CONTRIBUTION TO SECURING BYOD SYSTEMS IN FINANCIAL AUTHORITIES AND PUBLIC ADMINISTRATIONS IN FREE TRADE ZONES

Patrick Aurélien AMPIRI KWA[1], Rostand Martialy Davy Loembe Souamy[2,3], Aristide MANKITI FATI[1,4]

[1]Department of Electronic and Telecommunication, High Polytechnic School of Brazzaville, Marien NGOUABI University.
[2]Department of computer science and Technology 210023, Jiangsu Provincial Key Laboratory for Novel Technology, Nanjing University, PR China.
[3]Laboratory of Automation, School of Automation, Nanjing University of Post and Telecommunication, Nanjing 210003, China.
[4]Admitelecom Academy laboratory of Microwave, Fiber optic transmission and Networking. Accra (GHANA)

ABSTRACT

The growth of digital tools, such as mobile phones, computers, and tablets, and the advent of new information and communication technologies have generated new phenomena in terms of communication capacity and data processing. This phenomenon is called BYOD, which stands for Bring Your Own Device, meaning employees use their own devices to access company resources within the company's IT network, whether internally or externally. On the one hand, it has brought many benefits and opportunities, but on the other hand, it carries many cybersecurity risks. Incidents of cybercrime, embezzlement, espionage, and cyberattacks. These are recorded every day in ZELECAF countries in general and in Congo Brazzaville in particular. In this article, a contribution and optimization to the security of BYOD systems in the financial authorities of the countries of the African Continental Free Trade Area are presented. Congo Brazzaville was chosen for the field study, and a few Central African countries were chosen for an online study. The results obtained are encouraging to the extent that the survey carried out revealed the use of digital tools in financial management by workers. Also, the lack of solid security in the existing computer networks within these structures was noted. The principles of raising public awareness of cybersecurity culture, protecting information, authenticating passwords by the IT manager or network administrator, hiding the wireless network, and enabling the firewall are part of the attempted solutions proposed. Compared to studies in the literature, the methodology is adapted, so that in the literature [14], [15], the majority of surveys were carried out in the field, with a very limited number.

KEYWORDS

Bring Your Own Device (BYOD), Cybersecurity, Public Administration.

1. INTRODUCTION

The rapid growth of new information and communication technologies, also requiring the use of high-performance transmission media such as optical fiber [1], and the introduction of smartphones, tablets, and computers to the general public market have forever changed the computing landscape for mobile devices [2]. These mobile devices are today carried here and there by the African people in general and the people of Central Africa in particular, which even

DOI:10.5121/ijmvsc.2024.15201

means that all the youth have the tendency to walk with a lowered head while surfing on their phones. These digital tools are also the gateway to espionage on computer networks, especially when they are used in businesses [3]. Bringing your digital tools to the workplace is often known as BYOD, which stands for Bring Your Own Device. BYOD has been discussed since the 1990s but is not widely used as of 2011 [4]. Many organizations are implementing BYOD to improve their IT resources, particularly hardware. BYOD is also believed to actually increase employee productivity. Mobile devices are widely used in offices in Africa in general and in Central Africa in particular. In 2018, there were approximately 10 billion devices available, which means that every person in the world will have more than one device, and 69% of employees use personal mobile devices to connect to the corporate network even in a non-BYOD organization [4]. As many organizations find that BYOD technology brings a lot of benefits to employees as well as organizations, they also worry about the disadvantages and challenges they face. The primary security concern is not about devices or information inside the organization, but controlling user and device access to organizational information and increasing exposure to enterprise networks and malware due to a lack of control and visibility of mobile devices [4]. The great danger is that the user cannot be monitoring in real time the management of his mobile phone; for example, he may also lend his phone, and in such cases, the user becomes a gateway to the entry of spies [5]. In Central Africa, the majority of workers bring their mobile phones to the point of duty and use them once connected to the company network, with the risk of being attacked proportional to threats, breaches, and countermeasures. [5]. In this article, we propose a study resulting from the convergence between bring your own device (BYOD) and cybersecurity. BYOD symbolizes the management of digital tools in public and private administrations. The case chosen for our study is that of Congo-Brazzaville.

