Determinants of Cyber Security Use and Behavioral Intention: Case of the Cameroonian Public Administration

Doriane Micaela Andeme Bikoro[1], Samuel Fosso Wamba[2(✉)], and Jean Robert Kala Kamdjoug[1]

[1] GRIAGES, Catholic University of Central Africa, Yaoundé, Cameroon
dorianebikoro@gmail.com, jrkala@gmail.com
[2] Toulouse Business School, Toulouse, France
s.fosso-wamba@tbs-education.fr

Abstract. The development of information and communication technologies has brought in its wake the upsurge of cybercrime and has raised the need to take cyber security measures at all levels. One of them consists in placing the human being at the center of computer security, notably by studying the individual perceptions behind the desire to perform acts of security, including cyber security. This research work actually aims to use a mixed method to determine the rationale behind the intention of Cameroonian authorities to adopt and implement cyber security measures. The theoretical underpinnings of this research were posed by the Unified Theory of Acceptance and Use of Technology and the Health Belief Model.

Keywords: Cyber security · Behavior · UTAUT · HBM · Cameroon

1 Introduction

The use of information and communication technologies has spanned virtually all spheres of activity; in both the private and public sectors, exalting the competitive advantages, technological development and the popularization of the Internet (Fielder et al. 2016; Hughes et al. 2017). As a result of such expansion, there has been an astonishing increase in the amount of information circulating online today (Henshel et al. 2015; Savulescu 2015); which justifies the significant online migration that is being observed on a daily basis (Choejey et al. 2015). Given the momentum of the Internet and related tools, the giant of information and communication technologies, Microsoft indicated that by 2020, nearly 4 billion Internet users will be recorded globally, accounting for more than 50% of the current statistics (Wheeler 2016; WSJ 2017). As the mass of information circulating is increasing exponentially, this represents an appropriate avenue for cybercriminals and helps developing cybercrime around the world. Microsoft further points out that cybercrime generate financial losses estimated at about 300 billion dollars (MarketWatch 2016, Wheeler 2016; WSJ 2017). The company Cyber security Ventures, on its part, indicates that the value of information stolen globally as

Á. Rocha et al. (Eds.): WorldCIST'18 2018, AISC 746, pp. 1087–1096, 2018.
https://doi.org/10.1007/978-3-319-77712-2_104

a result of cybercrime practices is estimated at about 429 million dollars. And according to financial results for the first quarter of 2017 of ThreatMetrix, nearly 130 million attacks were detected and thwarted in the world (ThreatMetrix 2017). Regarding specifically Cameroon, it appears that nearly 63% of indictments filed by the National Agency for Financial Investigation (NAFI) were related to cybercrime in 2014 (Cameroon-info 2016; Cameroun 2016). In addition, the Cameroonian Treasury recorded significant financial losses (about 7 million in dollars) in 2015 as a result of cybercrime (Cameroon-info 2016). Furthermore, the National Agency for Information and Communication Technologies (NAICT) detected in 2016 about 8594 indices of vulnerabilities following investigations in 74 public and private Cameroonian organizations (Cameroon-info 2016). Cameroon is therefore an attractive place for cybercriminals, and it would be interesting to study the determinants of cyber security use in this country. For the purpose of this study, we have limited our scope to public administration.

Cyber security can be perceived as the digital protection of intellectual and commercial property against excessive use and/or unauthorized authorship (Kaplan et al. 2011; Andeme bikoro et al. 2017). Fighting against cybercrime is a delicate, costly mission. In this regard, Ventures argues that between 2017 and 2021, the overall cost of creating a reliable cyber security arsenal will cost about $ 1 billion (Steve Morgan 2016; Wheeler 2016).

The particularity of this work is that it takes into account both behavioral aspects such as individual perceptions as well as structural and demographic aspects. This, to explain the determinants behavioral intentions and the use of cyber security in a context of developing countries contrary to what already exists in the literature. This permits us to put together elements of UTAUT and HBM to emerge an explicit framework to delimit individual perceptions influencing in turn the desire and use of cyber security.

After introducing our remarks, we will throughout this work, present in turn a literature review to discuss what has already been done in previous studies. Next, the presentation of the conceptual framework will follow with the two theories used in this paper. Study (UTAUT and HBM); the explanation of different constructs that we took in these theories to build our research model. The methodology of this study will be presented in the fourth part, in which the main steps of data collection of this work are presented. These data have been the subject of a rigorous analysis by software such as XLSTAT, Smart PLS. Furthermore the results of this analysis are detailed in part 5. The final lines of this work represent the discussion of the results and the presentation of the limits and contribution.

