International Journal of Advanced Technology and Engineering Exploration, Vol 7(68)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2020.762051

Review Article

Cybercrimes awareness, cyber laws and its practice in public sector Tanzania

Cesilia Mambile[1*] and Peter Mbogoro[2]
Admission and Examination Officer, Department of Admission and Examination, Tanzania Public Service College, Tanga, Tanzania[1]
Tutorial Assistant, Tanzania Public Service College, Tanga, Tanzania[2]

Received: 20-June-2020; Revised: 25-July-2020; Accepted: 26-July-2020

Abstract
The objectives of this paper was to determine the awareness of cybercrimes and cyber laws in the public sector. Since the services offered by the public sector to the citizens are the implementation of government wishes/goals. And anything that has to be completed in order to improve our country and to provide services to the people, is determined by the work of public servants. Public servants have a massive task and perform a significant role to make service provision work for the people. Nowadays, most of the public servants perform various works using the internet, but despite the fact that the internet has become a powerful platform in accomplishing our day to day activities in Tanzania, there has been a challenge public servant do not understand, that internet is not "high seas". Most public servants know very little about cybercrimes, cyber laws and their impacts causing lack of confidentiality and integrity in Information Systems, publication of false news, theft of intellectual property and government data. The study was qualitative method whereby literature reviews, questionnaire and interviews were used to collect information. The research findings show that public servants who access internet are many compared to those who do not use because it offers tremendous benefits and it is one of the fastest developing areas of technical infrastructure development. Also, there is an increased rate of activities done using computer systems and smart phones since internet services cost is often lower compared to services outside the network. Furthermore, results show that most of the public servants are not aware of cybercrimes so they cannot take any precaution as well as they cannot protect the country and themselves from the substantial danger caused by cybercrimes. Results revealed that public servants know very little about the laws and others do not know even its existence. The government together with Higher education institutions need to provide awareness training, workshops and certification to public servants to ensure that they are aware of cybercrimes and cyber laws so that they can avoid committing cybercrimes as well as preventing their organization and the society in general against Cybercrimes.

Keywords
Cybercrimes, Cyber law, Computer misuse, Public sector, Public servants.

1.Introduction
Government of Tanzania provides services such as education, healthiness, security, transportation, water, electricity, wellbeing and accommodation, on a huge scale. These are public services, which are offered by public servants as an implementation of government goals on behalf. Anything that has to be accomplished so as to improve our country and to provide services to the people, is determined by the work of public servants. Public servants have a massive task and perform a significant role to make service provision work for the people, and must ensure safety.

In public sector and other sectors nowadays almost, every activity has become dependent on significant benefits of information technology [1]. Means that more activities are done using computerized systems, for example financial activities offered in accounting and finance department, Procurement activities, student registration, processing student's results, data storage as well as production of student final results to mention few. All this work has been automatized and performed when connected to the internet, the number of people using the Internet is more than 2.4 billion, all demanding online services [2]. The term internet can be defined as a network of networks, linking numerous computers together and offering an arrangement for the use of email, databases and other computational resources [3, 4].

*Author for correspondence
This work was supported in part by Tanzania Public Service College, Tanga, Tanzania in 2019 to 2020

Despite the fact that internet has become a powerful platform in accomplishing our day to day activities in Tanzania, there has been a challenge public servant do not understand that internet is not “high seas”. Most of public servants know very little about cybercrimes, cyber laws and their impacts that is why maintaining confidential information handled by computer systems is a long process yet increasingly problem [5]. Cybercrimes are any kind of crime performed on the internet by using smartphone or computer as either a tool for performing a crime or a targeted victim. [6, 7]. The following are few examples of cybercrimes; pornography, identity theft, publishing of false information, forgery and any other illegal action executed using computer software, hardware, network and internet. Most of public servants have very little ideas about cyber laws. Cyber law, also known as cybercrime law, is legislation which concentrates on the tolerable behavior use of technology such as internet, networks, computer software and hardware [8]. Or we can say that cyber law is area of law that deals with internet, cyberspace and their respective legal issues. If someone breaks a cyber law, will be subjected to law. Tanzania as in any other countries, there is cybercrime law, called THE CYBERCRIME ACT, 14/2015. Unfortunately, in Tanzania many people including public servants think that when using internet, they can do anything without ever being brought to justice. On the contrary, misuse and abuse of internet platform brings with its number of liabilities [9].

