Cyber Crime a Rising Threat for Internet - Based Businesses in Western Region, Kenya

Lutta V. O. Department of Civil and Structural Engineering, Masinde Muliro University of Science and Technology
vlutta@mmust.ac.ke

Obiri1 J. F. Department of Disaster Management and Sustainable Development, Masinde Muliro University of Science and Technology
jobiri@mmust.ac.ke

Abstract : In Kenya internet technology has fastened communication, information sharing and business networking including mushrooming of cash transfer initiatives. However, the flip side of this technology has been the rise of cybercrime that include fraud, account hacking, dissemination of offensive materials, theft of identities among others. In Kenya internet-based businesses are increasingly susceptible to cyber crime which is becoming a disaster to the micro and macro-economy. This study investigated the nature of cyber crime and its effects on internet-based businesses in the Western Kenya. Data was collected via questionnaire interviews and results indicated that internet-based businesses were negatively affected by cyber crimes such as malwares, fraud, cyber bullying among others. As a remedy internet-based business resorted to piecemeal strategies such as use of anti-viruses, public awareness creation, encrypted passwords, and registering new email accounts as old accounts got hacked. These strategies are not effective as businesses remain vulnerable. The study exposed the vulnerability of internet-based industry and recommends for a policy and regulation framework on cybercrime protection for internet-based businesses. This should be coupled with enhanced law enforcement particularly cyber crime information sharing between enforcement agents.

Keywords: Cyber crime, technological disaster, internet-based businesses, Western Kenya.

———————————— ◆ ————————————

- *Lutta V. O. Department of Civil and Structural Engineering, Masinde Muliro University of Science and Technology vlutta@mmust.ac.ke*
- *Obiri1 J. F. Department of Disaster Management and Sustainable Development, Masinde Muliro University of Science and Technology jobiri@mmust.ac.ke*

INTRODUCTION

Since the 1990s the World Wide Web has gained exponential growth and popularity, bringing people closely together by creating virtual cyberspace communities [1]. Undoubtedly, the internet has also revolutionalized life in Africa and particularly Kenya where cash transfer and various form of data files are extensively exchanged. Tremendous benefits have been drawn in business and communication sectors as transactions over extensive regions, which were previously difficult to reach, have now been vastly improved. On the contrary insecurity in the internet systems or cyber insecurity has concomitantly grown resulting to risks and disasters that are technologically oriented [2],[3]. Such risks and disasters are man-made and include computing malfunctions [4], extensive monetary frauds [5], information distraction and hacking amongst others. According to the Kenya Cyber Security Report of 2014 [5] various cases of fraud have been reported some of which have led to disasters in businesses linked to the internet. For instance, In January 2013, over 100 websites belonging to various Kenyan government ministries and agencies were hacked in a single day. More recently in December 2014, numerous foreign hackers have been found breaking into the Kenya government's systems and financial accounts of individuals [6]. Coupled to this the number of new malware identified is increasing exponentially with mobile device platforms being the new frontier of attack [5]. The report further points to cyber bullying as another major problem for Kenyans online. Everyday there are new cases reported of individuals who are cyber bullied. As more people embrace the use of social media, more cases of cyber bullying will be reported with many losing vital information to fraudsters including hacking of websites, stolen email accounts and identities including illicit electronic fund transfers.

Cyber insecurity occurs when vulnerabilities of computer systems are exposed, including flaws or weaknesses in both hardware and software, and individuals with access to them. It takes the forms of cyber warfare, espionage, crime, attacks on cyber infrastructure, and exploitation of computer systems [5]. Everyone is exposed to the above-mentioned activities if proper protective mechanisms and procedures are not in place.

This study investigated the various types of cyber crime, their effects on internet-based businesses in Kakamega Town in the Western region of Kenya. It further sought to establish strategies of mitigating the cyber crimes and thus ameliorate disasters that may arise from them.