2 Summary of Literature Review

The literature on cyber security is rich enough in both terms quantitative and qualitative terms.

In his article on factors influencing decision-making to invest in cyber security, (Fielder et al. 2016) argued that the cost of implementation and the impact of this new solution on the company's business fundamentally underpin any investment in cyber security. In other words, these two support factors should be considered in the selection

of the set of cyber security control tools that can maximize the chances of effective curbing cyber-attacks.

When developing a holistic and predictive cyber security risk assessment model, human factors such as the human behavior are needed to understand how the actions of cyber users, defenders and attackers can affect cyber security (Henshel et al. 2015). Trust has proven to be a crucial element affecting a person's role in an online system. In particular, this article focuses on the notion of trust, showing its links to the inherent and external characteristics of humans interacting with computer networks (Abubakar et al. 2015; Henshel et al. 2015).

On the other hand, there are studies focusing on the phenomenon of conscientious cybernetic citizens. There are "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; Arabo 2015). Other studies have been conducted to understand factors determining the intention to perform safety-related behaviors and interventions that can positively influence these factors (Anderson and Agarwal 2010).

Furthermore, studies such as those by (Drew 2012) analyze the threats, vulnerabilities and risks associated with computer networks in order to provide appropriate measures to secure the valuable assets of an organization. Some of them also discuss the role of cyber security in e-governance. With the rapid growth of information technology, organizations are taking extra precautions to protect their information. The scope of online governance control and its impact in a community defines a system that is more than just a sum of simple systems (Conklin and White 2006; Drew 2012). To test security issues across the system, a new method of analysis is needed, resulting in a community cyber security exercise.

As for (Andeme bikoro et al. 2017), they present a set of global perceptions that influence the adoption of security attitudes, and by extension, cyber security practices. Such contribution is much more directed at the protection of electronic data in the Cameroon context.

3 Conceptual Framework

In this section, we present our research model with its hypotheses. It should be noted here that this model is inspired by both the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al. 2003; Turan et al. 2015) and the Health Belief Model (HBM) (Rosenstock 1974). Indeed, we borrow from UTAUT various behavioral factors such as intention to perform security related behavior and utilization; this to highlight the determinants that influence this lighthouse construct of our research model. The literature on UTAUT has clearly laid the foundation for this behavioral theory of acceptance and use of new technology(Venkatesh and Davis 2000; Venkatesh et al. 2003). At HBM, we extracted some individual perceptions such as perceived vulnerability, perceived barriers and cues to action. These will be tested on intention to perform security related behavior to highlight the connection between these constructs. So lay down new foundations in the theory. We therefore have the following:

3.1 Core Constructs

Perceived vulnerability (PV) is the perception by individuals of a damage that can cause a computer attack (Claar 2011). It's about doing behavioral acts to lower the risk. It is obvious that when an individual believes that he can be reached, it will be more likely to find a solution to avoid this (Janz and Becker 1984).

H1: Perceiving vulnerability to an incident is positively related to the intention to achieve security-related behavior.

Perceived benefits (PBe) are advantages for individuals to use a new technology (Claar 2011). In other words, it is the vision an individual has about the utility of a new behavior in order to reduce the risk of being attacked (Rosenstock et al. 1988).

H2: Perceived benefits are strongly related to the intention to achieve security-related behavior.

Cues to action (CuA) are external events that cause people to do certain things (Graham 2002). These are the experiences outside of you that can push you to use technology (Janz and Becker 1984; Rosenstock et al. 1988).

H3: Cues to action are positively related to the intention to achieve security- related behavior.

Intention to perform security-related behavior (IPS) is the desire aroused in an individual to perform an act (Anderson and Agarwal 2010; Andeme bikoro et al. 2017). Desire generally caused by perceptions of the individual which will push to pose acts related to the behavior.

H4: The intention to achieve safety-related behavior is positively related to the use of safety.

Computer security usage (CSU) is the intention to adopt computer security (Kim et al. 2016; Andeme bikoro et al. 2017).

3.2 Moderator Constructs

They refer to socio-demographic factors influencing individual perceptions (Damanpour 1991).

Age

H5: Age significantly moderates the relationship between the intention and security-related behavior realization and utilization.

Gender

H6: Gender significantly moderates the relationship between the intention and security-related behavior realization and utilization.

