ISSN No:-2456-2165

The Role of Academia in Cyber Crimes Prevention

MUTIJIMA Asher Emmanuel

Abstract:- This paper discusses Cyber security which refers to the way data is protected and how IT infrastructure are protected from possible cyber threats and security breaches. There is lack of awareness of the cyber law, and lack of cooperation with law enforcement results into lack of real-time information on current trends in cyber space for the academia. Research objectives were to assess the role of academia in the prevention of cyber-crimes, to identify the determinants factor for academia to preventing cybercrime, and to provide a framework for cybercrime prevention. This research design was description in nature and used survey for data collected, however it also used secondary data from different sources. The target population was academicians and students at the University of Tourism Technology and Business studies being 522 and the yielded sample sized was 150. This research discusses the role of academia in cybercrime prevention and identifies considerable determinants of cybercrime prevention including cyber law awareness, ethical behaviors and digital literacy. Findings revealed that academia needs to ensure that all academicians and students are certified for digital literacy. This should be done in collaboration with law enforcement through awareness campaigns and cyber security students' clubs for cyber law for the students and academicians to know what the cyber law is and what is expected of them in compliance with the law.

Keywords:- *Cyber-crime, Digital literacy, Cyber law.*

I. INTRODUCTION AND BACKGROUND

The technology provides users with important benefits that can be cited in the light of serious security risks. (Biscay, 2017) Defines cybersecurity as information security, IT security, data security[1].

With a single click of a button, IT users might share information with across the world with individuals and organizations. Unfortunately, as described by (Igba , et al., 2018) with more things, more technologies there are, there will be more damages as result, technology might be when misused, or used with malicious intention with internet use. (Igba , et al., 2018) added that the risk is to users privacy, their files, their identity and their valuable bandwidth. As it is revealed, theses cybercrimes involve some level of cyber terrorism, data and identity theft, PC counterfeiting, chat rooms, crimes related to credit card, and relay server left open. Not forgetting to mention pornography and hacking that impacts on university students.(Igba , et al., 2018)

"Cyber security includes; Computer Security, Network Security, Internet / Communications Security, Application Security, Disaster Recovery, Business Continuity, Risk Management, Mobile Security, Internet of Things Security" (Biscay, 2017)

Academic Institutions Represented and Affiliated by the Partner in Prevention of Cybercrime through knowledge development and sharing; legislation and policy development; for the purposes of technology and technical standards; the technical assistance delivery; and cooperation with law enforcement agencies. (Steven, et al., 2013)

In the perspective of Knowledge development and sharing, academic institutions have needs to establish specialized educational programs, training centres and curriculums to consolidate research and knowledge, also synergies increase in knowledge across disciplines and different fields of study.

The question of cybercrime is a worrying one, which is why many authors concerned have greatly reinforced the situation, cybercrime being an omnipresent phenomenon which hides in the face of the development of each nation. Cybercrime has come as a surprise and a strange phenomenon that for now lives with us in Nigeria. Every passing day, the society is on alert of cases of cyber-crimes in Nigeria, in the middle of each new case more shocking than the previous one.(Igba , et al., 2018)

According to (Steven, et al., 2013), an increasing number of universities offer degrees, certificates, and professional education in topics related to cyber security and cybercrime to educate young adults and future professionals about safe computing practices and technical subjects.

In Rwanda, some higher learning institutions to promote applied learning and relevant development of anti-cybercrime social networks through the organization of conferences and workshops. These types of activities offer possibilities for exchanging information and advice on prevention and intervention measures, establishing informal cooperation, mechanisms for informing specific actions and for solutions that are technical.