Public servants do not know if they do something wrong when using internet will be answerable to law means that they will be brought to justice. The main objective of this study is to ensure that public servants are aware of cybercrimes, cyber laws and also, they understand issues which will result for them to be answerable in the hands of law. For example they need to know cybercrimes in the workplace which include, but not limited to, publishing false information, accessing sites that are not work related, theft of intellectual property e-mail abuse, government data and identity, pornography, illegal accessing of data, illegal data interference, gaming, denial of service attack, malware targeting mobile device and downloading programs which are not work related such as movies [9]. Furthermore, using internet too often at work, which is normally mentioned as 'cyber slacking' is also a cybercrime committed at work. [5, 9]. In the end, these abuses refer to employees being on line during work hours and not responsible for tasks related to accomplishing organizational goals [9].

Public servants also need to know about user generated content, and what will happen to them if they generate bad content when using internet or computer systems. Bad contents are nude pictures, deformation, insults, posting dead bodies, publication of false news, and others of the like. It is good to take precautions about posting your own information on the internet even if others are happy to post pictures of their belongings, their details, or any other personal stuff. Remember what goes online, always stays online. (Parris-Long, 2012). User generated content can be defined as any form of content such as digital images, video, discussion from posts, audio files, blogs and any other media produced or published by internet users for example in social media and it is publicly available to other internet users [10].

2.Materials and methods

The study was qualitative method whereby literature reviews, questionnaire and interviews were used to collect information. Through the interviews casual talks were conducted for the collection of information, and we interacted with the public servants from different organization together with top level management. Furthermore, structured questionnaire was also administered to public servants and relevant data for understanding to what extend do they understand cybercrimes and cyber laws was collected. Structured Questionnaire was created using survey monkey.

2.1Study area description

The information gathering was conducted in Tanga District. It is one among the eight Districts of Tanga Region in Tanzania. The District is bordered to the South by Muheza District and to the North by Mkinga District. The administrative capital of the District is Tanga city. According to the 2012 Tanzania National Census, the population of Tanga District was 273,332.

2.2Research design

From the study area, data were collected for four months. It was 1st February to 30th May 2020. Four months was sufficient since the study didn’t need any experiment.

A structured questionnaire was created online using Survey Monkey.com. Survey Monkey is a survey tool based on cloud, it helps users to create, send and

analyze surveys. Using this tool, users can email their surveys to participants and publish them on social media platforms to seek more response rate [11]. This questionnaire was used to understand if public servants know what is cybercrime? What is internet abuse in the workplace is? What are cyber laws? Etc. Interview was conducted to public servants to find out if they are aware of cybercrimes and its consequences. Interview is always a worthy tool for complete understanding of what users do, how and why? Interview is used to gather facts through speaking. [12, 13].

2.3Sample size and sampling technique

The sample size of the study was 100 respondents form ten wards of Tanga district namely Chumbageni, Mabawa, Makorora, Kange, Maweni, Nguvumali, Usagara, Sahare, Majengo and Raskazone We used a random sampling technique to get all the participants. We left it open for anyone to participate. The sampling process was dynamic in the sense that whoever attended the questionnaire had a chance of participating in the study; the only requirement was that this person must be public servant and willing to do so.