All this results in the model below (Fig. 1):

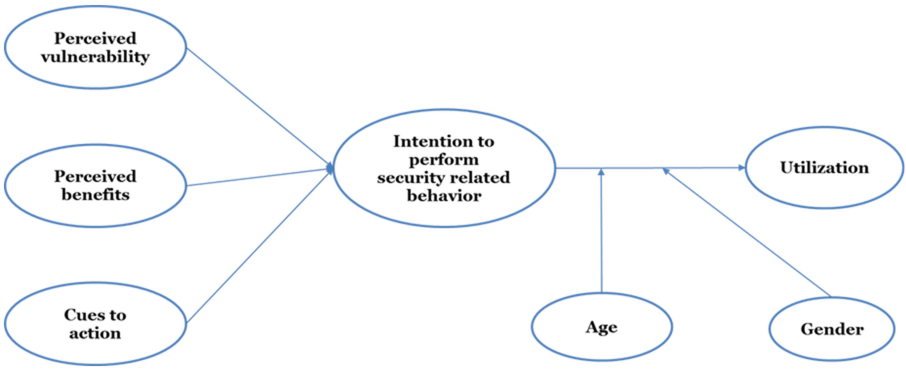

Fig. 1. Research model

4 Methodology

The mixed method has been used here, as it can be used in a qualitative or qualitative way (Jick 1979; Venkatesh et al.2013). It consisted in administering a questionnaire to 4 public and para public establishments, and in interviewing 10 government officials. In terms of quantitative methodology, a hypothetico-deductive approach was applied at an earlier stage to enable a pre-test phase with 6 various Master's students from the Catholic University Central Africa. After the pre-test, the pilot phase was conducted with 47 students from the same university. The questionnaire was finally administered based on the results obtained during these two phases. We distributed 260 copies in French and 37 copies in English. We eventually received 150 returned questionnaire forms (137 in French and 13 in English) which came from State agents serving in various public administrative establishments, within a period of 3 months. We opted for a voluntary sampling. For the analysis of these statistical data, the software applications XLSTAT 2017 and SmartPLS 2015 were used (Henseler et al. 2009). Regarding the semi-structured interviews that were conducted, they lasted on average 30 min and the operation took more than a week; the data collected were processed by simple content analysis.

5 Results

We have obtained a predominantly young population whose age range is between 25–40 years, a highly educated population whose level of education is at the Master. This predominantly male population is 73% male compared to 27% female.

As mentioned above, we used the statistical tools XLSTAT 2017 and SmartPLS 2015 to process and analyze the data collected. The reliability test gave the following results (Table 1):

Table 1. Test of reliability

	Cronbach's Alpha	rho_A	Composite reliability	Average Variance Extracted (AVE)
CSU	0.826	0.951	0.916	0.845
CuA	0.7	0.773	0.794	0.574
IPS	0.977	0.977	0.988	0.977
PBe	0.717	0.736	0.819	0.603
PV	0.830	0.841	0.888	0.666

Regarding the discriminant validity, the table below describes the results (Table 2):

Table 2. Discriminant validity

	CSU	CuA	IPS	PBe	PV
CSU	**0.919**				
CuA	0.159	**0.758**			
IPS	0.229	0.266	**0.989**		
PBe	−0.038	0.040	0.143	**0.777**	
PV	0.181	0.058	0.452	0.115	**0.816**

The Goodness of Fit (GoF), which is an overall indicator of the model's appropriateness, testifies to the quality of the author's model as follows: 0.8 in relative value (Tenenhaus et al. 2005; Henseler et al. 2009), which is the threshold of acceptability set forth by theoreticians for this kind of model (Table 3).

Table 3. Goodness of Fit

	GoF	GoF bootstrap
Relative value	0.862	0.869

The results obtained clearly indicate that the various reliability indicators, particularly the Cronbach's Alpha of this model, are good because they are greater than or equal to 0.7. In the same light, the table of the discriminant validity shows a perfect correlation between the constructs of our model, thereby corroborating results from the Goodness-of-Fit indicator. In short, we have the model appearing below, which describes the path coefficients and the degree of its significance (see stars) (Fig. 2).

6 Discussion

In substitution to the desire to perform an act of security, including of cyber security, the intention to achieve security-related behavior positively influences the use of cyber

security measures. This is justified by three perceptions, namely perceived vulnerability, perceived barriers and cues to action.

Perceived vulnerability is the most frequent perception among employees who desire to take security actions, as it has a coefficient of 0.429. Indeed, the single perception that a system may be corrupted by a virus or by a computer worm causes the employee a strong desire to take a computer security measure. Therefore, perceived vulnerability strongly influences the intention to achieve security related behavior. It is perception that influences individuals in these jurisdictions to adopt cyber security attitudes. Indeed, it shows that perceived vulnerability is very strongly related to intent to perform security related behavior. The desire to use cyber security is stronger when individuals are aware of the vulnerabilities they face in terms of data loss, information theft and forgery of data. Perceived vulnerability is therefore presented as the strong link in the chain of determinants of behavioral factors that influence intention to perform security related behavior and utilization. This highlights the need for global awareness on this issue and on improving the skills of public sector employees on cyber security issues.