Over the past two decades, the number of academic journals on cyberspace, cybersecurity and cybercrime has increased significantly. Awareness and research on related issues has resulted in an increasing number of technical reports, peer-reviewed research and publications, analysis

[1]I.Nsude, "cybercrime, A hidden danger of information communication technology (ICTS) in the 21st century: The case of Nigeria," The Nigeria Journal of Communication (1&2) 2005 Enugu Precision publisher limited

of agency data and exclusive unpublished work of researchers. (Steven, et al., 2013)

Looking at cybercrime prevention in Legislation and policy development perspective, we realize that University experts provide a meaningful contribution to the related development and most likely amendment of legislation and policy. At the national and international level, academics provide the best legal advice and draft legislation on a range of topics such as criminalization, confidentiality and privacy, and legal protections. This advice from academics is provided through a mechanism, including participation in groups for advisory and special groups and individual contracts, as well as through technical assistance programs. In higher learning institutions cyber research unite serves as coordinators of exercises of specialized researchers within some work areas related to awareness of cybercrimes.

Universities do contribute in one way or another to computer forensics, evidentiary and data analyses. In addition, universities also represent relevant partners and facilitators of cooperation for cybercrime prevention through active participation in professional and standards organizations not forgetting to mention technical working groups. Other national cybersecurity strategies do mention the role of higher learning institutions in efforts to securing cyberspace.

According to (Steven, et al., 2013), Higher learning institutions' technical assistance programs in the area of cybercrime are often developed and delivered to national and international law enforcement, criminal justice and national security agencies. Universities provide technical assistance programs to businesses, small and medium-sized enterprises, and other academic institutions. These programs cover many important areas of investigative methods, evidence gathering and digital forensics; malware analysis content analysis (other than forensics); policy, governance and compliance; drafting and amending legislation and supporting prosecution and judicial proceedings.[2]

"In conjunction with knowledge development and technical assistance activities, a few universities have developed special educational programs, for example, in cybercrime investigations and digital forensics, to which police and governmental authorities formally second their employees as students."(Steven, et al., 2013)

Law enforcement agencies can consider incentives to actively cooperate with higher learning institutions due to their expertise in cybercrime and cybersecurity. University academicians find it easy to cooperate with law enforcement agencies in knowledge development, technical assistance and standards.

[2] Other topics include international cooperation, transnational organized crime, general telecommunications and technology, and prevention issues.

➢ *Problem statement*

Academia contribute in cybercrime prevention by educating citizens on cyber space and secure use of internet, however, there is lack for resources, openness and awareness of the law, and not forgetting to mention more applied research conducted by academia.

Inconsistent cooperation with law enforcement results into lack of real-time information on current trends in cyber space for the academia therefore making little room for academia to contribute in the cybercrime prevention.

➢ *Objectives of the study*

- To study the role of academia in cybercrime prevention
- To assess the impact of cyber law awareness in the prevention of cyber-crimes
- To identify the effect of ethical behavior on preventing cybercrime
- To examine the contribution of digital literacy in cybercrime prevention

➢ *Hypothesis*

H1: There is a positive relationship between cyber law awareness and cybercrime prevention
H2: There is a significant relationship between ethical behaviors and cybercrime prevention
H3: There is a positive relationship between digital literacy and cybercrime prevention

II. LITERATURE REVIEW

➢ *Academia in cyber-crimes' prevention*

In an interview at cyber security summit 2019 with (Tim Watson, 2019) when asked about the role of information sharing between academia, industry and government, given the importance of co-operation and co-ordination in combating cybercrime. While Tim agrees that information sharing is important, he emphasized that it is not a solution in of itself, and there is no problem where information sharing alone can provide the answer. Tim said that while it was difficult at times for, in particular industrial partners to share information comprehensively due to its potentially sensitive nature, there is a significant willingness within the industry to share as much as possible – the challenge lies in balancing the protection of information with the benefits of open academia research and publishing.

The role of academia bodies in Cyber Security is developing cutting-edge solutions and conducting research for the ever-changing nature of cyberspace where cybercrimes occurs and that cannot be understated.

