comments according to which employees are still the main perpetrators of corporate security incidents (Shamala, Ahmad et al. 2015). And especially those internal crimes be likely to cost firms more than those committed by external sources (Warkentin, Johnston et al. 2016). This is why researchers are increasingly recognizing the crucial role played by users in the security of the information system (Vance, Anderson et al. 2014). Because if a user poses an act of insecurity, it is the security of the whole system that can be compromised (Vance, Anderson et al. 2014). And this status of weak link in the security chain is not unknown to hackers and cybercriminals. This is why these hackers usually use many social tricks to encourage users to install malware or avoid technical security checks(Vance, Anderson et al. 2014, Warkentin, Johnston et al. 2016). Cyber security is therefore needed for all entities, encompassing public and privatesocieties, but the insurance of security is often difficult (de Bruijn and Janssen 2017). Hence the need to address the human factor in cyber security.

Cyber security is apprehended by many scientists as the new form of war; because in today's world is identified with a place of continuous battle between hackers and the various actors of the security of information systems to protect systems (de Bruijn and Janssen 2017). Cyber security is therefore a tough socio-technical challenge for governments, requiring the involvement of all. It can be understood as "*the ability to defend cyberspace from online attacks that may stunt, stop, reverse or examine the digital environment in an acceptable manner".*We define it as a set of regulatory, human and technical measures put in place to secure online information circulating in a given environment.

The context of Cameroon is no exception. Indeed, the National Agency of Financial Investigation in 2014 expresses many indictments including 63% find their sources in cybercriminal activities(ANDEME BIKORO, KAMDJOUG et al. 2017). The following year 2015, will be the year of all records alarming because the Cameroonian public cash will lose about 4 billion of CFA; about 7 million euros. This always because of cybercriminal activities (cameroon-info 2016). The audit of 74 locals companies will only confirm this major problem of cybercrime. Indeed, it reveals that approximately 8594 vulnerability indices were found in these organizations(Cameroun 2016). These security issues also call into question the effectiveness of technologies used to secure national assets; the question should therefore be asked of the role of the human factor in the data protection process, particularly in cyber security in Cameroon.

The main difference between the related work and the proposed work is that this study in addition to taking into account the behavioral or even human factors that influences the relationship between attitude towards security and intention to perform security related behavior. This study comes to innovate by basing itself in case of developing countries.

2 PREVIOUS RESEARCHES

Some previous research on cyber security shows that:

The impact of the human factor in cyber security is a current concern as stated (Evans, Maglaras et al. 2016). In addition, the behavior of individuals is presented as an insurance factor in cyber security. This is why the results of this work will make it possible to assess the reliability of human beings in established industrial sectors. This will facilitate the development of a framework of good practices on human aspects in cyber security (Evans, Maglaras et al. 2016).

In order to develop a holistic and predictive model that will assess the risks of cyber security, it is necessary to highlight human factors in order to perceive the impact on cyber security of the actions of users, advocates and attackers (Henshel, Cains et al. 2015). This requires trust, which is an important factor conditioning a person's role in an online system. This article focuses on trust by presenting its link with the internal and external character traits of

individuals interacting with the information system (Henshel, Cains et al. 2015).

In this paper (Anderson and Agarwal 2010), he conducts two studies that allow him to understand the behavioral intentions related to security and the factors that have a positive influence on these intentions. For this, he will use the concept of careful cybernetic people which refers to "individuals who are motivated to take the necessary precautions under their direct control to secure their own computer in a family setting."(Anderson and Agarwal 2010).

This article examines the contribution of users in the risk management process related to the security of information systems (Spears and Barki 2010). A mixed analysis has also been done here; starting with the qualitative component to assess the compliance of security controls with the Sarbanes-Oxley Act. Following this, a questionnaire was administered. This work made it possible to underline that the participation of the users makes it possible to improve the performances in the matter of security control thanks to the sensitization, the alignment between the management of the security risks and the business environment finally the development of the control (Spears and Barki 2010).

This paper of (ANDEME BIKORO, KAMDJOUG et al. 2017), studies the contribution of cyber security to the electronic protection of data in Cameroon. Indeed, it traces the outlines of an association between individual perceptions and attitudes towards security. Theconclusions of this paper present cyber security as a favorable outcome in terms of electronicdata protection in Cameroon through the analysis of certain behaviors.

