International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 6, Issue 1, pp 54-57, January-2022
https://doi.org/10.47001/IRJIET/2022.601011

Factors Affecting Cyber Security Awareness in Combating Cyber Crime in Kenyan Public Universities

[*1]M. K. Chizanga, [2]J. Agola, [3]A. Rodrigues

[1,2,3]Jaramogi Oginga Odinga University of Science and Technology, P.O. Box 210-40601, Bondo, Kenya
*Corresponding Author E-mail: mchizanga@jooust.ac.ke

***Abstract* - Over the years, cyber-based attacks have become widespread and are growing rapidly with the increasing use of technology. As a result, cyber security is best understood as a process designed to keep cyberspace safe from potentially known and unknown threats. Therefore, cyber security awareness is vital as it plays an important role in preventing these cyber attacks due to the increasing use of information and communication technologies (ICT) as well as e-learning platforms in universities. Therefore, the paper assesses the key factors influencing cyber security awareness in the fight against cybercrime in the context of Kenyan public universities. A survey tested academic staff from 31 public universities for the variable cyber security awareness, the variable cyber security self-perception, and the factors influencing cyber security awareness. The results show that a significant number of respondents do not have adequate cyber security training. The paper also highlights that most public universities do not have a mandated cyber security policy, as well as adequate infrastructure for ICT cyber security practices.**

Keywords: Cyber Security Awareness, Public Universities, Cyber Attacks, ICT.

I. INTRODUCTION

In the current information age, the dependence on institutions in cyberspace has increased [1]. It is widely believed that this advanced information technology age will have far-reaching consequences if it penetrates an institution's information system. This is because over the years cyber attacks have been reported on various platforms with increasing frequency [2]. Furthermore, it is emphasized that this infiltration into the information system of the institutions leads to a loss of data protection and a competitive advantage for the organization as well as the loss of the trust of the interest groups [3]. Hence, a number of institutions and governments around the world have invested heavily in ICT, implying the greatest importance of cyber security. This is because ICT has a significant impact on many sectors of the economy [4].

This also corresponds to the statement that various ICTs help to improve access to education, to strengthen the importance of education for the increasingly digital world of work and to increase the value of education, among other things by improving the quality of education [5]. It is also noted that the trend in cyber-attacks and information-related security breaches is similar in different countries. This is based on the premise that most cybercrimes are carried out to make a profit for the cybercriminals, but others to damage or destroy computers or networks, in order to spread malware and illegal information [17]. Universities, however, are one of the many institutions that rely heavily on information systems to provide university students with all the information they need. The availability of such technology with advanced computing environments, networks and applications is critical to today's online and offline educational processes and interactions, especially in times of the corona virus pandemic which required a reduction in classroom teaching. This is underlined by the idea that a number of students and academic staff can access unlimited amounts of information in order not only to broaden their learning and knowledge horizons, but also to complement their dynamic educational experiences [6]. However, it becomes difficult to keep them safe from malicious activity. As such, attackers could use malware and spyware to attack and not only damage the facility's reputation by also stealing the facilities' sensitive information, further exacerbating the digital and knowledge divisions [7]. The lack of management vigilance has exposed many information systems to security breaches, and universities in Kenya are no exception, according to experts pointing to the need for more effective security and a greater emphasis on higher education and research [8]. This is because a study found that e-learning readiness and awareness of information security remains a challenge in Kenyan educational institutions [9]. Hence, studying the factors influencing cyber security awareness in the fight against cybercrime in Kenyan public universities becomes crucial.

1.1 Objectives of the Paper

In line with the above mentioned, the motivation of the paper was to highlight through descriptive analysis, the factors

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 6, Issue 1, pp 54-57, January-2022

https://doi.org/10.47001/IRJIET/2022.601011

affecting cyber security awareness in combating cyber-crime in Kenyan public university context.