➢ *Technical assistance for cybercrime prevention*

According to (Steven, et al., 2013), University technical programs in the field of cybercrime and cyber security are often designed for and provided to national and international law enforcement agents, national security agencies and criminal justice. Universities also provide technical assistance programs to corporates, SMEs, and to other educational institutions. These technical programs

ISSN No:-2456-2165

cover a range of substantive fields related to investigation techniques, preservation of evidence and digital forensics; analysis of malware, analysis of content; governance, policy, compliance; amendment and drafting of legislation, trial support and prosecution.

(Steven, et al., 2013) Argued that in conjunction with technical assistance activities and knowledge development, only fewer universities have developed dedicated educational programs, whose example include; digital forensics and cybercrime investigations, to which governmental and police authorities considers their employees as students.

➢ *Conceptual framework*

Independent variables	Dependent variable
Cyber Law awareness	Cybercrime prevention
Ethical behavior	
Digital literacy	

Table 1

III. RESEARCH METHODOLOGY

➢ *Design, and data collection*

Research methodology is defined according to (Kothari, 2004) as a scientific and systematic search for pertinent information on a specific topic. He also described the purpose of research as to discover questions' answers through application of scientific Procedures.

Researcher adopted descriptive design whereby he used secondary data to improve the meaning of primary data identified as relevant to this study. This secondary data were collected from a variety of sources ranging from online sources and other publications availed to the researcher. Researcher collected data with a questionnaires as data collection instruments and formed qualitative questions with to gather feedback and recommendation from respondents on current trend in regards with cybercrime preventions in academia.

➢ *Target population sampling*

The target population from which a sample size was retried, consisted of academicians, university students. The total population was 522 individuals with relevant characteristics to this study.

The sample size consisted of individuals who are anyhow involved by cybercrime prevention in the University of Tourism Technology and Business studies, Rwanda. The sample size was 150 participants for the survey.

➢ *Results and discussion of the findings*

Findings below describe the distribution of participants' demographic

ITEM	DESCRIPTION	PERCENTAGE
Gender	Male	40%
	Female	60%
Age	19-39	42%
Marital status	Single	78.%
Education	Undergraduate	46%
Nationality	Rwandan	43%

Table 2:- Demographic description of participants

Researcher used descriptive analysis in this study to enable respondents answering questions, Likert scale measure with the options ranging from 1 to 5 whereby 1 for strongly disagree to 5 for strongly disagree.

DEPENDENT VARIABLE	MEAN	STANDARD DEVIATION
Cybercrime prevention	20.16	6.01
INDEPENDENT VARIABLES	**MEAN**	**STANDARD DEVIATION**
Cyber law awareness	23.04	7.912
Ethical behavior	17.21	7.124
Digital literacy	25.94	9.334

Table 3:- Descriptive analysis

The above findings vividly reveals that digital literacy has the highest mean value of 25.94 and the second highest mean being cyber law awareness with value of 23.04 amongst academicians and university students.

Findings imply that a lot need to be done to ensure that all academicians and students are certified for digital literacy and university in collaboration with law enforcement (RIB for the case of Rwanda) needs to conduct a lot of awareness campaign for cyber law for the students and academicians to know what is the cyber law and what is expected of them in compliance with the law.

DEPENDENT VARIABLE	**Alpha Value**
Cybercrime prevention	0.757
INDEPENDENT VARIABLES	**Alpha Value**
Cyber law awareness	0.967
Ethical behavior	0.954
Digital literacy	0.958

Table 4:- Reliability Testing

Findings illustrated above for the reliability of variables (both independent and dependent) are beyond 0.70 and it highlights that the value is identified as consistent and very stable. The variable with the highest value is cyber law awareness $\alpha = 0.967$ while the variable with the lowest value is ethical behavior with $\alpha = 0.954$.

