International Journal of Computer Trends and Technology
ISSN: 2231-2803/ https://doi.org/10.14445/22312803/IJCTT-V70I2P106

Volume 68 Issue 7, 37-42, July 2020

Original Article

Constraints in Prevention of Cybercrime in Public Cybercafés in Kisumu City

Vivian Anyango Oloo[1], George Raburu[2] and Michael Oduor Okoya[3]

[1]*School of Computing and Informatics, Maseno University, Private Bag, Maseno, Kenya*
[2,3] *Jaramogi Oginga Odinga University of Science and Technology (JOOUST), P. O. Box 210-40601 Bondo, Kenya*

Received Date: 23 May 2020
Revised Date: 11 July 2020
Accepted Date: 14 July 2020

Abstract *- The World Wide Web or internet has gained exponential growth and popularity, bringing people closer together by creating virtual cyberspace communities during the last three decades. Undoubtedly, the internet has also revolutionised life in the developing world, including Kenya, where cash transfers and various forms of data files are extensively exchanged. On the contrary, insecurity in the internet systems or cyber insecurity has concomitantly grown, resulting in risks and disasters that are technologically oriented. The Cybersecurity Report shows that Kenya lost Sh21.1 billion to cybercrime in 2017, a 40 per cent increase from Sh15.1 billion in 2015. Although security measures such as Simcard registration and control of Internet Protocol (IP) have been initiated in public cybercafés, the little effect seems to have been achieved with scanty information available with regards to constraining factors. The purpose of this study was to explore factors constraining the prevention of cybercrime among public cybercafés in Kisumu City. Specific objectives were to: assess the infrastructure among public cybercafes and to assess the factors constraining the prevention of cybercrime among cybercafés. The cross-sectional survey design was employed on a sample of 48 attendants from randomly selected 18 cybercafés operating in the city. A questionnaire was used for data collection, while descriptive statistics were used for data analysis. Findings revealed that there is inadequate infrastructure to aid identification and monitoring of cybercrime, coupled with few and untrained attendants in the public cybercafés in Kisumu City. The major constraints affecting cybercrime prevention were lack of awareness and education on cybercrime detection and prevention, inadequate training, non-reporting of cybercrime to relevant authorities, low awareness of government policies and poor infrastructure, as evidenced by a low number of internet access points and cyber attendants within the cybercafés. The study recommends that thorough awareness and education on cyber security be launched by stakeholders to curb this menace.*

Keywords *- Cyber Crimes, cybercafes, infrastructure, prevention constraints, cyber security.*

I. INTRODUCTION

The introduction, growth, and utilization of information and communication technologies (ICTs) during the last three decades have been accompanied by an increase in criminal activities. One of the criminal activities that transcend territorial boundaries is cybercrime. Cybercrime is a range of illegal digital activities targeted at organizations in order to cause harm (KPMG, 2014). Ali (2016) defined cybercrime as any criminal activity that uses a computer either as an instrument, target or a means for perpetuating further crimes or offences or contraventions under any law.

According to Norton (2015) and Priya (2016), for every three seconds, someone's identity is stolen as a result of cybercrime. PricewaterhouseCoopers (PwC, 2011) asserts that cyber-crime is reported as one of the top four economic crimes perceived by all organizations, with the number of criminal cases set to reach a high-level worldwide by 2022. Lakshmanan (2019) argues that a major factor constraining war against cyber-crime is the fact that the act does not have territorial barriers. In turn, prevention strategies and implementation have been slow amongst businesses. The losses caused by cybercrimes can damage both the finances and the reputation of businesses (Vahdati and Yasini, 2015). These crimes and resulting fears also discourage many customers from buying goods online. Spanaki et al. (2019) and Tsohou and Holtkamp (2018) identified major challenges faced by consumers when they become victims of cybercrimes. These consumers faced issues such as credit problems (including rejection of loan applications), disruption to normal life routines and psychological difficulty in providing personal data to organisations and banks during an investigation.

A. Statement of the Problem

The contribution of the internet to the development of the nation has been marred by the evolution of new waves of crime. The internet has also become an environment where the most lucrative and safest crime thrives. Cybercrime has become a global threat from Europe to America, Africa to Asia. Cybercrime has come as a surprise and a strange phenomenon that has come with devastating consequences. Although measures such as

CCTV monitoring, registration of Simcard, and control of Internet Protocol (IP) has been initiated, minimum favourable outcomes seem to have been realized, particularly in the developing world, including Kenya. Ranking third regionally and forty fifths globally, Kenya lost over 21 billion shillings to cybercrime in 2017 alone, with most cases emanating from public cybercafés. The study, therefore, sought to establish factors that hinder the prevention of cybercrime in Kenya, taking Kisumu city as a case.