2. Literature Review

The studies conducted have provided various reasons for the impact of BYOD on users in an enterprise network. As an illustration, we have the work of [6], where he examined the cybersecurity issues associated with the integration of BYOD into work in selected locations in Kenya, focusing on a non-governmental organization. The specific objectives of the study were to investigate the level of awareness of BYOD security challenges and the measures put in place to address cybersecurity issues associated with BYOD. The results indicate that organizations need to create more awareness about BYOD security since the level of awareness is low. The results also show that security and BYOD measures have been neglected. It is also imperative that organizations implement security measures that will ensure data integrity, confidentiality, and availability. Also, the work of [7] examined the factors affecting information security and program implementation. Bring Your Own Device (BYOD) in the Kingdom of Saudi Arabia (KSA), where it used quantitative metrics to assess user acceptance of the Bring Your Own Device (BYOD) program and identified key factors affecting their adoption using the Technology Acceptance and Use Theory (UTAUT) model. Constructs, such as perceived commercial (PT-Bs) and private (PT-Ps) threats as well as employer attractiveness (EA), were also added to the UTAUT model to provide the public, private, and voluntary sectors with an acceptable method of adopting BYOD programs. Factors affecting the adoption of BYOD programs by the surveyed sectors of Saudi Arabia were derived from the responses of 857 participants. This was followed by the work of [8] on national cybersecurity policies oriented by BYOD (Bring Your Own Device): Systematic review. This work is structured around a systematic review of the real situation of BYOD, trends, and impacts. It will continue with the local situation and a proposal for recommendations oriented towards a national policy in Ecuador. Not forgetting the work of [9], which is on a review of Bring Your Own Device security issues, discussing the background, prevalence, benefits, challenges, and challenges of BYOD. Possible security attacks We then review the contributions of academic researchers to BYOD. At University Putra Malaysia, online databases (such as the IEEE Xplore Digital Library, Elsevier, Springer, and the ACM Digital Library) were used to search for peer-reviewed academic publications and other relevant publications on the BYOD. The Google Scholar search engine was also used. Our in-depth review shows that security concerns are the most significant challenge facing BYOD and that very little has been done to address this challenge. We hope that this review will provide a theoretical framework for future research and enable researchers to identify areas for BYOD research. It would be an aberration to move on without mentioning the work of [10], which focuses on The Involuntary Administrator, Bring Your Own Device in the Zimbabwe Case, whose aim is to show how banks can mitigate information security risks caused by the unwitting administrator using the BYOD Behavioral Information Security (BISB) model. A literature review of BYOD information security and organizational information security culture was conducted. A questionnaire was developed from the literature and sent to 270 banks employed in Zimbabwe. In total, 205 employees participated, and 179 completed the questionnaire. An expert review comprising Chief Information Officers (CIOs) of banks in Zimbabwe was conducted to evaluate the proposed model. From the review literature, individual traits of attitude, knowledge, and habits, as well as organizational traits of environment, governance, and training, were identified as key traits that constituted the BISB model. The overall theme of this article is that banks can mitigate BYOD information security challenges using the BISB model. Beyond these works presented above, a very important aspect is not really mentioned, in particular, showing how the supporters of espionage make electronic devices such as tablets, telephones, and many more. others connected to the company network, an intrusion vulnerability. Also, minimize the risk of attack in the management of these devices useful for communication and data exchange within the company. These are the elements that will be the subject of our research in the case of Central Africa in general and Congo Brazzaville in particular.

3. THEORETICAL FRAMEWORK

3.1. Security Challenges Imposed by BYOD

Bring your own device is a new way to interact with companies´ information and data that originated as a method to deal with the difficulty of using common infrastructure. Companies want to use this new tool to gain a competitive advantage for their business and to facilitate the interaction between the company and its work-at-home employees. Using their personal devices for work helps the company increase its economy and its employees’ occupational comfort [11].

3.2. Impact to use BYOD

By using BYOD, all devices will be connected, which generates doubt amongst companies that consider that implementing this tool is detrimental due to security reasons. This is based on the assumption that there will be other companies utilizing the same network that can potentially access their database or steal any employees' devices and use their information for their own benefit. Society nowadays cannot imagine a world without mobile devices; for that reason, instead of restricting the use of mobile devices, the company has to create policies to control them [12].

The BYOD phenomenon has a major advantage :it reduces the company's infrastructure. This indicates that the company does not need to spend money on extra devices for their workers as they bring their own and can work at home. The essential problem is that not all these devices are considered IT tools, so the IT team cannot apply the same security policies to them [13].