MATERIALS AND METHODS

This study was undertaken in the Western region of Kenya specifically in Kakamega town. Kakamega town is a fast growing urban centre that is the capital for the regional County Government and thus keenly targeted for cyber crime. Besides, Kakamega was particularly chosen for its high population (second most populous County in Kenya, after Nairobi County) and rapidly increasing urbanization where numerous internet-based businesses of various sizes are mushrooming. The study population included cyber café operators, cyber café clients, bank managers and the police. Stratified sampling was used on cybercafé operators who were divided in terms of the size of their businesses. They were stratified into categories of small, medium and large-scale business units. Small businesses were operating between 5-10 computers, medium businesses had 10-25 computers while large-scale businesses were those with over 25 computer terminals. In this study, 80% for the cyber operators (n = 25) and 65% (n =8) for the banks was carried out since the study population was small. For every sampled cyber cafe two respondents were randomly interviewed based on gender. Thus a sample of 50 clients was interviewed. A total of five policemen attached to the criminal investigation unit were also interviewed. Four sets of interviews, using structured questionnaires, were administered to the four types of respondents: cybercafé owners, internet users, bank staff and the Kenya police personnel. Most questions were tailored towards investigating the types of crimes experienced, awareness and cases reported, and preventive measures put in place to combat cyber crimes. Secondary data was collected from existing documented information on cybercrime from various sources.

RESULTS AND DISCUSSION

Awareness of cyber crime across different stakeholders in the internet based businesses

All stakeholders involved in the internet-based business were at least aware of cyber crime however, their degree of awareness differed (Figure 1). Awareness, and particularly the acknowledgement on the existence of cyber crime, was highest among the police (100%), followed by 75% bank managers and least (35%) among clients. The results showed that the police were the most informed about cyber crime most probably because they understood and treated the reported cyber crime cases like any other crime. However, reports on cyber crime in banks were low particularly most likely because respondents from banks, especially bank managers, were afraid of negative publicity. Views of minimal reports on cybercrime from banks for the reasons of fearing damage to bank reputation and loss of public confidence have been reported in many other cases elsewhere [7][8]. The fact that most crimes are not reported remains one of the biggest drawbacks to fighting this vice [8]. Cyber clients being the least informed were more vulnerable to cyber crime.

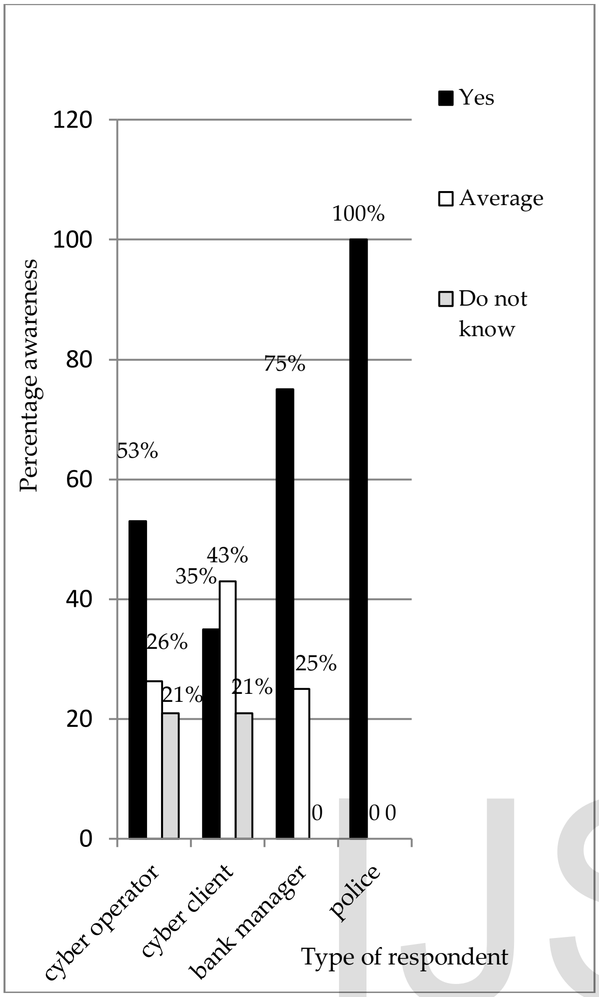

Figure 1: The awareness of respondent about cyber crime.