3 CONCEPTUAL FRAMEWORKS

The conceptual framework of this study offerings in turn the theories in terms of information system that have been used in this article and the research model specific to this work. It must be emphasized here that we used Unified Theory of Acceptance and Use of Technology (UTAUT) by (Venkatesh. 2014) and Health Belief Model (HBM) by (Rosenstock 1974). The mixture of these two theories made it possible to draw the following constructs:

3.1 Core construct

Perceived vulnerability (PV): it represents the feeling that an individual has damage that can cause him an online attack (Claar 2011).

H1: The perception of the vulnerability of an online attack is positively linked to the attitude towards security.

Perceived benefits (PBe): refer to the benefits perceived by individuals in adopting safety attitudes (Claar 2011).

H2: Perceived benefits considerably influenced attitude towards security.

Perceived gravity (PGr): ells represent an individual's feeling about the impact of a computer crash (Claar 2011).

H3a: Perceived gravity is considerablylinked to the attitude toward security.

H3b: Perceived gravity is considerablyinfluenced intention to perform security related behavior.

Attitude towards security (ATS): Is the trust in the Importance of cyber security (Anderson and Agarwal 2010).

H4: Attitude Toward Security is positively linked to intention to perform security related behavior.

Intention to Perform Security Related Behavior (IPS): refers to the wish to accomplish cyber security acts(Anderson and Agarwal 2010).

3.2 Moderator construct

These are demographic variables that considerablyregulates individuals perceptions of security and by extension of cyber security (Claar 2011, Venkatesh. 2014).

Age

H6a: Age considerablyregulates the link between attitude towards security and intention to perform security related behavior.

H6b: Age considerably regulates the link between perceived gravity and intention to perform security related behavior.

Gender

H7a: Gender considerably regulates the link between attitude towards security and intention to perform security related behavior.

H7b: Gender considerably regulates the link between perceived gravity and intention to perform security related behavior.

Hence the development of the model below:

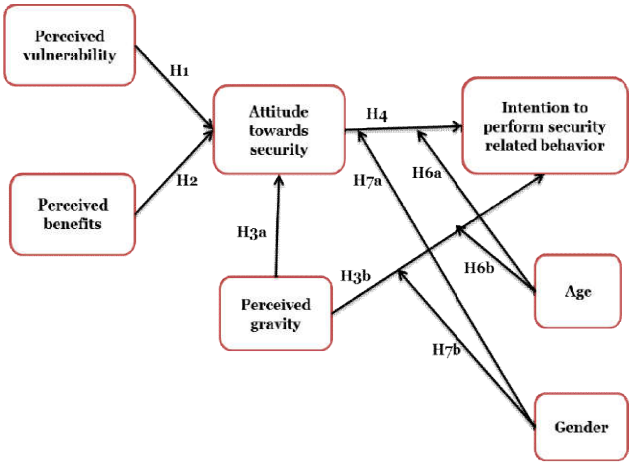

Figure 1 :**Research Model**

4 METHODOLOGY

We used a scientific approach based on a mixed research method that allows us to judge both the quality and quantity of information (Venkatesh, Brown et al. 2013) . This approach is divided into two main parts as follows:

4.1 Quantitative Analysis

This first step started with the pre-test phase. In fact, this phase was carried out with 47 different master's students (Information Systems, Banking and Finance, Accounting and Finance and Audit and Management Control) of the Catholic University of Central Africa. On average it was realized in two weeks. After this phase, we proceeded to the pilot phase which was carried out with 6 students from the various levels of studies mentioned above. It is the concatenation of these two stages that allowed us to design the final questionnaire that was administered to the employees of four publics and parapublicsadministratives establishments. Our population is 150 respondents. The final phase of administering the final research questionnaire took us on average three months. the analysis of the collected data was made by the software "XLSTAT" 2017 and "SmartPLS" 2015 (Wold 1985).

4.2 Qualitative Analysis

It was the last step of the data collection. In fact, it has been carried out among ten government officials working in certain public and parapublic administration. The average time for each interview was thirty minutes and this stage lasted a week. The analysis of the collected data was done by a content analysis.