B. Objectives

- To assess the state of cybercafe infrastructure among public cybercafes' in Kisumu City, Kenya.
- To explore factors that constrain the prevention of cybercrime among public cybercafés in Kisumu City, Kenya.

II. LITERATURE REVIEW

Literature on the prevalence of cybercrime has been widely documented. However, the perspective of cybercafes has not been adequately documented compared to other sectors such as financial institutions, governments, and internal security, among others. Ali (2016) carried out a study with the aim of identifying the determinants factor for preventing cyber-crime to the online business entrepreneur in Malaysia. The research assessed factors such as law enforcement, awareness program, and prevention process in combating cybercrime issues. A survey was conducted, and the questionnaires were distributed to the respondents, who were mainly online entrepreneurs. Based on the result of this research, we found a positive relationship between preventing cyber-crime against law enforcement, attitude awareness, ethics, and IT Technology were found.

Van Niekerk (2017) conducted a high-level analysis of "newsworthy" cyber-incidents that affected South Africa. The 54 incidents that were considered were categorised according to impact type, perpetrator type, and victim type, and the trends were assessed. It was found that the most common impact type was data exposure, which was also one that had increased noticeably in recent years. The most prevalent perpetrator type was found to be hacktivists, which had also exhibited a recent increase in inactivity. A particularly concerning trend was the recent high number of incidents of data exposure caused by error, a trend running contrary to the drive to improve cybersecurity. It was also found that of the incidents considered, 54% targeted state-owned or political entities as victims. In general, the results appeared consistent with global reported trends.

Chiroma et al. (2011) investigated the contribution of academic community cybercafés in perpetrating cybercrime. Four hundred (400) questionnaires were distributed among academic staff, non-teaching staff and students in four (4) higher institutions of learning in Gombe state, located in the northeastern part of Nigeria. The results obtained show there is a significant difference in perception of academic staff, non–teaching staff and students in perpetrating cybercrimes in academic community cyber caf´es. The perception of the three variables on perpetrating phishing, credit card fraud, cyberpiracy, virus dissemination, hacking and cyber plagiarism was equal.

A study done in Kenya by Ajayi (2016) established that it is not as if relevant laws and regulations are not in place because some advanced nations in the world have, in one form or another, laws against cybercrimes, yet, the challenge of cybercrimes remains intractable and bewildering. As nations across the globe strive to curb cybercrimes through the instrumentality of the law, so are the cybercriminals devising new and sophisticated techniques to further their trade, thereby rendering impotent the extant legal measures

III. MATERIALS AND METHODS

A. Research Design

The study employed a cross-sectional survey design which allows the collection of information from a population with the purpose of making inferences about the targeted group in a more objective way (Kombo&Tromp, 2006). This type of study is carried out at a single point in time which makes it suitable for this work; it does not involve manipulation of variables and allows the researcher to look at numerous things at once. This design was used to administer questionnaires to the respondent, who were cyber operators and cybercafé attendants of public cybercafés in Kisumu city.

B. Population

The target population is comprised of cybercafé operators and attendants of public cybercafés. The cyber operators were proprietors or someone in charge of the cyber café. On the other hand, attendants were people who were employed or worked in the cybercafés.

C. Sampling Procedure and Sample size

The study used purposive and simple random sampling techniques to select the sample. Purposive sampling was used to identify cybercafés where the study was to be conducted. On the other hand, simple random sampling was used to select the cybercafés to be studied. The technique was selected based on its suitability to select a sample without bias from the target population (Oso & Onen, 2011).

The sample size used was forty-eight (48) respondents, which were obtained from the eighteen (18) cybercafés out of the twenty-four (24) that were identified through purposive sampling. The eighteen (18) cybercafés were then randomly selected for study based on the estates. All the cyber operators and attendants in the selected cybercafés were interviewed. Some cybercafés had one,

two or more than two attendants; the total number of respondents obtained was forty-eight (48). Table 1 presents the distribution of cybercafés.