Types of cyber crime

The respondents were asked to identify specific types of cyber crime they encountered in the course of transacting their businesses. They identified three major categories of cyber crime, which included internet thefts (hacking and phishing), malware propagation (via viruses, Trojans, worms) and cyber bulling as illustrated in Figure 2.

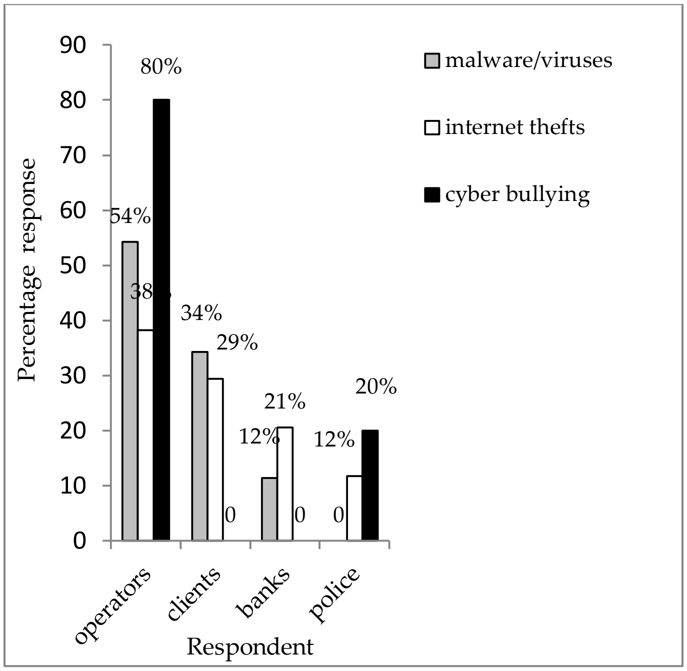

Figure 2: Type of cyber crimes indentified by respondents

The results showed that crime linked to internet thefts (e.g. hacking and phishing) were the most common across all stakeholders. They were followed by spreading of malware (viruses, trojans and worms) reported by 54% of the operators, 34% of the clients and 12% of banks. This suggested that malware (viruses, trojans and worms) were the biggest threat to cyber café businesses as compared to other businesses. Malware-linked crimes affect cyber businesses in various ways such as malfunctioning of computers, client's email accounts being attacked and their information stolen or in other cases, client's account logins were deliberately changed such that they could not access their accounts. Among clients, 34% were affected by malware while 29% by internet thefts (hacking and phishing). Banks were affected by internet thefts (hacking and phishing) 21% and malware (viruses, Trojans and worms) 11%. This was on a lower percentage as compared to cyber cafes and their clients. Cyber bullying was the third type of crime identified by the respondents. They were reported as receiving threatening or cunning emails to extort money from innocent internet users. This was reported by 80% cyber café operators and 20% of the police. However, clients and banks did not report any cyber bulling most probably because they were embarrassed to admit that they had been tricked by con artists or fraudsters.

Business size of cyber café versus type of cyber crime

Although all types of cyber crimes were common across the different sizes of internet cafes, small businesses were the most affected by malware (viruses, Trojans and worms), followed by medium-sized businesses (54%) and least by large businesses (33%) (Figure 3). Similarly the businesses most affected by internet thefts were the small (38%) and the medium-sized businesses (43%). This suggests that small and medium-sized businesses face critical challenges combating malwares and thefts most probably due to limited resources. The speed at which new malwares evolve makes it expensive for these businesses to regularly update their security software. Cyber bullying was reported across all the different businesses but predominantly in the large-sized businesses (33%).