3.Results

The analysis of the collected data was done using Bar Charts, Radar Charts Visualization together with the support of descriptive statistics. Bar chart is a used to show and relate the frequency, number or other measure for example mean, for dissimilar groups of data [14]. In this study bar chart was used because of its simplicity and easiness in interpretation. Radar Chart is a useful tool for comparisons between results obtained [15]. Descriptive statistics provide simple summaries about the sample and the measures together with graphics analysis.

3.1Respondents profile

Table 1 provides the full distribution of public servants in selected wards. Most of them have the age between 20 to 66 years. The mean age is 43 years.

Table 1 Participants (public servants Tanga District), 2020

S. No	Ward	Respondent number
1	Chumbageni	13
2	Mabawa	12
3	Makorola	11
4	Kange	11
5	Maweni	10
6	Nguvumali	10
7	Usagara	9
8	Sahare	8
9	Majengo	8
10	Raskazone	8
11	Grand Total	100

3.2Public servant's internet access and increased rate of activities done using computer systems and smartphone

Nowadays almost every public servant accesses the internet whether for private use or for work purposes. *Figure 1* shows that public servants who access internet are many compared to those who do not use internet, because it offers tremendous benefits and it is one of the fastest developing areas of technical infrastructures development. Also, internet services cost are often lower compared to services outside the network [16]. *Figure 2* shows increased rate of activities done using computer systems. It was discovered that most of the activities in public sector are done using computer systems compared to few years ago. Nowadays in public sector e-mails have displaced traditional letters. Results shows that e-education is penetrating in most of the universities and colleges. Also, in different organizations it was found that online meetings, trainings and presentations are more important nowadays than hard copy materials. Online communication and phone services are developing quicker than landline. One of the respondents said that "the accessibility of online services offer a great number of benefits for organizations, individuals and society at large, I can attend the evening classes while sitting at home" During this study it was discovered that, electronic education, electronic commerce, electronic government, electronic environment and electronic health are enablers of development, since they offer a well-organized and effective way to serve a lot of basic services in town and remote areas.