II. LITERATURE REVIEW

It is believed that numerous institutions are linked by information systems to enable faster dissemination of data for work, communication and study, a high risk of information security and cyber attacks for such organizations. Studies show, for example, that countries like Uganda, Kenya and Tanzania, to name but a few have faced organizational and institutional challenges due to the loss of critical information and the breach of private data [14]. Cyber-attacks on universities in Africa have been found in the past and in current literature to increase. This indicates the need for more effective security and a greater emphasis on university education and research. With such great concern, other scientists are of the opinion that the cyber-attacks on African universities are not a serious problem and are bundled as simple information technology problems. Thus, the increase in the number of cyber attack incidents is partly due to the availability of online information about the conduct of attacks.

However, some other studies related to the study conclude that a significant number of Kenyan higher education institutions have gone so far as to adopt and improve their information system security management [15]. This is to be achieved by regularly updating management for security updates. This is on the basis that training academic staff in information security management systems would help improves the management of information security systems of the institutions. Most of the research carried out also identified the main problems encountered in the management of information security systems, including user errors, software bugs, computer system theft, and viruses, to name a few [16] Information security awareness is not limited to specific countries, but is global Problem. Other studies show that, according to a survey of medium-sized and large companies in the United States, fewer than 50% of the workforces are employed [10].

In addition, other research carried out also shows that most American educational institutions are at high risk from cyber attacks and large numbers of students in high schools and colleges are involved in the heinous act of information security breach. This is based on the fact that the misuse of information systems has resulted in actual financial losses to institutions, negative publicity, reduced academic or organizational viability and competitive disadvantages [11]. In addition, other studies show that the vulnerability of institutions and organizations in the US is increasing due to the increasing use of e-commerce, increasing computer literacy, improved computer user complexity, and advanced software tools [11] [12].

III. METHODS AND MATERIALS

The paper utilized a positivist, quantitative research approach, while relying on both primary and secondary data acquired from surveys as well as published work that is related to the study. The study population consisted of academic staff (school deans and directors) from Kenyan public universities (n=305). Tara Yamane's formula to determine the study sample [18].

$$n = \frac{N}{1 + N(e)^2}$$

Purposive sampling was used in the study to ensure that only the deans and directors could participate in the study. After the survey was carried out, there was a response rate of 82% (143 participants) of the completed questionnaires. In the social sciences, a response rate of 50% is considered sufficient [13]. The questionnaire consisted of three different sections. In the first section there was the collection of the demographic information of the participants. The second section of the questionnaire consisted of 9 questions, mostly focused on respondents' awareness of cyber security measures. Section three of the questionnaire focuses on the factors influencing cyber security awareness and steps that need to be taken to address cyber security threats. This includes ICT infrastructure, resources and personnel, technical knowledge or skills in ICT, level of education, management support, programs and training courses to raise awareness of cyber security.

The questionnaire was analyzed using the Statistical Package for Social Science (SPSS) version 20 and descriptive statistics, which measure frequencies and percentages, were also used to present the research results. In addition, multiple regression analysis was used to test whether the independent variables have a statistically significant relationship to the selected dependent variables. This was done on the basis that a multiple regression model comprises several independent variables that are intended to predict a continuous outcome of the dependent variable [19].

IV. FINDINGS AND DISCUSSIONS

The findings are revealed and discussed below:

Demographics

The aim of the study was to examine the cyber security awareness of academic staff at Kenyan public universities. Therefore, the demographic results of the study are presented

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 6, Issue 1, pp 54-57, January-2022

https://doi.org/10.47001/IRJIET/2022.601011

to characterize the study accordingly. The study sample consisted of 75 (52.4%) men and 68 (47.6%) women. 83.2 percent of the study participants were between 46 and 75 years old. The smaller population of participants who were between 25 and 45 years old (16.8%). With regard to the distribution of the designation, this was evenly distributed among all public universities with 76 (53.1%) deaneries and 67 (46.9%) director positions. In terms of years of employment, a majority of 137 (95.8%) of the participants worked for more than 5 years, while a smaller group of the population 6 (4.2%) worked for less than 5 years. Additionally, 90 (62.5%) of academic staff said they had not received cyber security awareness training, with only 54 (37.5%) receiving the training.