According to the IBM source, BYOD decreases 5.5 million dollars in infrastructure and support costs by an average of 3 years. Likewise, BYOD increases the productivity of workers because they perform their work better in the place they want. There are brands like IBM that have a services manager that allows the best use of the devices that a company owns [15].

3.3. Policies of use BYOD

A BYOD policy needs to be easy to access; easy to understand and allow employees to give feedback, so the company can protect the information they use. The company needs to follow these aspects [14]:

- Employees must secure their devices with passwords and two-factor authentication methods when possible.
- Password must consist of more than 16 characters, alternating between numbers and letters without any meaning.
- Employees should be trained in application usage and download/installation best practices.
- Employees need to report stolen/lost devices so that actions can be taken to minimize security risk.
- Employees are expected to understand what third-party usage is. Can employees let their kids use their phones? If they do, what do they need to ensure when doing so?

3.4. Vulnerabilities, Threats, Risks and Systems Control of BYOD

Some vulnerabilities have been discovered in the last months [16].

They are:

✓ **Insecure Application Usage**

Employees can use their own devices to install any application from Internet. They can download some applications which are designed to steal confidential information and gain access from company’s servers. For that reason, organizations must create policies to restrict applications usage and protect the datacenter.

✓ **Lost/Stolen Devices**

Without appropriate supervision, some devices may be lost or stolen and third parties can intercept the information or cyber criminals can have access to it. For that reason, all devices must be protected and transmit encrypted information.

✓ **Access from Non-Employees**

When employees use their own devices, or when they forget to log off, other people can access the company´s information and even accidentally share confidential information.

✓ **Network Risks**

When employees use their own devices, they can connect to different networks. These networks can be a risk if the information is not encrypted or has no security resource to protect the information and the network when all the employees’ devices are connected.

✓ **Mobile Malware**

Mobile Malware can infect smartphones´ OS. Infection techniques such as Repackaging, Browser Attacks, Update Attack, Drive-by Download (McAfee, 2011) are commonly used. Hackers can cause financial charges to smartphone users by creating mobile malware that sends SMS messages without the knowledge of the user. There are some vulnerabilities when using mobile devices like information stealing or apps designed to ask for information about user such as IMEI, IMSI, location, lists of contacts or installed apps and download history. Mobile malware [17] is one of the most important threats, not only to the security of an individual, but also to the security of critical infrastructures. Researches have proposed different kinds of defense analysis techniques to protect against mobile malware. For example, L4Android is a virtualization-based isolation technique that allows a mobile device to run two isolated operating systems for home and work functionality on the same mobile device.

4. CYBERSECURITY

The prefix "cyber" relates to the IT environment and to the activities made possible by digital and Internet technologies. Cyberspace (all digital infrastructures, data, and networked services) is an extension of our natural space, which reflects our society with its political, economic, social, and cultural realities. But unlike the earth, the sea, the air, and outer space, cyberspace is a pure creation of human beings that does not come from nature [18]. The root "cyber" comes from the word cybernetics, which was formed in French in 1834 to designate the "science of government", from the Greek Kubernêtiké, meaning "to direct, to govern". The term was taken up in 1948 by the mathematician Norman Wiener in the United States at the origin of cybernetics, a science consisting of all the theories relating to the control, regulation, and communication between living beings and machines [18].

Cybersecurity concerns computer security, information security, and the security of networks and environments connected to the Internet. The security of systems accessible via cyberspace can be compromised, among other things, by cyberattacks. Thus, due to the extensive use of the Internet, new threats have appeared, generating additional risks whose impacts, of varying levels of importance, can affect individuals, organizations, or states. The notion of computer security refers to the properties of a computer system, which are expressed in terms of availability (D), integrity (I), and confidentiality (C). These basic criteria (DIC criteria) are achieved by implementing security functions and services, such as those for access control or incident detection, for example. Security services related to authentication (notions of authenticity and veracity) or even non-repudiation, imputability, or traceability contribute to protecting digital infrastructures (Figure 1.1) [18].

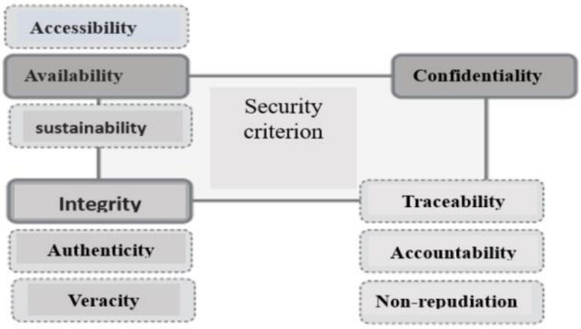

Figure1: Security criteria [18].