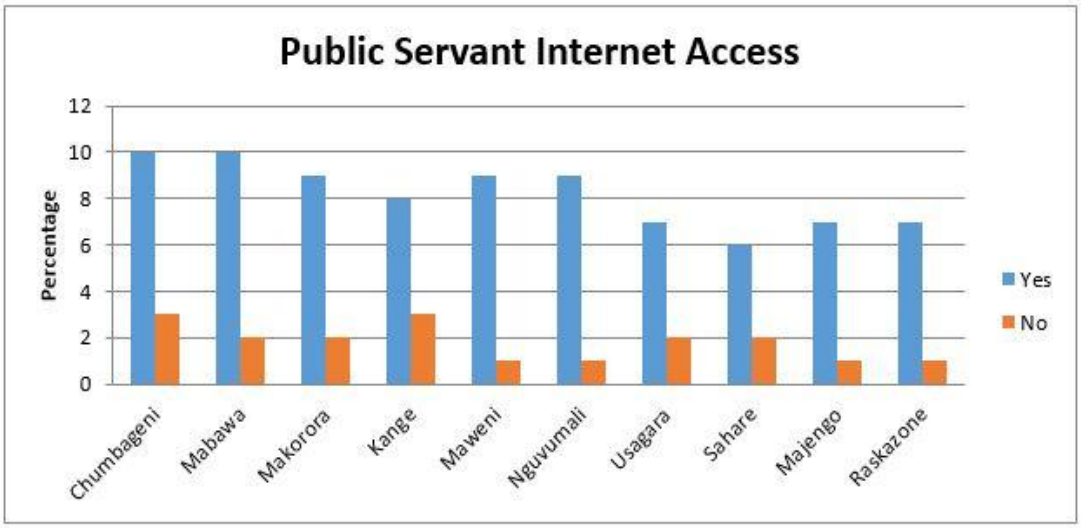

Figure 1 Description of Public servant's internet usage, 2020

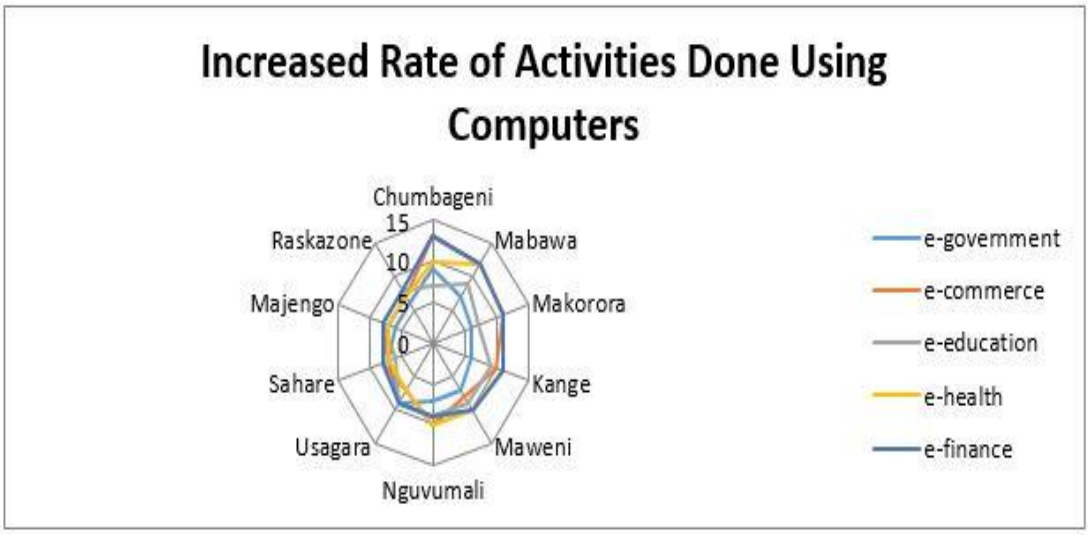

Figure 2 Description of Increased rate of activities done using computers, 2020

3.3Cybercrime and cyber laws awareness in public sector

In this study the degree of understanding cybercrimes committed at work place was assessed. Results show that most of public servants have very little understanding of what exactly is a cybercrime. Most of them did not understand if cyber slacking is a cybercrime committed at work place. Also, they did not understand if accessing sites which are not work related, email abuse, gaming, downloading programs of personal use, theft of intellectual property, and publishing false information are all cybercrimes committed at work place. *Figure 3* below provides the description of degree of understanding cybercrimes committed at workplace.

Figure 4 provides the description of cybercrime awareness in public sector; the description shows that most of the public servants are not aware of cybercrimes and its impact. It was discovered that public servants are not aware of a danger so it is obvious that they can neither take any precaution to protect themselves nor the country from the substantial danger caused by cybercrimes. They can also commit the crimes.

Cyber law gives the punishment after someone has committed the cybercrime. Unfortunately, the study shows that in public sector people are not aware of cyber laws. *Figure 5* provides the description of

awareness of cybercrime Act, 14/2015 of Tanzania. The study shows that public servants know very little about the laws and others do not know even its existence. During the interview, one of the respondents said "I thought that when using internet I can do anything without ever being liable" Because of its importance, cyber laws should be known to public servants. Below is a short description of Cybercrime Act, 2015 of Tanzania, which will enable people to understand the law easily.