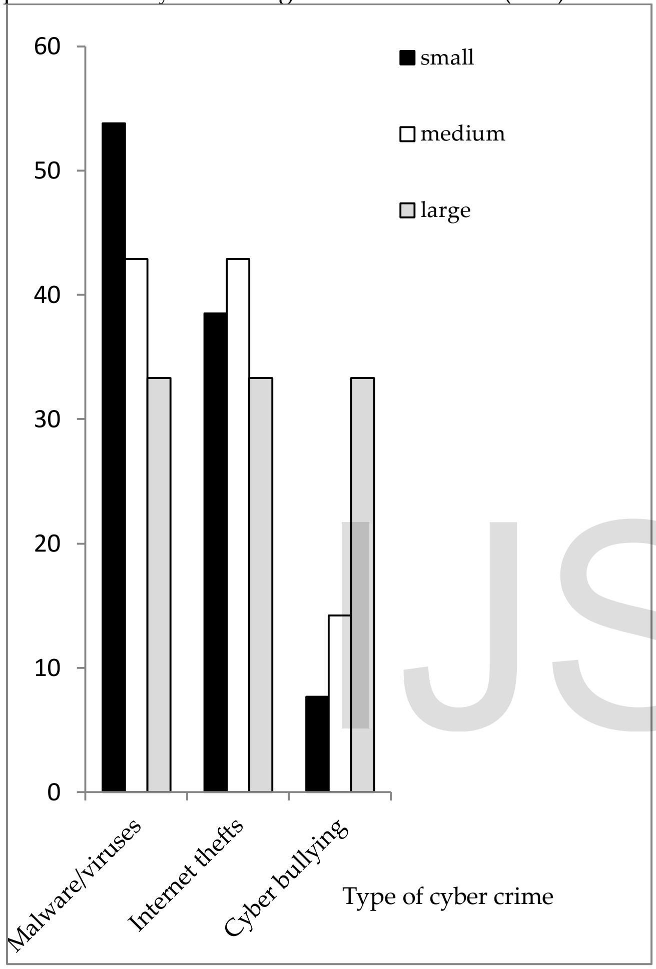

Figure 3: Types and percentages of crimes encountered in the small, medium and large-sized cyber cafés.

With real threat to their businesses, the respondents (particularly internet owners) stated that cyber crime affected their businesses or use of internet services in various ways such as reduction in customer base, denial of service or denial of access, loss of information and malfunctioning of computers. Ultimately these could lead some of the businesses closing down and finally to economic-based disasters.

Effects of cyber crime on internet-based businesses

The respondents were asked the hazards their businesses encountered as a result of internet use and responded as in Figure 4.

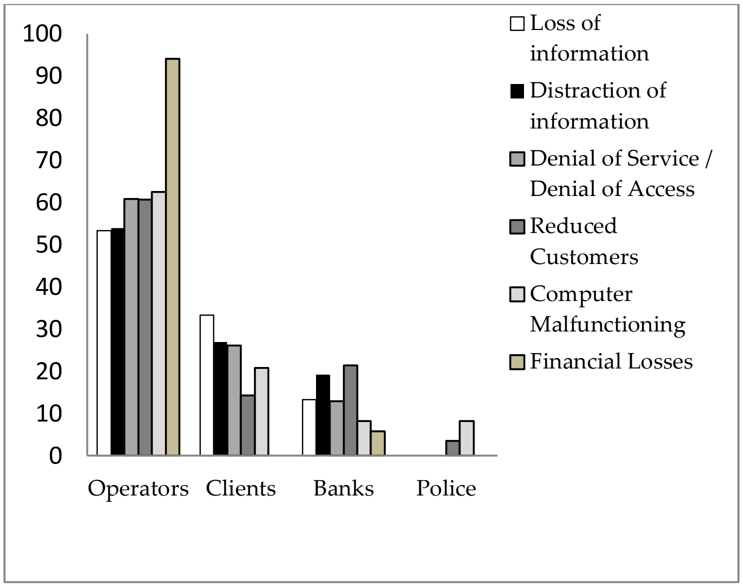

Figure 4: Effects of cyber crime on various internet based businesses.