Table 1. Percentage distribution of public cybercafés by estate

Estate	Frequency (No. of Cybercafés visited)	Percentage
Kisumu CBD	5	27.8%
Nyalenda	2	11.1%
Polyview	2	11.1%
Kondele	4	22.2%
Manyatta	3	16.7%
Migosi	2	11.1%
Total	**18**	**100%**

D. Data Collection Instruments

Semi-structured questionnaires were used as the main tools for collecting primary data, while secondary data was captured through literature review. Interviews were used for this study to collect qualitative data. The selection of data collection tools was guided by the nature of the data to be collected, the time available as well as the objectives of the study. Since this study was a survey, questionnaires and interviews were the most suited tools for data collection as the study was mainly concerned with views, opinions, feelings, perceptions and attitudes, information which can be best collected through these tools (Kavulya, 2005; Bell 1993; Touliatos& Compton, 1998). This view is also supported by Touliatos and Compton (1998), who concur that where variables cannot be directly observed, such as views, opinions, perceptions and feelings of respondents, questionnaires are appropriate for data collection. Furthermore, the target population was largely literate and therefore unlikely to have difficulties responding to questionnaire items.

IV. DATA ANALYSIS

The quantitative data that was collected was subjected to descriptive analyses to come up with descriptive statistics especially mean, frequency and percentages. These statistics were vital for the assessment of the dimensions of characteristics of variables under investigation (Saunders, Lewis and Thornhill, 2009). The data was edited, cleaned and analyzed using Statistical Package for Social Scientists (SPSS 15) and Microsoft Excel 2007. The results were then presented in the form of percentages, pie-charts, bar-charts and tables, while interpretation was made by the researcher, taking into account the findings and already existing literature review.

V. FINDINGS AND DISCUSSIONS

The objective of the study was to investigate constraints experienced in the prevention of cybercrime in public cyber cafés in Kisumu city. The variables considered in assessing the objective were: infrastructure, education of cyber operators and attendants, government policies and legislation, among others.

A. Infrastructure

Infrastructure refers to the physical facilities or equipment and the software used in the public cybercafés. This includes the devices that are used to access the internet, devices used to identify or detect users of particular machines, devices used to secure the computer systems and software such as packet tracers, firewalls, spam filters and also the personnel in the public cybercafés.

B. Number of Public Cybercafé Attendants

A cybercafé attendant is any person that works in the public cybercafé. They range from those working at the printing pools, assisting or attending to clients in the cybercafé, cleaners, typists and the person in charge of the cybercafé.

Most cybercafés visited had 1 to 2 attendants, as indicated in figure 1, meaning that they clean, operate the printing pool, attend to clients, and also manage the cybercafé. This scenario presents a very busy attendant who hardly has time to carry out his duty efficiently. At the same time, due to the ever-evolving nature of the ICT world, the attendant is expected to be technology savvy by keeping abreast with advances in technology in order to serve all manner of clients and also monitor clients and their activities in the cybercafé. This finding paints a picture whereby physical monitoring of activities within the public cybercafés, as was the case in most of them, remains a challenge hence making them vulnerable to cybercrime. This is because the operators may be so busy that they do not have time to advance their knowledge and skills in cybercrime prevention in public cybercafés. Ajayi (2016) also concurs with this finding and maintains that perpetrators of cybercrimes are usually not easily identified due to challenges of identification. Given this challenge, physical monitoring and identification can only be successful where more attendants are deployed to monitor clients and their activities, and such attendants are able to advance their ICT knowledge on new cyber security measures from time to time.

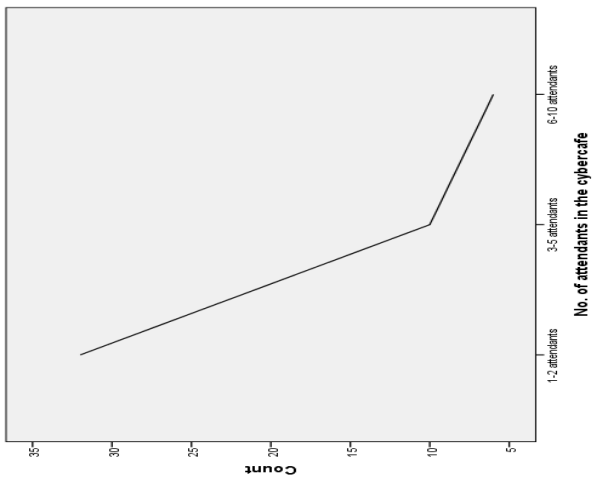

Fig. 1 Number of attendants and operators in cybercafés

C. Usable Internet Access Points

When respondents were asked about the number of internet access points in their cybercafés in table 5, the findings reveal that most of the sampled cybercafés had between 1 to 5 internet access points 41.7%, followed by 6 to 10 internet access points 37.5% and cumulatively those cybercafés with 1 to 10 access points represent more than three-quarters of these cybercafés 79.2%.