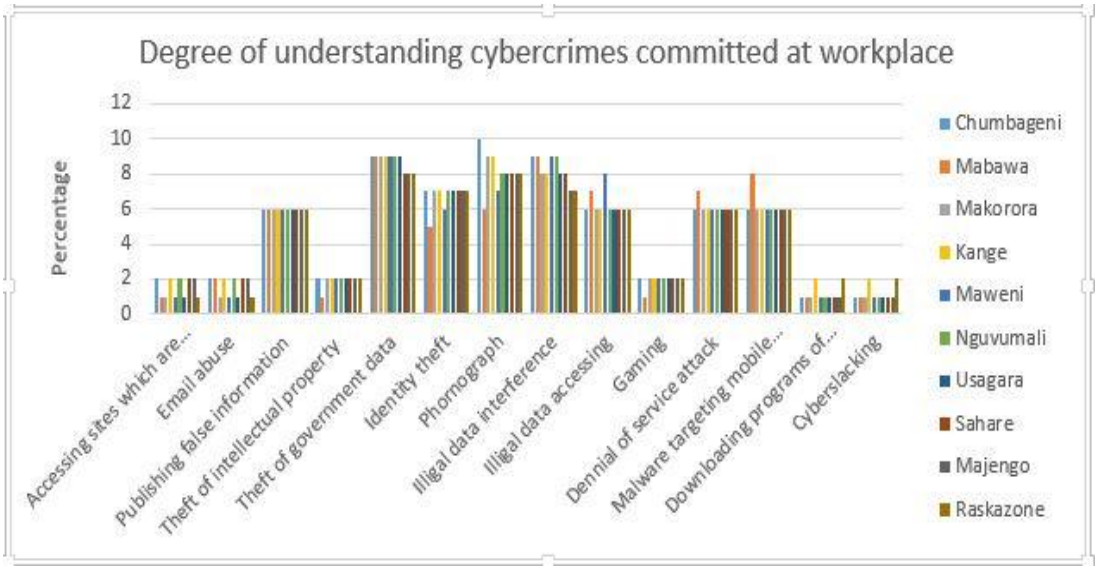

Figure 3 Degree of understanding cybercrimes committed at workplace, 2020

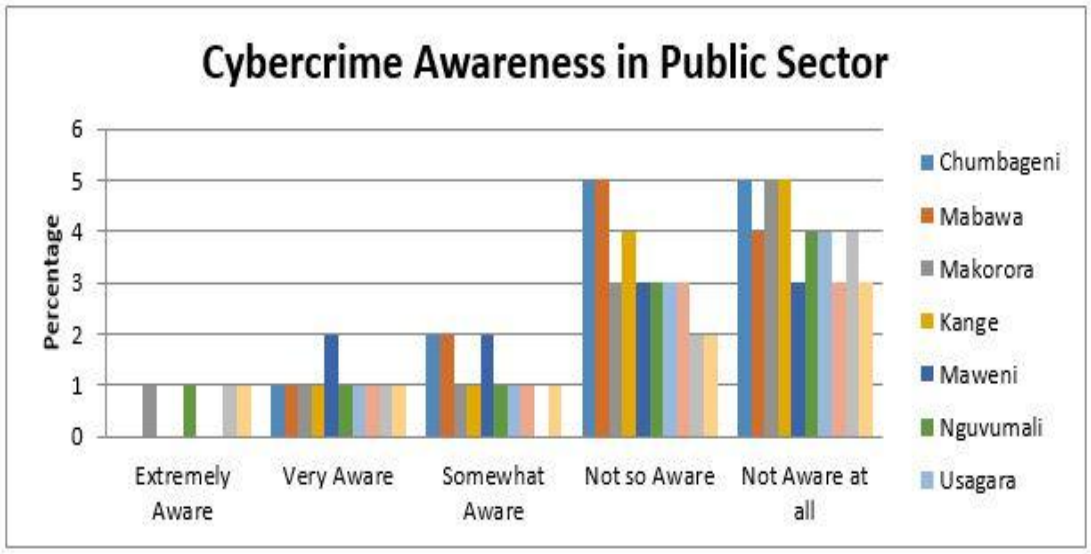

Figure 4 Description of Cybercrime Awareness in Public Sector, 2020

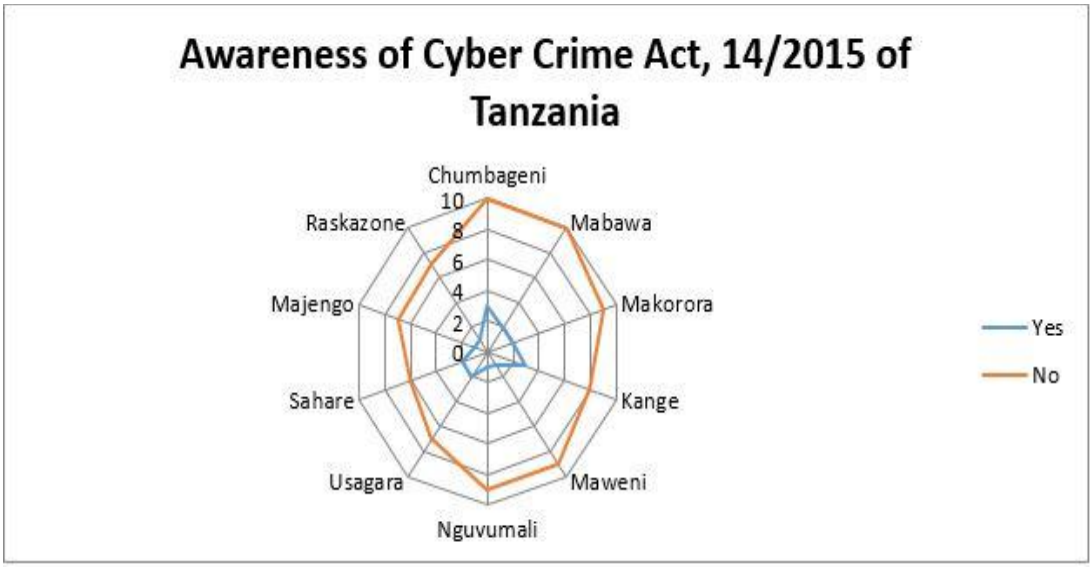

Figure 5 Description of awareness of cybercrime Act, 2015 of Tanzania, 2020

4.Discussion

According to [17] 76.02% of public servants have constant access to the internet, This study also shows that today most of the public servants use internet to accomplish their day to day activities as a result, the tendency to digitization is developing too fast and its impact on society is real, hence more activities are done using computer information systems, this is a fact that cybercrime and cybercrime laws awareness is required.

Without cybercrime and cyber laws awareness, maintaining the confidentiality of information processed by computing systems will always be a problem for example in the study done by (Mussa, Kipanyula, Angello, & Sanga, 2016) shows that, In Developing countries like Tanzania there is no confidentiality of information processed by computers because many public servants commit cybercrimes and are not reported. And the study shows that, this is happening due to the lack of cybercrimes awareness and cyber laws awareness. Cyber laws are among the strategies for minimization and or stoppage of cybercrimes since they are enabling the investigation, prosecution and punishment for online criminal activities. It applies to the actions of the public, groups, individuals, government, as well as private organizations that violate the use of internet. For example employers or employees who access the computer internet system illegitimately and have a personal gain in which he could not have the same is committing an offence of illegal accessing of information or computer system and is liable to fine as stipulated under Section 4 (1) and (2) of Cybercrimes Act, 2015 of Tanzania states that 'A person shall not intentionally and unlawfully access or cause a computer system to be accessed. A person who contravenes Subsection (1) commits an offence and is liable, on conviction, to a fine of not less than three million shillings or three times the value of undue advantage received, which is greater or to imprisonment for a term of not less than one year or to both'.

Another example of the offences which can be done by the public servant is publication of fake news when sharing information or dissemination. It is now a tendency that people do share information by using social networks or internet without taking time to research such news which some are just rumours, so with or without knowing sharing such information pilot to breach of the law and warrant a person to be taken to justice. As per Section 6 of the same Act stipulate that 'Any person who publishes information or data presented in picture, text, symbol or any other form in a computer system knowing that such information or data is false, deceptive, misleading or inaccurate, and with intend to defame threaten, abuse, insult or otherwise deceive or mislead the public or counselling commission of an offence, commits an offence, and shall on conviction be liable to fine of not less than five million shillings or to imprisonment for a term of not less than three years or to both'.