There were four key problems reported that affected internet based businesses; loss and distraction of information, denial of services, reduction of customer numbers and financial losses. The incidences of these problems were highest among the internet café operators, followed by clients and banks and least among the police. Financial losses were most reported in small-business operators (94%) with some operators lamenting that these could lead to fiscal disasters and ultimately business closure. Beside operators, banks were the only other stakeholders who complained of financial loss although much less (6%). Hazards and problems resulting from computer malfunction was stated by all stakeholders the most being operators (63%) and least the bank (8%). Banks were minimally affected by information loss (13%) largely because they had instituted measures such as having Banking Fraud Investigation Departments (BFID) that handle cyber crimes. Computer malfunctioning was the most reported among the internet operators (63%), followed by clients (21%) and least in banks (8%).These effects had broad financial consequences for cyber cafes and banks. First, the number of clients reduced significantly, which directly affected the profit margins of these business entities as clients shied away because of cyber crime inconveniences. On this issue 94% of internet operators stated they were hit by financial losses as compared to 6% among the banks.

Cyber Crime Preventive Measures

Given the above vagaries of cyber crime the study assessed the mitigation strategies used to curb cyber crime across the different stakeholders.

To investigate the respondents' attitudes towards enhanced mitigation measures against cyber crime, they were asked their views on the introduction of a mandatory logging into the internet computers using the national identification details. Their views were as indicated in Figure 5.

Generally all stakeholders were certain about want they wanted, with regards to use of identification for logging, since they either agreed or disagreed and none gave the 'did not know' response. The biggest supporters to the use of identification for logging were they police who all strongly agreed (100%), followed by bankers 62% who strongly agreed and 38% agreed to the suggestion. Clients and operators had mixed feelings with this suggestion as views varied from strong disagreement to strong agreement but largely the operators were more opposed to this suggestion.

Generally, the option of users logging with identities into the internet was not popular among the operators and clients. The mixed feelings towards use of identification in logging as been registered elsewhere [8]. Logging with identification has been successfully tried in many other cities [9] and the same could be achieved in the Kenyan case.

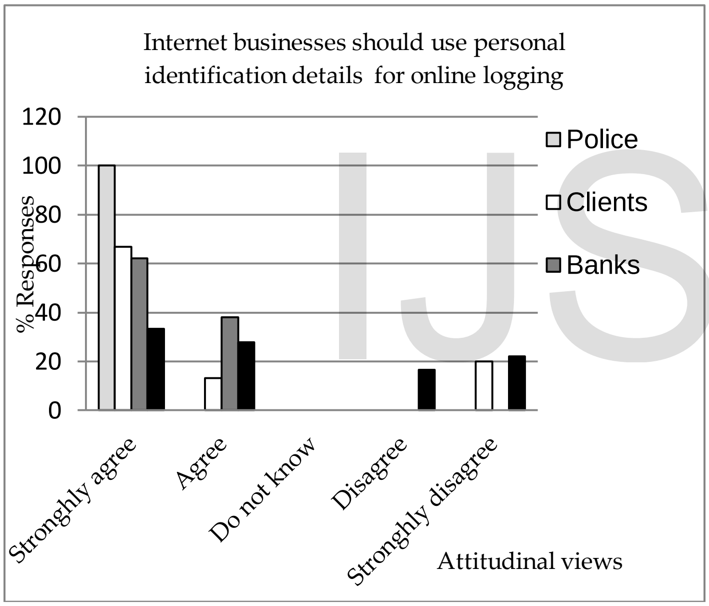

Figure 5: Views of stakeholders of the internet based business on the use of national identification detail for logging in cyber cafes.

Mitigation measures undertaken by Cyber café operators

Figure 6 shows the measures employed by cyber operators in preventing incidences of cyber crime.