Cyber security awareness

With regard to the topic of cyber security awareness, a significant proportion of the participants in the seminars and seminar forums, with a proportion of 24.3%, obtained information about cyber security, followed by universities and technical colleges (22.9%). However, the results suggest that the majority of respondents had learned about cyber security in the various roles they played. In addition, regarding the nature of the association between cyber security training and cyber security awareness, Table 1 shows that there is a positive and strong association between respondent training and cyber security awareness (r = 0.738). This relationship is statistically significant with a p-value of 0.051. Therefore, increased training will increase respondents' awareness of cyber security and thus reduce cybercrime.

Table 1: Symmetric Measures

			Value	Asymp. Error[a]	Std.Approx. T[b]	p-value
Nominal	by	Phi	.038			.048
Nominal		Cramer's V	.038			.048
Interval	by	Pearson's R	.038	.084	-.454	.651[c]
Interval						
Ordinal	by	Spearman Correlation	0.738	.084	-.454	.651[c]
Ordinal						
N of Valid Cases			143			

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.

c. Based on normal approximation.

Regression analysis

A standard multiple regression analysis was performed on the subject of various factors influencing cyber security awareness such as ICT infrastructure, technical skills, cyber security awareness programs, and training. In this case, cyber security awareness was used as the dependent variable and management support, ICT infrastructure, technical skills, cyber security policy and risk management, level of education, cyber awareness programs and training as predictor variables. From the model summary in Table 2 below, it is clear that the adjusted R2 is 0.565, which means that the combination of these independent variables accounts for 56.5% of the variation in cyber security awareness at designated public universities in Kenya.

Table 2: Model Summary

Model	R	R Square	Adjusted Square	RStd. Error of the Estimate
1	.793[a]	.637	.565	.48774

a. Predictors: (Constant), Management Support, ICT Infrastructure, Technical Skills, Cyber Security policy and risk management, Level of Training, Cyber Awareness Programs and Training, Human and Social Aspects of security and privacy

From the ANOVA results in Table 2 below, it can be seen that the standard general multiple regression model (the model with constants), Management Support, ICT Infrastructure, Technical Skills, Cyber security Policy and Risk Management, Education Level, Cyber Awareness Programs and Education, Human and Social Aspects of Security and privacy are very important for predicting how, management support, ICT infrastructure, technical skills, cyber security policy and risk management, level of education, cyber awareness programs and training, human and social aspects of security and data protection determine cyber security awareness at public universities in Kenya. The model achieves a high degree of adaptation, which is reflected in an R2 of 0.637 (F = 19.1; P = 0.002 <0.05). Hence, they are statistically significant.

Table 3: ANOVA[a]

Model		Sum Squares	ofdf	Mean Square	F	Sig.
1	Regression	1.256	6	.209	19.2	.002[b]
	Residual	32.353	136	.238		
	Total	33.608	142			

a. Dependent Variable: Cyber Security Awareness

b. Predictors: (Constant), Management Support, ICT Infrastructure, Technical Skills, Cyber Security policy and risk management, Level of Training, Cyber Awareness Programs and Training, Human and Social Aspects of security and privacy

V. CONCLUSION

In relation to the literature review, the paper concludes that factors influencing cyber security awareness in the fight against cybercrime in the context of Kenyan public universities include: management support of institutions, ICT infrastructure, technical capabilities of institutions, human and societal aspects of security and privacy, cyber security policy and risk management of the institutions, and the level of cyber

ISSN (online): 2581-3048
Volume 6, Issue 1, pp 54-57, January-2022
https://doi.org/10.47001/IRJIET/2022.601011

security education. In addition, the study found that most respondents did not know what a strong password is, how to protect personal information, whether personal information is used with malicious intent, how to securely store and access information. Most of the study participants say that they did not give much thought to the handling of sensitive data. After all, public universities in Kenya are expected to achieve effective information security and consequently to be able to fight cyber security attacks, which they employ appropriate information security and cyber security controls.