Cues to action, with a path coefficient of 0.224, shows that some external sources of information are able to elicit from these employees the desire to take security acts, which may include TV broadcasting and share of experiences by loved ones or even alerts from manufacturers of digital devices. Therefore, cues to action also strongly influence the intention to achieve security-related behavior. In literature, it is a perception that weakly influences the health belief model. But in our research, this construct also presents itself as a strong link in the prediction of the use of cyber security in case of developing countries. This shows that the experiences of others in the use of cyber security are an essential asset. Because this research has demonstrated that the desire to use cyber security is strongly accentuated in an individual who is aware of the harms that happen to third parties who have not taken cyber security measures. In the same way, good public awareness is needed and especially it would be wise for this government to present as examples cases of public sector companies that have already been subjected to cyber attacks. In addition to talking about the losses they have recorded.

Perceived benefits do not strongly influence individuals to perform security acts. This means that neither the cost nor the time is major obstacles for individuals to resort

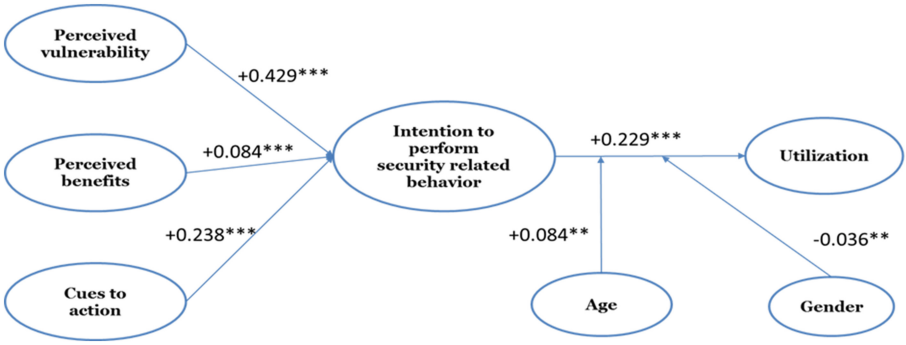

Fig. 2. Research model with path coefficient (***= $p < 0.001$,**= $p < 0.01$,*= $p < 0.5$)

to cyber security. As a result, the perceived benefits influence significantly the intention to achieve security related behavior.

The relationship between the intention to realize security-related behavior and the use of cyber security is therefore strengthened. Evidence to this are the values of the various indicators, which show that the desire aroused in individuals to perform cyber security acts pushes them to rely on cyber security measures.

In terms of demographic factors, we have: Regarding age, young people are those who are better able to move from intention to the effective use of cyber security; unlike the elderly; this shows that in these public administrations, it would be wise not to use an aging staff. Regarding gender, the use of cyber security is more driven by intention to perform security related behavior among women at the expense of men as indicated by the sign of the value −0.036.

In sum, in the Cameroonian public administration, young people are more concerned about the inconveniences that could result from the non-use of cyber security measures. It is this perception that strongly supports the relationship between intention to perform security related behavior and utilization. This shows that the rise of cybercrime is a fact that will push these companies to take cyber security measures.

As mentioned above, the main recommendation to formulate for the Cameroonian state would be to sensitize the civil servants and state agents on the venerability of unprotected systems as well as on the importance of safeguarding immaterial assets. One of the best ways to achieve this could be through reporting and disseminating the experiences of Cameroon-based companies and organizations that have already faced cyber-attacks and have succeeded in curbing them efficiently. It is also important to popularize what is being done by those entities to improve their arsenal for cyber security issues.

7 Limits and Contribution

The main contribution of this study stands at the theoretical level. In a context characterized by the paucity of the relevant literature on information systems and related issues such as cyber security; it is obvious that the compass of our study on this topic is some how narrowed. That not withstanding, this research work will hopefully throw off the shackles of impassiveness among the public authorities of Cameroon and of some other countries, for them to definitely ponder on cyber security. In practical terms, this study gives rise to a better understanding of the rationale behind individuals taking cyber security actions.

In addition, this study makes it possible to lay the theoretical foundations for the relationships between individual perceptions such as perceived vulnerability, perceived benefits, cues to action and intention to perform security related behavior and the use of cyber security.

This confirms the fact that many cyber attacks are increasingly an uncomfortable situation for individuals hence the desire to take cyber security measures (Wheeler 2016).