5. RESULTS AND DISCUSSIONS

5.1. Verifying the Existence of the Problem

To achieve our objectives, we undertook a process consisting of carrying out a field investigation in order to first justify the veracity of the existence of the problem, in particular if the workers brought their phones, tablets, or PCs to the workplace. This was approached in two parts. First, we carried out the investigation with the financial authorities of Congo Brazzaville. To do this, financial authorities such as the Public Treasury encourage the banking of populations, particularly those excluded from the traditional banking system. The MUCODECs are also part of the Congolese economic landscape thanks to the division of civil servants' salaries and retirees' pensions, and a few banks, which we named B1, B2, B3, and B4, were chosen. Some public ministries were also chosen for the survey experiment. Three variables x, y, and z were chosen, where x represents the number of women who have either a smartphone, a tablet, or a PC, y is the number of men who have a powerful digital tool, and z is the number of those who do not have a smart tool. Table 1 illustrates the data collected from financial authorities.

Table1: Data from financial authorities on the BYOD of some institutions

x	y	z	Financial authorities
48,00	57,00	05,00	Public Treasury of Brazzaville
31,00	48,00	09,00	Public Treasury of Pointe Noire
67,00	107,00	51,00	Public treasury in the interior of the country
44,00	43,00	08,00	MUCODEC of Brazzaville
37,00	41,00	03,00	MUCODEC of pointe Noire
66,00	101,00	41,00	MUCODEC of the interior
21,00	31,00	0,00	B1
18,00	29,00	0,00	B2
23,00	44,00	01,00	B3
15,00	30,00	02,00	B4

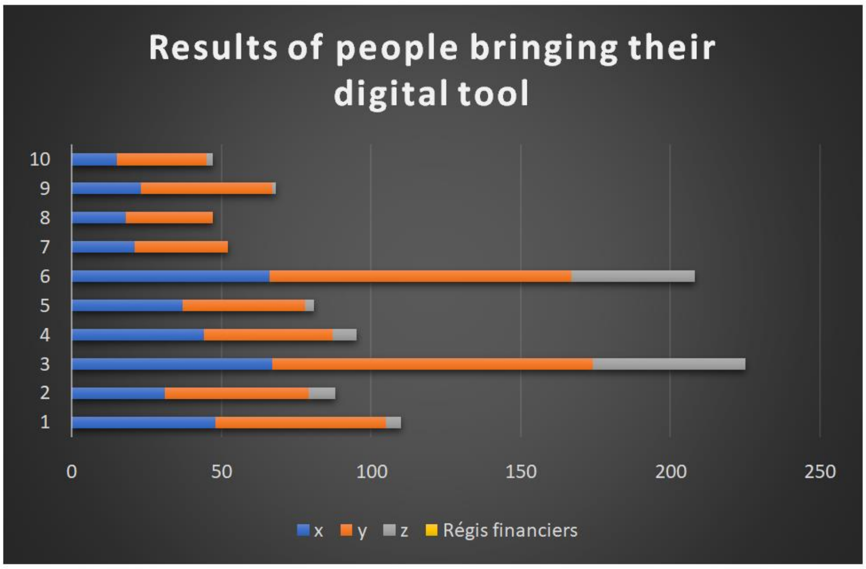

Figure 2: Simulation result of the field survey

Figure 2 represents the results of the survey carried out in some financial authorities in the Republic of Congo. It should be noted that almost everyone brings either their phone, their tablet, or their laptop to the place of service, so in Table 1, just inside the country where we observed that people bring their digital tools to the place of service, we understood that this was due to the absence of local networks in certain public administrations and the high cost of data. The same survey was carried out in some public ministries of the Congolese state; for reasons of confidentiality, we kept these different ministries anonymous and named them M1, M2, M2,... M10. The results of the survey are shown in the following:

Table2:Data from some ministries on the BYOD

x	**y**	**z**	Ministries in the Republic of Congo
71,00	109,00	30,00	M1
55,00	98,00	19,00	M2
87,00	111,00	21,00	M3
31,00	150,00	18,00	M4
47,00	77,00	11,00	M5
66,00	101,00	31,00	M6
25,00	99,00	25,00	M7
31,00	151,00	12,00	M8
51,00	89,00	21,00	M9
37,00	90,00	32,00	M10
55,00	94	17,00	M11
44,00	170	25 ,00	M12
53,00	98	19,00	M13
23,00	87	33,00	M14
57,00	108	45,00	M15

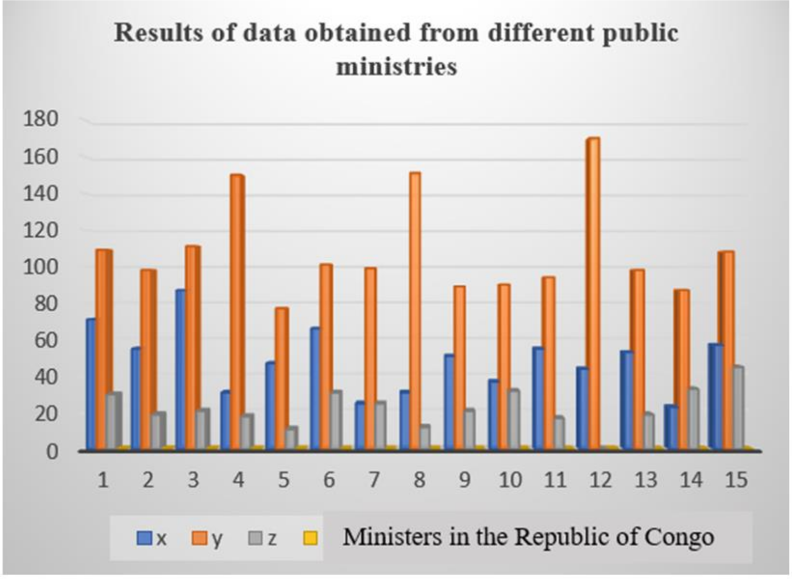

Figure 3: Simulation result of the field survey in the case of public ministries

Figure 3 represents the results of the survey carried out with some public ministers in the Republic of Congo. Note that out of the 36 ministers where we submitted a request, counting the number of workers with a smartphone, a tablet, or a PC who can access the local network of the minister or cabinet, just 15 ministers gave us access on the condition of not highlighting the name of the minister in the article; this is for the sake of confidentiality. If we notice in the graph in Figure 3 or the results from Table 2, the number of those who do not have smartphones or other digital tools is very high compared to financial authorities. This is simply due to the lack of local networks among the majority of these ministers. Although the number of smartphones is high in these institutions, the study being carried out is a warning for the next few years given the advancement of information and communication technologies.

5.2. Results of Some Countries of the African Continental Free Trade Area

A study was carried out in the field by submitting a series of questions on the internet to those working in the financial public service and in some bank by using social networks, notably Facebook and WhatsApp, in three member countries of the free trade zone, namely Tchad, the Central African Republic, and the Democratic Republic of the Congo. The questions submitted are put in the following table3:

Table 3: Online results obtained on the ground for the few member countries of the African Continental Free Trade Area

QUESTOINS	**Positive assessment: "YES"**	**Negative rating: "NO"**	**Observation (RATE)**
Do you use your own computers for professional tasks?	20	10	**67%**
Do you use your phones or tablets for professional tasks?	16	14	**53%**
Do you regularly make backups (PC or smartphone)?	13	17	**43%**
Do you apply for updates regularly?	18	12	**60%**
Are you using up-to-date antivirus?	9	21	**30%**
Have you implemented a policy for the use of strong passwords (9 characters minimum)?	19	11	**63%**
Have you enabled a firewall? Do you know the filtering rules?	6	24	**20%**
Have you secured your messaging (phone or tablet)?	8	22	**27%**
Do you think it is necessary to install office software on a server?	18	12	**60%**
Do you think it is necessary to install office software on all client workstations?	26	4	**87%**
Do you control digital risks during missions or business trips?	6	24	**20%**
Do you control digital risks during missions or business trips?	6	24	**20%**
Have you secured your WiFi (with MDP by default)? And with what protocol?	23	7	**90%**
WEP	7	23	**23%**
WPA1	5	18	**17%**
WPA2	11	7	**37%**
Do you make purchases on the Internet (shopping)?	12	18	**40%**
Have you ever been the victim of an internet threat or attack?	21	19	**70%**