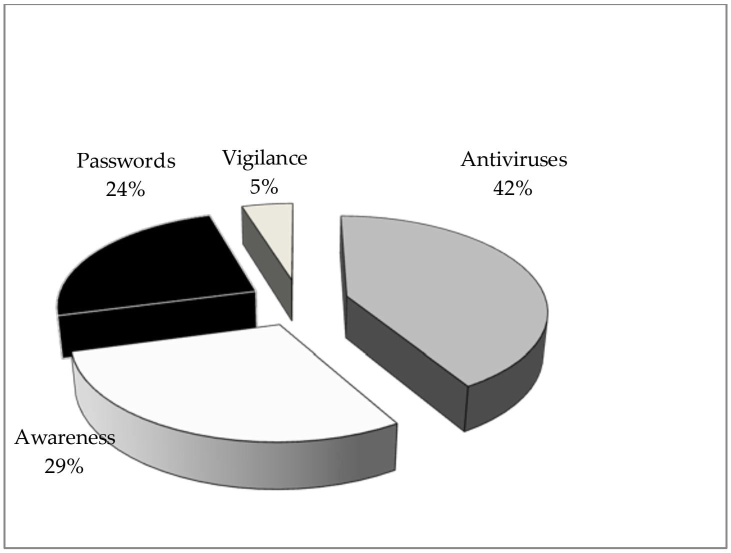

Figure 6: Mitigation measures used by operators

The findings indicated that cyber café operators' most preferred mitigation method was use of anti-virus (42%) to protect their computers from malware attack. Second was creating awareness to customers (29%) and least was use of vigilance (5%). This meant that cyber cafes were more vulnerable to viruses given the use of anti-virus as the most preferred measure. The extensive use of anti-virus was attributed to the fact that most clients visit the cyber cafes with external storage devices such as flash disks that exacerbate the rate of spread of such attacks.

Mitigation measure taken by cyber café clients

The study sought to know how cyber café clients protected themselves against cyber criminals. Results showed the most preferred measure was use of encrypted password (42%). The clients used anti-virus (32%), some ignored strange emails (5%), others backed up information (5%) and 5% opened new email accounts (Figure 7).

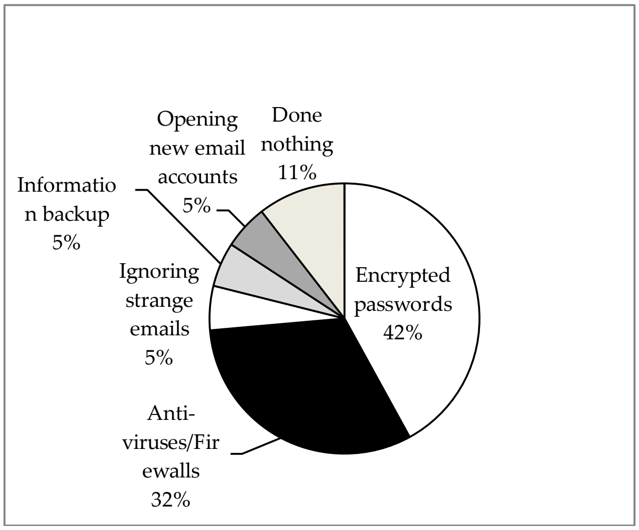

Figure 7: Mitigation Measures among clients

Mitigation measures taken by banks

Figure 8 shows the most preferred measures used by bankers were the use of anti-virus (26%), constant software upgrade (20%) and the use of embedded microchip in the Automated Teller Machine 16%). Others measures were the use of passwords (11%), cooperating with the Banking Fraud Investigation Department and the Criminal Investigation, BFID-CID (11%), creating awareness about cyber crime to the public (5%), operating independent networks and instant alerts via short text messages (5%).

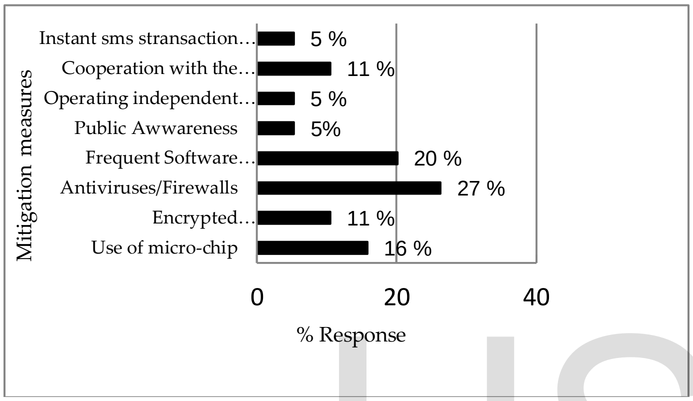

Figure 8: Mitigation Measures in banking institutions.