5 RESULTS

In terms of the results provided by the software "XLSTAT" 2017, "SmartPLS" 2015 and the analysis of the content, we carried out several tests among others:

Reliability test

Table1: **Reliability Test**

Latent variable	Manifest variables	Loadings ≥0.6	Alpha Cronbach ≥0.7	Rho ≥0.7	(AVE) ≥0.5
PV	PV1	0.863	0.827	0.888	0.662
	PV2	0.862			
	PV3	0.842			
	PV4	0.7			
PBe	PBe1	0.950	0.702	0.835	0.543
	PBe2	0.7			
	PBe3	0.6			
PGr	PGr1	0.777	0.784	0.861	0.606
	PGr2	0.850			
	PGr3	0.7			
	PGr4	0.787			
ATS	ATS1	0.939	0.961	0.969	0.839
	ATS2	0.910			
	ATS3	0.895			
	ATS4	0.932			
	ATS5	0.910			
	ATS6	0.909			
IPS	IPS1	0.989	0.977	0.988	0.977
	IPS2	0.988			

Discriminant validity

Tableau 2: **Discriminant Test**

	PV	PBe	PGr	ATS	IPS
PV	0.813				
PBe	0.054	0.736			
PGr	0.655	0.126	0.778		
ATS	0.363	0.180	0.285	0.915	
IPS	0.391	0.014	0.344	0.230	0.988

GoF

Gof Heard by Goodness of Fit, this is an indicator to measure the overall fit of our research model. The literature sets its acceptability threshold at 0.8 in relative value (Wold 1985). So we have the table below:

Tableau 3: **Goodness of Fit**

	GoF	GoF (Bootstrap)
Relative value	0.862	0.864

Final Model with path coefficient and contribution index

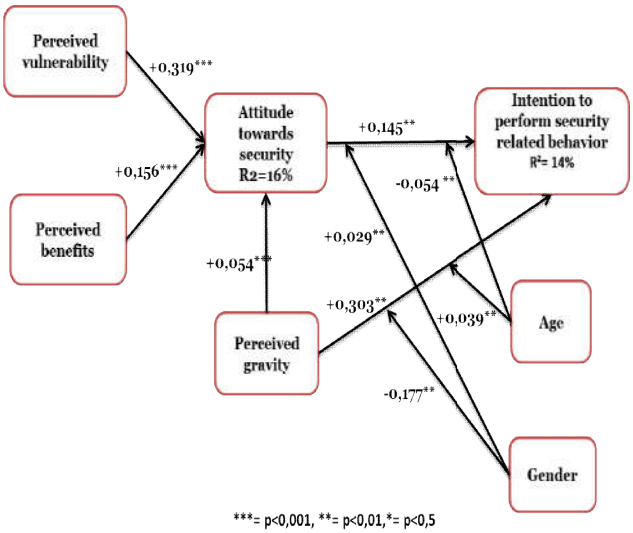

Figure 2: **Final Model**

6 DISCUSSION

In this part of the article, we present the managerial and practical implications of these results. Without forgetting to present the contribution.

6.1 Managerial Implications

The work that has been done has yielded largely acceptable results in terms of the different indicators presented. Perceived vulnerability proves to be the most influential construct in the relationship between attitude towards security and performance to perform security related behavior with a path coefficient of 0.319 and a strong three-star contribution. The perceived benefits and the perceived severity with respectively 0.156 and 0.054 also contributes significantly to the formation of the link between our two flagship builds. It must be emphasized here that perceived seriousness strongly contributes to the desire to perform a cyber security act.

As a result, this work has many managerial implications, particularly for the public authorities.

First, it shows that the Cameroonian government should better educate its employees on the vulnerabilities of cyber attacks. Indeed, the results showed that perceived vulnerability is the perception that has the most influence on the relationship between attitude towards security and intention to perform security related behavior.

Second, it would be wise to share experiences of local businesses that have already been attacked. This would raise a collective awareness. Because the results have also shown that impact.

Finally, it would be important for the State of Cameroon to improve the skills of its employees on data protection measures in general and cyber security in particular.

6.2 Theoretical implications

The results of this work consolidate the link between attitude towards security and intention to perform security related behavior. Indeed, in agreement with the literature, there is a strong link between these two constructs in terms of adopting a technology and its use. These results also reveal that attitude towards security strongly contributes to the formation of intention to perform security related behavior.

We should not forget the influence of the moderating effects in this model; influence that proved significant. In fact, with regard to sign variations, it appears that perceptions differ according to sex and age. This work thus lays the foundation for an association between various individual perceptions (borrowed from the Health Belief Model) and constructs borrowed from the Unified Theory of Acceptance and Use of Technology.