In a nutshell writer saw it fit to break down the Cybercrime Act, 2015 of Tanzania, for a reader to understand what cybercrime is and what are the parts

comprised therein. The Act is divided into Seven (VII) Parts with 59 Sections which apply to both Tanzania mainland and Zanzibar except Section 50 which applies only to Tanzania mainland in exclusion of Zanzibar.

Part I is Section 1 up to 3, which are the preliminary provisions; that are short title, place of application of the Act which is United Republic of Tanzania and interpretation Section. From Section 4 up to Section 29 is the Part II of the Act, provides for the offences onto which a person can be liable when contravening from the same. The offences can be categorised to two parts. First part is Section 4 up to Section 12 which deals with the offences of technical aspects to internet which is done by the person with computer knowledge to use, access, interfere, hinder or restrict someone's else usage of computer without lawful consent. While the second part starts from Section 13 up to Section 29, which deals with the offences in platform that are the infrastructures given to different players with no direct cost, such as Google, YouTube and others of the like.

Part III of the act comprises Section 30 which provides for the jurisdiction of courts to try cyber matter. And here the court is mandated to try all the offences committed with in United Republic of Tanzania or elsewhere in a ship or plane registered in Tanzania. Part IV of the act includes Section 31 up to Section 36. This part deals with the search and seizure as the result from cybercrime. The part tells how seizure and search shall be done. Sections 39 up to Section 46 of the Act are Sections in Part V of the Act which deal with the liability of service providers who fail to take reasonable control of the use of internet in their disposal.

Part VI of the Cybercrime Act tells on the general provisions such as power to make regulations by the minister concerned, compounding offences and immunity for authorised officers over cybercrime offences among others. And the last part is Part VII which basically ventures itself in providing the consequential amendments made by the Act to other former Acts in the united Republic of Tanzania as from Section 52 up to Section 59.

5.Conclusion and future work

Public servants need to understand that technology adoption provides public sector with the most significant benefits as well as drives business innovation and growth in Tanzania while at the same time exposes the country as well as individuals to substantial risks such as new and emerging threats [18, 19]. Public servants need to understand that anyone who commits an offence will be punished according to the law as it is legally known that ignorance of the law should not be used as the defence. The awareness will ensure that they avoid committing cybercrimes as well as preventing their organization and the society in general against Cybercrimes [5]. In order to combat and win the fight against cybercrimes, we need a harmonized hard work between all important stakeholders such as educational institution, business organizations, government bodies and law enforcement authorities [6].

The government together with Higher education institutions need to provide awareness trainings, workshops, short courses and certification to public servants to ensure that they are aware of cybercrimes and cyber laws. Also, the government of Tanzania together with law enforcement authorities needs to improve the cyber laws since the existing Tanzanian laws do not recognize many cyber space crimes [5]. Tanzania needs a strong cyber security but firstly people need to be aware of the need to take precautions, and then teachers need to impart the skills required for precautions [20].

Together, cybersecurity and cyber law, face a lot of challenges because of the increased development of science and technology but they are sole savior to combat cybercrime and both provide confidence, integrity and safe availability of computer and online services to users [20]. Though achieving that to the maximum still have some miles to go before they can be truly effective.

Acknowledgment

The authors acknowledge Tanzania Public Service College Tanga Campus, for funding this publication and anonymous reviewers for their contribution.

Conflicts of interest

We confirm that the manuscript has been read and approved by all named authors and we have no conflict of interest to declare.

References

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf. Accessed 18 May 2020.

[2] Idrus SZ, Hitam NA. Social media use or abuse: a review. Journal of Human Development and Communication. 2014; 3:48-58.