The low number of access points in most public cybercafés in Kisumu means that the operators do not invest adequately in the business and, as a result, explain why most cybercafés do not have cybercrime preventive measures in place. The lack of sufficient resources to purchase equipment and applications necessary to collect evidence and also applications and instruments to detect and prevent such crime from happening are quite limited. A key component in the fight against cybercrime in public cybercafés is an improvement of the infrastructure; however, most cybercafés do not prioritize cybercafé security. Van Niekerk (2017) summarizes that the norm is business first, security later.

These findings are in agreement with Tsohou and Holtkamp (2018), who asserts that users of public cybercafés face serious information security challenges as information security in cybercafé are not taken into serious consideration by cybercafé owners. Although cybercafé owners play a role in increasing the freedom of customers to use the internet, they do not improve their computer security to protect customer information from hackers and malicious damage. It can therefore be suggested, based on these findings, that the infrastructure of most cybercafés in Kisumu city needs to be improved in order to ensure cyber security in public cybercafés.

Table 2. Number of internet access points

		Frequency	Percentage	Cumulative Percentage
Number of an internet access point	**1-5 access**	20	41.7	41.7
	6-10 access	18	37.5	79.2
	above 10	10	20.8	100.0

D. Level of Education of Respondents

The study unearthed that out of the sampled cyber operators in table 3, more than three quarters had tertiary and university education 79.2% while a paltry 20.8% had a secondary level of education .see Table 3.

		Frequency	Percentage	Cumulative Percent
Level of Education	Secondary	10	20.8	20.8
	college/university	38	79.2	100.0

However, this finding concurs with Chiroma et al. (2011), who assert that even information technology professionals lack skills and interest in cybercrime prevention. The fight against cybercrime should therefore entail training and retraining of cyber operators and attendants to enable them to detect and put in place adequate cybercrime preventive measures. Perhaps, this scenario explains why most public cybercafés do not operate beyond five years because, by this time, most of the operators may have acquired formal employment and left the business. This trend is rather undesirable because the business or industry does not get to overcome or develop strategies to curb the challenges facing it.

E. Awareness of Government Policies on Cybercrime

A good majority of the cyber operators, 87.5%, indicated an absence or lack of knowledge of any government policy in dealing with cybercrime. Only 12.5% affirmed that surely the government had a policy dealing with cybercrime, as shown in table 4.

F. Government Policies on Cybercrime

The study explored the awareness of respondents on government policy for handling cybercrime, as shown in figure 2. The results show that about 65% of the respondents were aware of the existence of national cyber security policy, whereas 30% mentioned charging cybercriminals in a court of law; especially the recent charging of Chinese cybercriminals in court in Nairobi, Kenya, which appeared in the local dallies as a case in point.

Table 4. Awareness of government policies

		Percent	Cumulative Percent
Awareness of government policy on cybercrime	Yes	12.5	12.5
	No	87.5	100.0