Mitigation measures taken by the police

The police stated they reduced incidences of cyber crime through use of cyber crime investigation units (50%), creating public awareness via community policing ideals that equips the public with information about cyber crime, and making arrests (25%) of cyber crime visible (Figure 9).

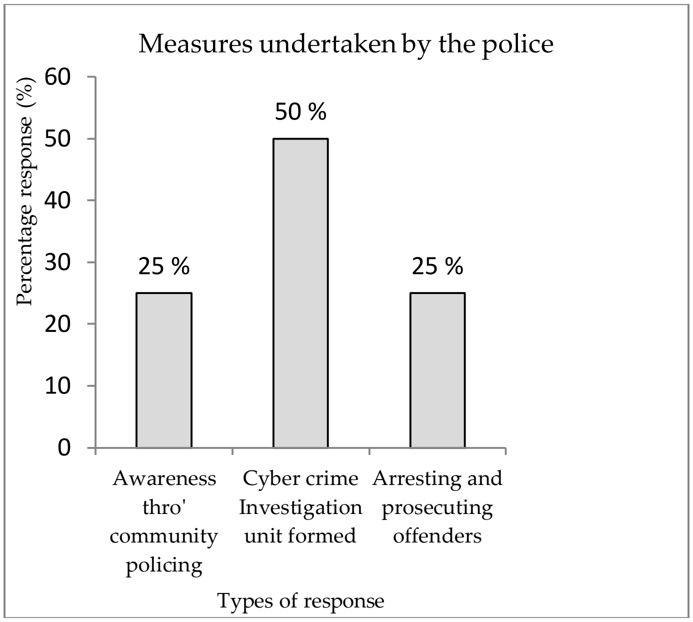

Figure 9: Measures taken by the police to curb cyber crime.

Strategic Opinion

Stakeholders gave six strategic options of curbing cyber crime (Figure 10). These were creating awareness to clients (31%), active use of encrypted passwords (21%), continuously updating antivirus (17%), having alert / sensitive operators (10%), introducing effective policies and regulatory frameworks in the industry and use of Closed-Circuit Television - CCTV (7%). The former was least popular especially among the cyber café operators as they cited the high costs of installation.

Studies elsewhere [10] show that creating awareness is perhaps the most relevant of these. With this regard the public must know the steps to take to protect with privacy, identities and financial resources that are online. Although stakeholders suggested strategic remedies to cyber crime; have been given a thought let alone implemented s been done in Kenya and there is an urgent need for the government to create a national framework and institution that will directly address the cyber security operations in the country.