REFERENCES

[1] Strassmann, P. A. "Cyber security for the Department ofDefense."http://www.strassmann.com/pubs/dod/cybersecurity-draft-v1.pdf

[2] Chandarman, Rajesh, and Brett Van Niekerk. "Students' cybersecurity awareness at a private tertiary educational institution." *The African Journal of Information and Communication* 20 (2017): 133-155.

[3] Gaudin, Sharon. "TJ Maxx security breach costs soar to 10 times earlier estimate." *Information Week.* http://www.informationweek.com/shared/printableArticle.jhtml (2007).

[4] Carvalho, Joana, Rita Francisco, and Ana P. Relvas. "Family functioning and information and communication technologies: How do they relate? A literature review." *Computers in Human Behavior* 45 (2015): 99-108.

[5] Veletsianos, George, and Royce Kimmons. "Scholars in an increasingly open and digital world: How do education professors and students use Twitter?." *The Internet and Higher Education* 30 (2016): 1-10.

[6] Dunn, J. "The importance of internet access in schools." (2012). http://www.edudemic.com/the-importance-of-internet-access-in-schools/.

[7] Kiptalam, George Kibet, and Anthony Joachim Rodrigues. "Internet utilization: A case of connected rural and urban secondary schools in Kenya." *International journal of computing and ICT research* 4.1 (2010): 49-63.

[8] O'Brien, James A., and G. M. Marakas. "Developing business/IT solutions." *Management information systems* 488489 (2011): 74-89.

[9] Ojwang, Charles O. *E-learning readiness and e-learning adoption among public secondary schools in Kisumu County, Kenya*. Diss. 2012.

[10] Mbowe, Joseph Elias, et al. "A conceptual framework for threat assessment based on organization's information security policy." *Journal of Information Security* 5.04 (2014): 166.

[11] Knapp, Kenneth Joseph. *A Model of Managerial Effectiveness in Information Security: From grounded theory to empirical test*. Auburn University, 2005.

[12] Aloul, Fadi A. "The need for effective information security awareness." *Journal of advances in information technology* 3.3 (2012): 176-183.

[13] Idrus, A. B., and J. B. Newman. "Construction related factors influencing the choice of concrete floor systems." *Construction Management & Economics* 20.1 (2002): 13-19.

[14] Nfuka, Edephonce Ngemera, Camilius Sanga, and Maduhu Mshangi. "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* 3.2 (2014): 182-199.

[15] Nyamongo, D. M. "Information Systems Security Management A Case Study of Private Chartered Universities in Kenya." *Nairobi: Strathmore University* (2012).

[16] Ndeda, Laureen Akumu, and Odoyo, Collins Otieno "Cyber threats and cyber security in the Kenyan business context". *Global Scientific Journals*, 7.9 (2019): 576-582.

[17] Jethwani, Kanika, and G. Surbhi. "Cyber Crime: Issues and Challenges." *Delhi: International Journal of Emerging Research in Management &Technology* (2015).

[18] Sawatarat, Soirithai. "Attitudes of mobile phone users toward multimedia messaging service (MMS) in Thailand: a case study of I-Mobile soft company." (2003).

[19] Brown, Scott H. "Multiple linear regression analysis: a matrix approach with MATLAB." *Alabama Journal of Mathematics* 34 (2009): 1-3.

Citation of this Article:

M. K. Chizanga, J. Agola, A. Rodrigues, "Factors Affecting Cyber Security Awareness in Combating Cyber Crime in Kenyan Public Universities", Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 6, Issue 1, pp 54-57, January 2022. Article DOI https://doi.org/10.47001/IRJIET/2022.601011

****