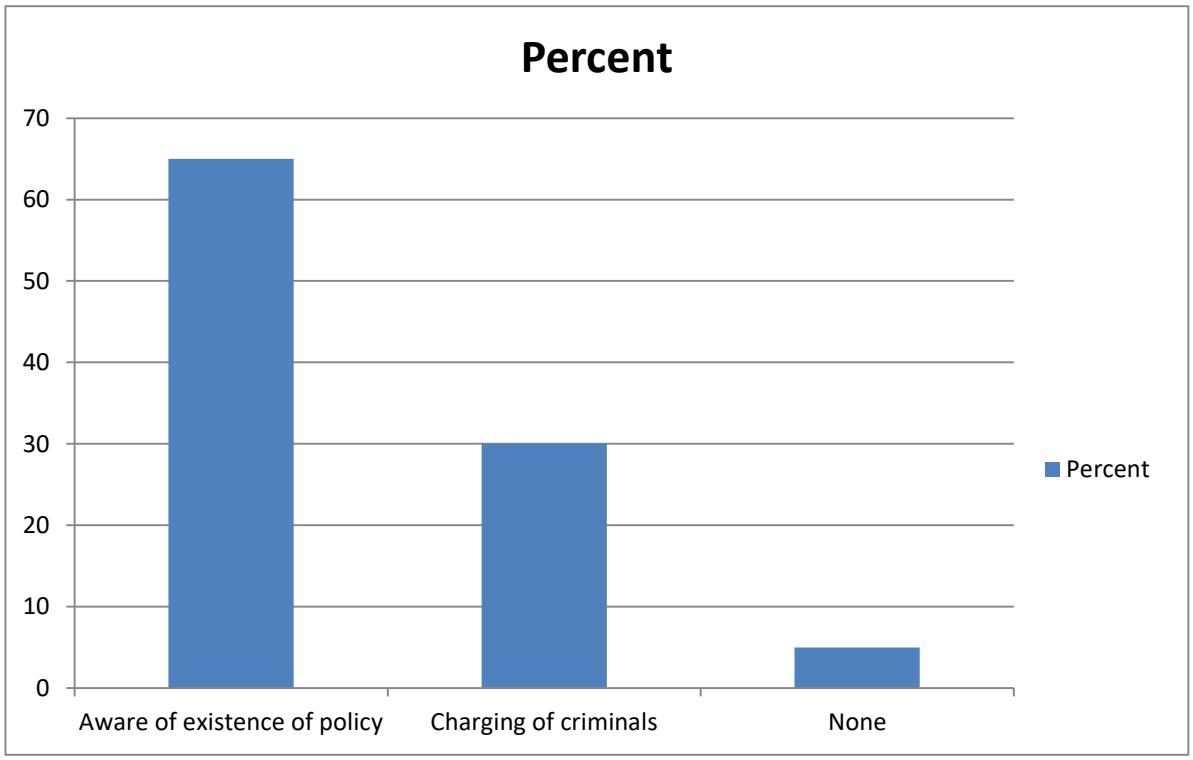

Fig. 2 Awareness of the existence of cybercrime policy

VI. CONCLUSION AND RECOMMENDATIONS

The researcher concludes that the schedule of cybercafé attendants allows little time for efficiency. The attendants are also not ICT knowledgeable to effectively monitor clients and their activities in the cybercafé. It is additionally concluded that there is inadequacy in ICT infrastructure to support the employment of cybercrime prevention measures. Finally, the cybercafé attendants are not aware of the requirements of cybercrime policy, although most of them have noted the application of cybercrime laws through the arraignment of offenders in court.

It is recommended that physical monitoring and identification should be enhanced through employment and deployment of more attendants to monitor clients and their activities. It is also recommended that cybercafé attendants should be adequately trained on the identification of cybercrime as well as on new cyber security measures from time to time. The authorities should also strengthen cyber security policies by including punitive penalties on offenders.

ACKNOWLEDGEMENT

My sincere gratitude goes to the cybercafé attendants for their very resourceful and special insights into the study. Many thanks also go to cybercafé owners for assisting me with the necessary data for this study.

REFERENCES

[1] Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy .Journal of internet and information systems, 6(1) (2016). 1 – 12.

[2] Determinants of Preventing Cyber Crime: a Survey Research. International Journal of Management Science and Business Administration, 2 (7), 16-24.

[3] Chiroma, H., Abdulhamid, S.M., Gital, A.Y., Usman, A.M., and Maigari, T.U. (2011). Academic Community Cyber Caf´es - A Perpetration Point for Cyber Crimes in Nigeria. Information Sciences and Computer Engineering, 2 (2), 7–13.

[4] Lakshmanan, A. Literature review on Cyber Crimes and its Prevention Mechanisms. Technical Report. (2019). Research Gate: DOI:10.13140/RG.2.2.16573.51684, https://www.researchgate.net/publication/331010726.

[5] Lutta, V. O. and Obiri, J. F. Cyber Crime a Rising Threat for Internet-Based Businesses in Western Region, Kenya. International Journal of Scientific & Engineering Research, 6, (3) (2015).

[6] Oso, Y.W., & Onen, D General Guide for Writing Research Proposal and Report.A handbook for beginning Researchers. Options Press and Publishers, (2011).

[7] Kisumu PricewaterhouseCoopers . Economic Crime Survey India Report, (2011).

[8] Tsohou, A. and Holtkamp, P. Are users competent to comply with information security policies? An analysis of professional competence models. Information Technology & People, 31 (5) (2018). 1047-1068.

[9] Spanaki,K., Gürgüç, Z., Mulligan, C. and Lupu, E., Organizational cloud security and control: a proactive approach. Information Technology & People, 32(3) (2019). 516-537.

[10] Vahdati, S. and Yasini, N., Factors affecting internet frauds in the private sector: a case study in cyberspace surveillance and scam monitoring agency of Iran, Computers in Human Behavior, 51 (A) (2015). 180-187.

[11] Van Niekerk, B. An analysis of cyber-incidents in South Africa.The AfricanJournal of Information and Communication (AJIC), 20 (2017). 113-132.