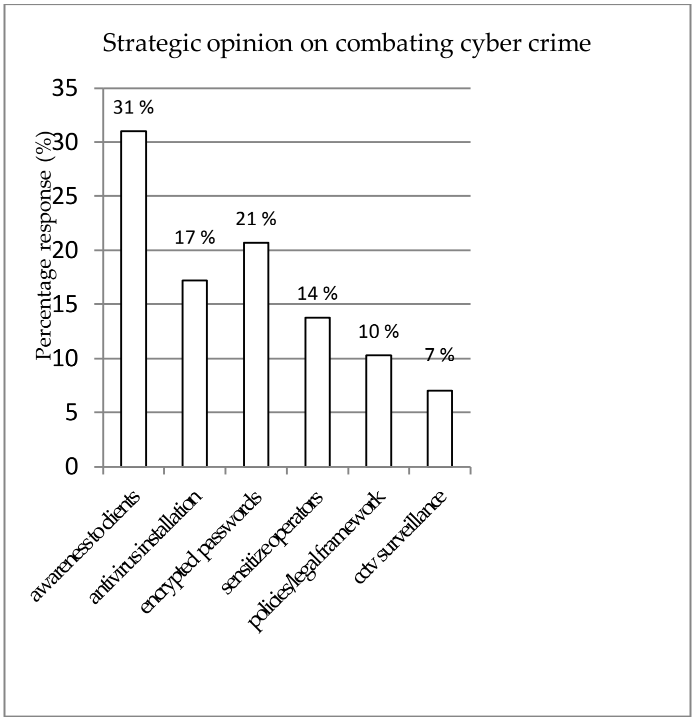

Figure 10: Strategic opinions for curbing cyber crime

CONCLUSION

The increase in cyber threats has resulted to an overhaul and re-strategizing of cyber policies and regulatory frameworks globally [11]. In Kenya these strategies still lag behind and largely none existent. Generally cyber operators and clients lamented of three main cyber crimes in Western Kenya. These were internet thefts via hacking and phishing, malware propagation done through viruses, trojans and worms and cyber bullying. Of the three the latter was least reported. On the other hand, banks considered internet thefts (hacking and phishing) and malware (viruses, trojans and worms) as their major cyber crimes as compared to cyber bullying.

Cyber crime negatively affected internet-based businesses in Kakamega with many reporting loss of information and distraction of information because of destroyed computer machines. Overall, both banks and cyber operators experienced loss of finances due to reduced client base with some being forced to shut down their businesses.

As strategies for mitigation against cyber crime, cyber operators used anti-viruses and public awareness campaigns. Cyber clients largely used anti-viruses and passwords to deter malicious software and internet theft respectively though this was not effective enough. Cyber bullying remains a big problem as many instances are not reported and also no measures have so far been employed against this problem. Although banks aggressively used antivirus to curb internet theft and malicious software, these measures were often challenged by the fast evolving cyber crime and particularly the entry of new viruses.

Invariably, cyber crime remains a problem in Western Kenya. The strategies currently used by businesses are not effective and continue to expose businesses to increased future cyber attacks.

The study recommends the need for a comprehensive policy that would govern the usage of internet in Kenya and help streamline and protect internet-based businesses from cyber crime. In this regard, it should be mandatory that online logging into the internet through cyber businesses be done using a personal identification number. The Kenya government should empower the Police service by providing the necessary training and technical resources required to discharge their duties effectively.

REFERENCES

[1] Baker, P. & Ward, A.C. (2002). Bridging Temporal and Spatial 'Gaps': The Role of Information and Communication Technologies in Defining Communities. Information,Communication & Society, 8, 207-224.

[2] Nissenbaum, Helen. (2004) Hackers and the Contested Ontology of Cyberspace. New Media & Society, 6 (2), 195–217.

[3] Hansen, L. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 53, 1155–1175.

[4] Computer Science and Telecommunications Board (CSTB). (1991). Computers at Risk: Safe Computing in the Information Age. Washington, DC: National Academy Press.

[5] Kenya Cyber Security Report (KCSR), (2014). Cyber report in Kenya. KCSR Publishers, Nairobi.

[6] BBC News Africa (2014). Kenya breaks Chinese-run cyber network. Retrieved 6th December 2014, from http://www.bbc.com/news/world-africa-30327412

[7] Rupert, J. (2006). Banks hiding online fraud, says Police. The Guardian December 5.

[8] Boateng, R., Olumide, L., Isabalija R.S., and Budu, J. (2011). Sakawa - Cybercrime and Criminality in Ghana. Journal of Information Technology Impact, 2, 85-100.

[9] News Wala (2013). City Police issue guidelines for Cyber Cafes for security. Retrieved October 2014, from http://www.newswala.com/Hyderabad-News/City-Police-issue-guidelines-for-Cyber-Cafes-for-security-31534.html

[10] Warren J.M. (2011). Protection of Australia in Cyber age. International Journal of Cyber Warfare and Terrorism, 1(1), 35-40.

[11] Lewis, T. (2006). Critical Infrastructure Protection in Homeland Security. New York, NY: Wiley.