[3] Dordal PL. An introduction to computer networks. 2020.
[4] Ciccarelli P, Faulkner C, FitzGerald J, Dennis A, Groth D, Skandier T. Introduction to Networking Basics. John Wiley & Sons; 2012.
[5] Nfuka EN, Sanga C, Mshangi M. The rapid growth of cybercrimes affecting information systems in the global: is this a myth or reality in Tanzania?. International Journal of Information Security Science, 2014; 3(2): 182-99.
[6] Quarshie HO, Martin-Odoom A. Fighting cybercrime in Africa. Computer Science and Engineering. 2012; 2(6):98-100.
[7] Saini H, Rao YS, Panda TC. Cyber-crimes and their impacts: a review. International Journal of Engineering Research and Applications. 2012; 2(2):202-9.
[8] https://online.norwich.edu/academic-programs/ resources / cyber-law-definition. Accessed 23 June 2020.
[9] Rensleigh CW. Controlling Internet abuse through effective content filtering: a higher education implementation. South African Journal of Information Management. 2002; 4(4):1-11.
[10] https://www.business2community.com/content-marketing/what-is-user-generated-content-and-how-it-is-relevant-02175516. Accessed 23 December 2019.
[11] https://www.softwareadvice.com/survey/surveymonkey-profile/. Accessed 18 May 2020.
[12] Law M, Stewart D, Letts L, Pollock N, Bosch J, Westmorland M. Guidelines for critical review of qualitative studies. McMaster University Occupational Therapy Evidence-based Practice Research Group. 1998:1-9.
[13] Sadiq M. Modeling the non-functional requirements in the context of usability, performance, safety and security.2010.
[14] https://developers.google.com/chart/interactive/docs/gallery/barchart. Accessed 18 May 2020.
[15] https://msktc.org/lib/docs/KT_Toolkit/Charts_and_Graphs/Charts_and_Graphics_Radar_508c.pdf. Accessed 18 May 2020.
[16] https://www.unodc.org/e4j/data/_university_uni_/understanding_cybercrime_phenomena_challenges_and_legal_response.html?lng=en&match=Understanding%20cybercrime:%20Phenomena,%20challenges%20and%20legal%20response. Accessed 18 May 2020.
[17] Saxena KB. Towards excellence in e-governance. International Journal of Public Sector Management. 2005.
[18] Müller M. Cyber Security Report 2019. Die Aktiengesellschaft. 2019; 64(19): r283-4.
[19] Igba ID, Igba EC, Nwambam AS. Cybercrime among university undergraduates: implications on their academic achievement. International Journal of Applied Engineering Research. 2018; 13(2): 1144-54.
[20] Venter IM, Blignaut RJ, Renaud K, Venter MA. Cyber security education is as essential as "the three R's". Heliyon. 2019; 5(12): e02855.

Cesilia Mambile is an admission and Examination Officer at Tanzania Public Service College, Tanga campus, Tanzania. She holds Masters in Information Communication Science and Engineering, Specializing in Information Technology Systems Development and Management graduated at Nelson Mandela African Institution of Science and Technology, Arusha Tanzania in 2019 and also holds a BSc in Information Technology graduated at The Institute of Finance Management, Dar es Salaam Tanzania in 2011. Currently, she is supervising diploma students with proposal development and their research work. Her research interests are Data Science, Machine learning and STEM Education Schools.
Email: mambile30@gmail.com

Peter E. Mbogoro has been a professional lawyer registered under profession body goes by the name of the Tanganyika Law Society for three consecutive years. He was hired by the Tanzania Public Service College, the Tanga campus as a Tutorial Assistant (Law) back in the 2017, and now serving as Manager of Programs at the same college from 2019. He graduated with his Bachelor of laws (LLB) at Mzumbe University in 2015 and later on 2016/7 he joined post graduate studies at the Law School of Tanzania taking Post Graduate Diploma in Legal Practice (PGDL) and graduated with flying colours.
Email: peter.mbogoro@tpsc.go.tz