7 LIMITS AND PERSPECTIVES

As all productions of the mind, this work has limits among others the delimitation of the geographical perimeter in a single city and the sampling by voluntary participation.Another limit is the size of our sample which is not representative enough but still acceptable. It should also be noted that studying the behavioral factors of individuals is somewhat theoretical and difficult for all to understand.

Many perspectives emerge from this work in particular: A greater valorization of the qualitative aspect, to increase the size of the sample for more representatively and to test this model for private companies.Another perspective would be the study of the post-adoption and post-use effects of this technology, always considering the human factor as influencing the links between attitude towards security and intention to perform security related behavior. This therefore refers to an assessment of the adoption and use of this technology.

REFERENCES

Abubakar, A. I., et al. (2015). "A review of the advances in cyber security benchmark datasets for evaluating data-driven based intrusion detection systems." Procedia Computer Science**62**: 221-227.

ANDEME BIKORO, D. M., et al. (2017). "Contribution of Cybersecurity to Electronic Data Protection in Cameroon."

Anderson, C. L. and R. Agarwal (2010). "Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions." Mis Quarterly**34**(3): 613-643.

Arabo, A. (2015). "Cyber security challenges within the connected home ecosystem futures." Procedia Computer Science**61**: 227-232.

cameroon-info (2016). "Cameroun - cybercriminalité: Les Etats-Unis proposent leur expertise au Cameroun." Retrieved September, 11, 2016, fromhttps://www.237online.com/article-30977-cameroun--cybercriminalit-eacute--les-etats-unis-proposent-leur-expertise-au-cameroun.html.

Cameroun, I. a. (2016). "La cybercriminalite, une problematique majeure pour le Cameroun." INVESTIR AU CAMEROUN. Retrieved September,07, 2016, from http://www.investiraucameroun.com/securite/0709-7867-la-cybercriminalite-une-problematique-majeure-pour-le-cameroun.

Claar, C. L. (2011). The adoption of computer security: an analysis of home personal computer user behavior using the health belief model, Utah State University.

Conklin, A. and G. B. White (2006). E-government and cyber security: the role of cyber security exercises. System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on, IEEE.

de Bruijn, H. and M. Janssen (2017). "Building Cybersecurity Awareness: The need for evidence-based framing strategies." Government Information Quarterly**34**(1): 1-7.

Evans, M., et al. (2016). "Human behaviour as an aspect of cybersecurity assurance." Security and Communication Networks**9**(17): 4667-4679.

Henshel, D., et al. (2015). "Trust as a human factor in holistic cyber security risk assessment." Procedia Manufacturing**3**: 1117-1124.

Kolkowska, E., et al. (2017). "Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method." The Journal of Strategic Information Systems**26**(1): 39-57.

Rosenstock, I. M. (1974). "Historical origins of the Health Belief Model. ." Health Education Monographs**2(4)**: 328-335.

securityventures, C. (2016). "Ransomware attacks are surging.". Retrieved November,2, 2017, from http://cyber securityventures.com/hackerpocalypse-cybercrime-report-2016/.

Shamala, P., et al. (2015). "Collective information structure model for Information Security Risk Assessment (ISRA)." Journal of Systems and Information Technology**17**(2): 193-219.

Spears, J. L. and H. Barki (2010). "User participation in information systems security risk management." MIS quarterly: 503-522.

Vance, A., et al. (2014). "Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG)." Journal of the Association for Information Systems**15**(10): 679.

Venkatesh, V., et al. (2013). "Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems." MIS quarterly**37**(1): 21-54.

Venkatesh., V. (2014). "Unified Theory of Acceptance and Use of Technology: U.S. Vs. China." Retrieved 2 november, 2016, from http://www.tandfonline.com/doi/abs/10.1080/1097198X.2010.10856507.

Wall, J. D., et al. (2015). "Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess."

Warkentin, M., et al. (2016). "Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination." Journal of the Association for Information Systems**17**(3): 194.

Wheeler, J. A. (2016). "Emerging Risks in Cyber security: Gartner's Top Ten Predictions." Retrieved November,9, 2017, from from http://blogs.gartner.com/john-wheeler/gartner-top-ten-cyber security-predicts/.

Wold, H. (1985). "Partial least squares." Encyclopedia of statistical sciences.

WSJ (2017). "Dow Jones Inadvertently Exposed Some Customers' Information." Retrieved November,9, 2017, from https://www.wsj.com/articles/dow-jones-inadvertently-exposed-some-customers-information-1500237742.