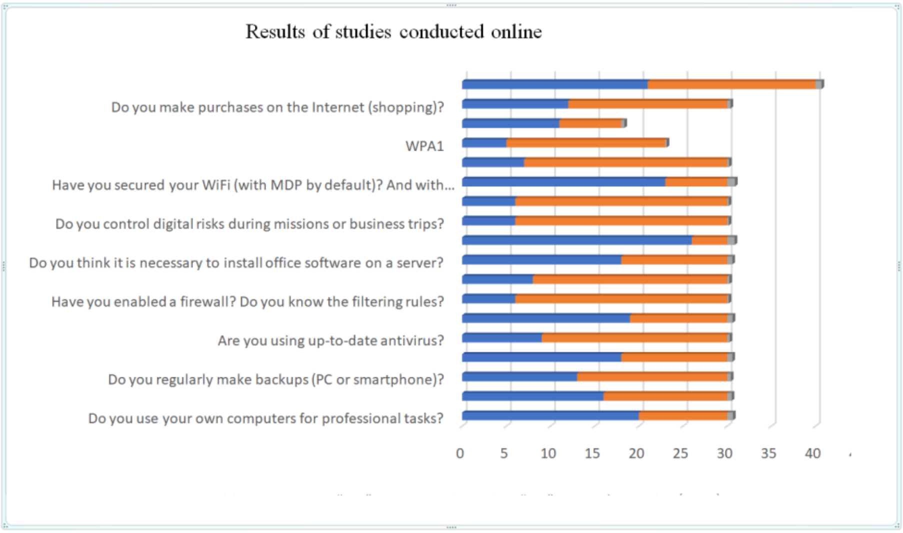

Figure 4: Online results from some ZLECAF countries (Chad, the Central African Republic, and the and the Democratic Republic of the Congo.

This figure shows us the results of the study carried out in the field in the few countries of the African continental free trade area (ZLECAF, in acronym). Which we obtained through online questionnaires in order to validate those obtained in Congo Brazzaville, where we have personally been in the field. In our quest for reliable data, we reached out to WhatsApp and Facebook groups to get this. It is clear that these countries suffer from the same disease, in particular the lack of reliable security within financial authorities, while security, as estimated by Doctor Jeff Crume and [18], is defined mathematically by the relationship:

$$S = P + D + R \tag{1}$$

Where:

S: the security,
P: the prevention
D: Detection
R: Response

This is how, with a view to prevention, we are highlighting this policy of raising awareness in the countries of the free trade zone within the framework of financial authorities. From Figure 3, we notice that more than 53% of workers bring their phones to the service, access the company network, and use the same tools in their homes. Also, more than 90% use Wi-Fi networks with default passwords.

5.3. Solution and Recommendations

Note that the risk of the network being vulnerable is defined [2]:

$$R=M*V/C \tag{1}$$

Where R is the risk that the network runs against hackers; M is threats; and C is the countermeasures that must be put into play to counter the attacks. In formula (1), we note that these cell phones, tablets, or other digital tools represent the vulnerabilities that can make the network vulnerable; to minimize the risk, the countermeasures must tend towards infinity or be just high. Among the countermeasures that must be strengthened to minimize the risk of being attacked, financial authorities, public ministers, and even other public or private institutions must follow these aspects:

- ✓ Employees should secure their devices with passwords and two-factor authentication methods where possible.
- ✓ The password must be composed of more than 16 characters, alternating numbers and letters without any meaning.
- ✓ Employees should be trained in application usage and download/installation best practices.
- ✓ Employees should report stolen or lost devices so that steps can be taken to minimize security risks.
- ✓ Employees must understand what third-party use is. Can employees let their children use their phones?

The IT manager must also activate the firewall for network security; he must also hide the WiFi and configure his router properly. The allocation of the password at the worker level also has a contribution, and every day the IT manager must change the password for his network. Also, raising worker awareness about espionage mechanisms would be a panacea for reducing risk. Protecting information with policy encryption restricts device application downloads. Only if necessary can employees have access to storage. Policies should be focused on all devices that connect to the internal or external network; it should be easy for everyone working on it; and workers should understand the importance of using BYOD and its risks.