		Cybercrime prevention	**Cyber law awareness**	**Ethical behavior**	**Digital literacy**
Pearson correlation P<0.001**	Cybercrime prevention	1.000			
	Cyber law awareness	0.976	1.000		
	Ethical behavior	0.877**		1.000	
	Digital literacy	0.945**			1.000

Table 5:- Correlation testing

According to Pearson correlation, a 1 means that variables are undeniably correlated. The table above, the entry of the correlation matrix whereby cybercrime prevention column and cyber law awareness row meet is the number .976. This is Pearson correlation amidst cybercrime prevention and cyber law awareness.

Independent variables	**Cybercrime prevention**					
	Standard coefficients Beta	R^2	Adjusted R^2	Sig. F change	F change	Durbin-Watson
Cyber law awareness	0.976	0.934	0.933	0.000	2084.957	0.414
Ethical behavior	0.877	0.902	0.902	0.000	1449.329	0.537
Digital literacy	0.945	0.897	0.896	0.000	708.231	0.172

Table 6:- regression analysis

Above data showed that the highest standard coefficient is cyber law awareness variable with the value of 0.934. The Standard Coefficient for cyber law awareness is ($\beta = 0.976$ ($p<0.01$), and has the greatest contribution equal to 96.6% to the variance in cybercrime preventing. Instead, the standard coefficient for variable digital literacy is only equal to ($\beta = 0.877$ ($p<0.01$), which has a relatively small with a contribution of only 8.8% of the variance commitment to cybercrime prevention. Durbin-Watson values are between 0.172 and 0.537 then have to prove that there is no autocorrelation as the value is in the range of 1.50 to 2.50. During this test, ($R^2 = 0.934$) whereby the value of (R2) was closer to 1.0 means the percentage contributed by the researcher is more accurate. This implies a 93.4% variation (R2) can be explained or be accounted by the variable of cyber awareness. Basing on significant value of $F = 0.000$ $P <0.01$ then the hypotheses H1, H2, H3 are acceptable and valid.