References

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

Andeme bikoro, D.M., et al.: Contribution of cybersecurity to electronic data protection in Cameroon (2017)

Anderson, C.L., Agarwal, R.: Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. MIS Q. **34**(3), 613–643 (2010)

Arabo, A.: Cyber security challenges within the connected home ecosystem futures. Procedia Comput. Sci. **61**, 227–232 (2015)

Cameroon-info: Cameroun - cybercriminalité: Les Etats-Unis proposent leur expertise au Cameroun (2016). https://www.237online.com/article-30977-cameroun–cybercriminalit-eacute–les-etats-unis-proposent-leur-expertise-au-cameroun.html. Accessed 5 Nov 2017

Cameroun, I.A.: La cybercriminalite, une problematique majeure pour le Cameroun (2016). http://www.investiraucameroun.com/securite/0709-7867-la-cybercriminalite-une-problematique-majeure-pour-le-cameroun. Accessed 29 Oct 2017

Choejey, P., et al.: Cybersecurity practices for e-Government: an assessment in Bhutan. In: The 10th International Conference on e-Business, Bangkok, Thailand (2015)

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

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

Damanpour, F.: Organizational innovation: a meta-analysis of effects of determinants and moderators. Acad. Manag. J. **34**(3), 555–590 (1991)

Drew, J.: Managing cybersecurity risks. J. Account. **214**(2), 44 (2012)

Fielder, A., et al.: Decision support approaches for cyber security investment. Decis. Support Syst. **86**, 13–23 (2016)

Graham, M.E.: Health beliefs and self breast examination in black women. J. Cult. Divers. **9**(2), 49 (2002)

Henseler, J., et al.: The use of partial least squares path modeling in international marketing. In: New challenges to international marketing, pp. 277–319. Emerald Group Publishing Limited (2009)

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

Hughes, B.B., et al.: ICT/Cyber benefits and costs: reconciling competing perspectives on the current and future balance. Technol. Forecast. Soc. Change **115**, 117–130 (2017)

Janz, N.K., Becker, M.H.: The health belief model: a decade later. Health Educ. Q. **11**(1), 1–47 (1984)

Jick, T.D.: Mixing qualitative and quantitative methods: triangulation in action. Adm. Sci. Q. **24**(4), 602–611 (1979)

Kaplan, J., et al.: Meeting the cybersecurity challenge. McKinsey & Company (2011)

Kim, J., et al.: User resistance to acceptance of In-Vehicle Infotainment (IVI) systems. Telecommun. Policy **40**(9), 919–930 (2016)

MarketWatch: This is the new reality for cyber security: accept that hackers will get in (2016). http://www.marketwatch.com/story/this-is-the-new-reality-for-cyber-security-accept-that-hackers-will-get-in-2016-12-09. Accessed 9 Nov 2017

Rosenstock, I.M.: Historical origins of the health belief model. Health Educ. Monogr. **2**(4), 328–335 (1974)

Rosenstock, I.M., et al.: Social learning theory and the health belief model. Health Educ. Q. **15**(2), 175–183 (1988)

Savulescu, C.: Dynamics of ICT development in the EU. Procedia Econ. Finance **23**, 513–520 (2015)

Steve Morgan, E.-I.-C.: Hackerpocalypse: a cybercrime revelation (2016). http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/. Accessed 23 Oct 2017

Tenenhaus, M., et al.: PLS path modeling. Comput. Stat. Data Anal. **48**(1), 159–205 (2005)

ThreatMetrix: 2017 Q1 Cybercrime Report. 160 W Santa Clara St San Jose, CA, 95113 United State (2017)

Turan, A., et al.: A theoretical model proposal: personal innovativeness and user involvement as antecedents of unified theory of acceptance and use of technology. Procedia-Soc. Behav. Sci. **210**, 43–51 (2015)

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

Venkatesh, V., Davis, F.D.: A theoretical extension of the technology acceptance model: four longitudinal field studies. Manag. Sci. **46**(2), 186–204 (2000)

Venkatesh, V., et al.: User acceptance of information technology: toward a unified view. MIS Q., **27**(3), 425–478 (2003)

Wheeler, J.A.: Emerging risks in cyber security: Gartner's top ten predictions (2016). http://blogs.gartner.com/john-wheeler/gartner-top-ten-cybersecurity-predicts/. Accessed 9 Nov 2017

WSJ: Dow Jones inadvertently exposed some customers' information (2017). https://www.wsj.com/articles/dow-jones-inadvertently-exposed-some-customers-information-1500237742. Accessed 9 Nov 2017