6. CONCLUSION

In conclusion, it is worth remembering that, although BYOD allows workers to be connected anywhere and access information with all possible mobility, there is no cybersecurity policy or strategy to ensure the connection and the information transmitted. For this, member countries of the African Continental Free Trade Area must define a good policy so that security corresponds to prevention, detection, and response. This is why these ZLECAF member countries must promote a good policy on the security of all data in general and of financial authorities in particular. First of all, raise awareness among workers, financial authorities, and many other actors in the public and private sectors. This awareness is the first solution, as is the training of IT management agents for network supervision and administration.

ACKNOWLEDGEMENTS

I would like to thank professor Jean Mathurin Nzikou, in order to help me joining the PhD program.

REFERENCES

[1] Aristide MANKITI FATI, “Study of the Valuation of Multimode Optical Fibers by Translation of Transmission Techniques of Optical Fiber and High Speed Mimo Radio Frequency in Local Area Network.” 25 octobre 2020.

[2] F. Jamal, I. Technology, I. Technology, A. Abdullah, I. Technology, and I. Technology, “BYOD Authentication Process (BAP) Using Blockchain Technology,” Adv. Res. Dyn. Control Syst., vol. 10, no. 11, pp. 166–172, 2018.

[3] Patrick Aurélien Ampiri Kwa, Mankiti Fati Aristide “Duality between E-commerce and Cybersecurity: Case of Central Africa” ,9 July 2023.

[4] Y. Wang, J. Wei, and K. Vangury, “Bring Your Own Device Security Issues and Challenges,” in The 11th Annual IEEE CCNC- Mobile Device, Platform and Communication Bring, 2014, pp. 80–85.

[5] Stephen Pao and M. Thorne, “BYOD Security : Expert Tips on Policy , Mitigating Risks , &Preventing a Breach Meet Our Panel of Data Security Experts :,” 2016. [Online]. Available: https://digitalguardian.com/blog/byod-security-expert-tips-policy-mitigating-risks-preventingbreach. [Accessed: 18-Sep-2018].

[6] David Njuguna1 , Wambui Kanyi2 “An evaluation of BYOD integration cybersecurity concerns: A case study” Published Date: 07-March-2023.

[7] Adel A. Bahaddad 1,* , Khalid A. Almarhabi 2 and Ahmed M. Alghamdi 3 “Factors Affecting Information Security and the Implementation of Bring Your Own Device (BYOD) Programmes in the Kingdom of Saudi Arabia (KSA)” Published: 11 December 2022.

[8] Andrea Vaca Herrera1,2, Mario Ron2 , Carlos Rabadão1,3 “ National Cyber-security Policies oriented to BYOD (Bring Your Own Device): Systematic Review”

[9] Morufu Olalere1,2 , Mohd Taufik Abdullah2 , Ramlan Mahmod2 , and Azizol Abdullah2,” A Review of Bring Your Own Device on Security Issues”

[10] Alfred Musarurwa1 | Stephen Flowerday2 | Liezel Cilliers,” The bring-your-own-device unintended administrator: A perspective from Zimbabwe”. Accepted: 18 December 2018

[11] Ballagas, R., Rohs, M., Sheridan, J. G., & Borchers, J. (2004, September). Byod: Bring your own device. In Proceedings of the Workshop on Ubiquitous Display Environments, Ubicomp (Vol. 2004).

[12] Thomson, G. (2012). BYOD: enabling the chaos. Network Security, 2012(2), 5-8.

[13] Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. Network Security, 2012(12), 5-8.

[14] IBM, (2017). IBM brings ROI to BYOD. [image] Available at: https://www-935.ibm.com/services/us/en/it-services/enterprisemobility/total-economic-impact-study-infographic/ [Accessed Mayo 2013].

[15] IBM, (2017). IBM brings ROI to BYOD. [image] Available at: https://www-935.ibm.com/services/us/en/it-services/enterprisemobility/total-economic-impact-study-infographic/ [Accessed Mayo 2013].

[16] Tokuyoshi, B. (2013). The security implications of BYOD. Network Security, 2013(4), 12-13.

[17] Seo, S. H., Gupta, A., Sallam, A. M., Bertino, E., & Yim, K. (2014). Detecting mobile malware threats to homeland security through static analysis. Journal of Network and Computer Applications, 38, 43-53.

[18] Vijay Yadav1,” A Study of Threats, Detection and Prevention in Cybersecurity”07 Issue: 05 | May 2020

AUTHORS

Patrick Aurélien AMPIRI KWA

Rostand Martialy Davy Loembe Souamy

Aristide MANKITI FATI