➢ *Results of hypothesis test*

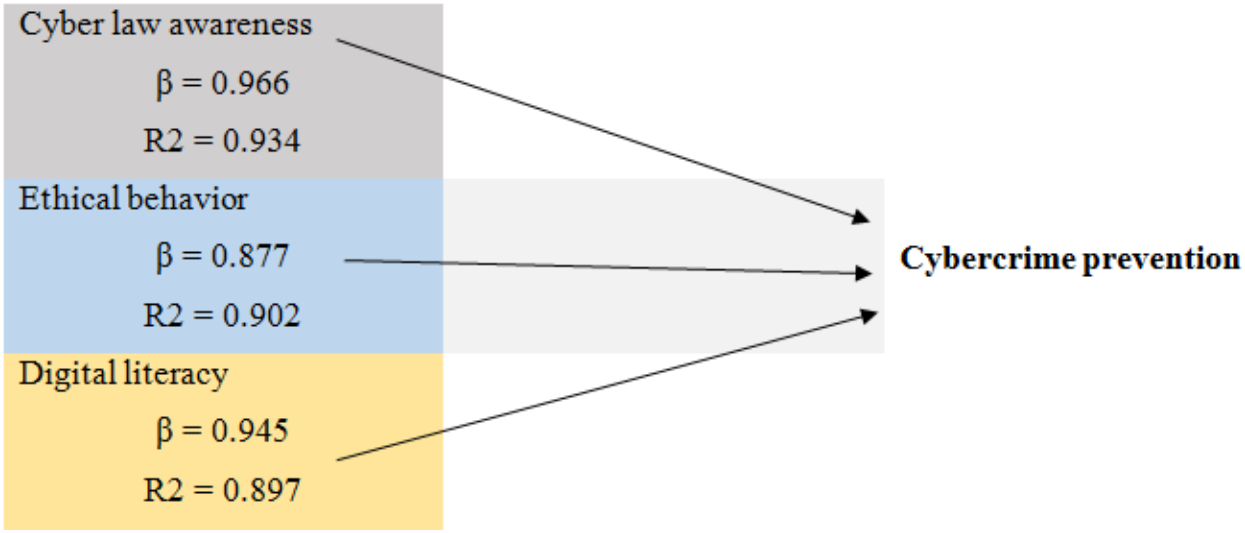

Fig 1

To serve the objective one, positive results yielded in hypothesis1that there is a positive relationship between cybercrime prevention against cyber law awareness (β = 0.966 (p < 0.01) where contributions shown by the independent variable is 94.60% of variance cyber law awareness among academicians and university students. To serve the objective two significant results yielded in hypothesis2 that there is a positive relationship between cybercrime prevention and ethical behaviors (β = 0.953 (p < 0.01) where contributions shown by the independent variableis95.30% of variance ethical behaviors among academicians and university., Hypothesis 3 yielded results revealed that there is a positive relationship between cybercrime prevention against digital literacy (β = 0.909 (p < 0.01) where contributions shown by the independent variable is 90.9% of variance digital literacy among academicians and university students. The later served the objective number three.

➢ *Determinants factors for cybercrime prevention*

- *Cyber law awareness*

From the survey conducted, 76% of the respondent revealed that they don't know about the newly published cyber therefore they tend to commit or find themselves involved in cyber-crimes without the intention due to the ignorance which is results of not knowing the cyber law. 65% of the respondent suggested that law enforcement agencies should conduct cyber law awareness campaign as much it is required to educate on the citizens especially the academic community of the cybercrime and how to stay safe while in cyber space.

- *Ethical behaviors*

From the survey done, 67% of the respondents revealed the existence of a good ethics while doing online education (e-learning) online business and online financial transaction should be addressed by academicians first as to speed up awareness on cybercrime prevention.

- *Digital literacy*

Digital Literacy is referred to as the ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and technical skills at a basic level.

78% of the respondent mentioned stated that is irrelevant to mention cybercrime to digital illiterate citizens. 90% recommended that universities and academia as a whole should encourage and promote digital literacy amongst the academic community which is most likely to results into safe use of cyber space and minimized cyber-crimes.

IV. RECOMMENDATION AND CONCLUSION

This research discussed the role of academia in cybercrime prevention and identifies considerable determinants of cybercrime prevention including cyber law awareness, ethical behaviors and digital literacy. At the university of Tourism Technology and Business studies digital literacy through ICDL certification program is integrated in the teaching curriculum with top priority so as to maximize chance of producing digital literate graduates who can facilitate in educating the rest of Rwandan citizen on cybercrime prevention. However, much needs to be done to raise awareness of the national cyber law is only known by the few 34% of the selected sample representing the entire population.

Findings revealed that university of Tourism Technology and Business studies needs to ensure that all academicians and students are certified for digital literacy. This should be done in collaboration with law enforcement (RIB for the case of Rwanda) through awareness campaigns and cyber security students' clubs for cyber law for the students and academicians to know what the cyber law is and what is expected of them in compliance with the law.

No one can deny that online environment can't and might never be clear of cybercrimes due to the uniqueness of Internet's architecture.(Ali, 2016)

REFERENCES

[1]. Ali, M. M. (2016). Determinants of Preventing Cyber Crime: a Survey Research. *International Journal of Management Science and Business Administration*.
[2]. Biscay, K. (2017). *Cybercrime and Academia: Current Trends.*
[3]. Igba , D., Chimezie Igba, E., Sunday Nwambam, A., Chijioke Nnaman, S., Egbe U., E., & Ogodo V. , J. (2018). Cybercrime among University Undergraduates: Implications on their Academic Achievement . *International Journal of Applied Engineering Research*.
[4]. Kothari, C. (2004). *Research methodology: methods and techniques.* New Age International Publishers.
[5]. Steven, M., Robyn, M., Anika, H., Cameron , B., Stefan , K., & Eva , I. (2013). *Comprehensive Study on cyber crime.* New York: UNITED NATIONS OFFICE ON DRUGS AND CRIME.
[6]. Tim Watson. (2019). Recognising-academia-cyber-security. (C. insider, Interviewer)