Journal homepage: www.greatjourns.com

Journal of Criminology and Security Studies > Vol.1 No.1, April 2021

ISSN: 2328-4870

Effects of Cyber Threats on Information Communication Technology Security in Uasin Gishu County, Kenya.

[1]Gitonga Cyrus Wairiuko

Master of Arts Degree in Security Studies and Criminology of Mount Kenya University

[2]DR. Ibrahiam Nyaboga (PhD)

Senior Lecturer in the School of Business and Economics Mount Kenya University

ABSTRACT

The motivation behind this investigation is to decide the impact of cybercrime on data correspondence innovation security in Uasin Gishu County, Kenya. The investigation was guided by effects of Cyber Threats on Information Communication Technology Security in Uasin Gishu County, Kenya.The examination study strategy which was utilized for this situation is of subjective and quantitative investigation techniques in nature and for breaking down the information the scientist utilized spellbinding measurement which incorporated frequencies, rates, implies (which demonstrates the normal pace of study factors). For subjective information, information examination was finished utilizing topical investigation which included perusing and coding content for developing subjects that relate to the investigation. After cautiously evaluating the archives, rising subjects was noted and thereafter recorded. The study findings revealed that 49.1% disagreed that online piracy always scans all removable storage devices like USB Flash Disk before using them on the computers, 53.6% were in unison that cyber stalking in Uasin Gishu County is carried out by qualified IT experts, 48.2% were in agreement that access to the county database is restricted to management personnel, 50% agreed that digital psychological warfare cause serious interruption or far reaching dread in the public eye. The study concludes that identity theft as a cyber threat on information communication technology was rampant in internet materials in Uasin Gishu County, cyber bullying in Uasin Gishu County was conducted through the use of computer carried out by qualified IT experts. The study recommends that the County Government should enact cybercrime laws that deal with harmonization and standardization of computer crime, as this would bring the county closer to attaining total justice to cybercrime victims. The knowledge would be valuable to individual utilized in basic foundation territories just as security organizations accused of ensuring basic advantages for helping them assemble or improve protection against insider and untouchable digital dangers.

Key Words: *Cyber Threats, Information Communication Technology Security*

1: Introduction

All inclusive in United States of America is seeing a fast development in the use `of Technology in both people in general and private segment. The contracting expenses of ICTs have made this across the board and decentralized, coming to a long ways past the political and financial elites of Western social orders, extraordinarily profiting the creating scene and explicitly Africa from multiple points of view. As expressed by Internet Africa had more than 167 million web clients with Nigeria speaking to in excess of 48 million web clients which thusly pulled in various universal financial specialists looking for new business openings over the mainland. Africa accepts that Africa is being advanced as the following worldwide innovation center and the landmass is said to be on the precarious edge of uncommon development and flourishing claims that "development has extended the accessibility, use, and usefulness of the web at a stunning rate. Today, there are in excess of two billion web clients all inclusive, an immense increment from the 361 million clients online in 2000". This is apparent in the developing number of cell phone and web clients crosswise over Africa as individuals keep on ending up increasingly more reliant on such advancements for ordinary use (Moeng, 2011).

Since the year 2000, an indispensable job in structure Kenya's economy and is viewed as a primary government need in the acknowledgment of national improvement objectives and destinations for riches and work creation, as stipulated in the 'Kenya Vision 2030' National Development Plan .Kenya has been encountering a quick increment in web infiltration over the most recent couple of years with the general web use getting to be less expensive, better and quicker. Presently.Such web paces empower enormous volumes of information to be sent and put away in a moment, improving the effectiveness among web clients (UNODC, 2013).

Also, in 2013 the advertise in Kenya arrived at an estimation of US$5.16 billion, of which media transmission administrations represented 71.9 percent, equipment made up 22.3 percent, and IT administrations and programming spoke to 3.0 percent and 2.8 percent, separately. Spending is relied upon to keep becoming over the estimate time frame to arrive at an estimation of US$5.86 billion out of 2017 (CCK, 2013).

The fast development of Kenya's division has made it a main African center in imaginative advancements, and Kenyans have rapidly turned out to be subject to the administrations given to them through government and business sites, banking availability, and simplicity of interchanges. Because of the enormous profitability gains and new abilities empowered by development of in Kenya, the Kenyan government has joined into countless applications and for all intents and purposes each area of the nation's basic foundation including: wellbeing, security, agribusiness, money related administrations, and exchange (IDC 2014).

In such manner, the Kenyan government has "executed electronic frameworks in different state offices and other state-claimed organizations, including the national duty framework, the migration data framework, the lawful data framework, the incorporated money related administration framework and the instruction framework. Besides, most of these frameworks are arranged in the National Treasury, Home Affairs Department and the migration Offices for instance, presently offers online administrations, for example, accommodation of expense forms and installments, just as duty related data to natives and organizations. For government organizations, for example, the, the web is of impressive significance to the sending of a national single window for exchange assistance, and the reconciliation of traditions, port and travel forms, which thus eventually lessens the expenses for government and exchanging endeavors .Penetration of an association data framework could have broad results particularly in the present time of data edge technique. Governments, business associations and people the world over have put resources into data and correspondences Technologies suggesting the frameworks' safety efforts, and create security strategies that determine the right conduct of workers, customers and natives. A safe e-governments data framework ensures execution of the framework and upgrades dependability, certainty and conviction, yet in addition fulfills the security guidelines (Kenya, 2013).

A protected and solid data framework is perceived as a premise of upgrading certainty of e-government frameworks Late improvement and selection of budgetary foundations in Kenya of on the web and portable financial administrations is driving associations and people to beforehand unchartered hazard levels and more extensive introduction.

The administration has presented various undertakings and some are currently offered on the web, for example e-resident, I-charge, Kentrade single window framework, incorporated money related administration data framework . Accessibility of taxpayer driven organizations through e-government other than offering to persuade genuine partners,

has additionally opened basic databases and framework to the danger of digital assaults Invasion of e-government frameworks could have an effect one-government clients' frameworks' certainty and selection .As of late different foundations have been focuses of digital frailty; 103 government associations were casualty of digital assaults in Kenya in the period of February 2012 according to the report by Serianu IT security counseling firm.

This paper assesses elements influencing digital security in Kenya with an inclination towards the Public Service. Digital security is fundamentally the way toward guaranteeing the wellbeing of the internet from known and obscure dangers. The International Telecommunications Union expresses that digital security is the aggregate utilization of techniques, safety efforts, plans, dangers organization strategies, commitment, preparing, foremost practices, affirmation and aptitude that can be utilized to protect the data framework, association and related resources .Digital assaults includes the noxious use of data and correspondence innovation either as an objective or as a gadget by a few malevolent on-screen characters. Digital security could likewise allude to the security of web, PC systems, electronic frameworks and different gadgets from the digital assaults.

Digital security has effects affected business. The present data age has expanded the degree of association's reliance on the internet an effective assault bargains the privacy, respectability and accessibility of an framework and the data it hampers in an association. Digital burglary (digital undercover work) can bring about introduction of financial, owner, or secret data from which the interloper can pick up from while the genuine association misfortunes income or patent data. Open workplaces are workplaces in the form of the Consolidated Fund or straightforwardly out of assets given by government to individuals living inside its purview, either legitimately (through the open part) or by subsidizing conveyance of administrations. These administrations are given by different open workplaces in attempted of their particular commands. As of late there has been an expansion of the open workplaces connecting with and offering administrations to their clients through the ICT framework (Bulgurcu et al., 2010).

1.1 Statement of the Problem

Cyber security frameworks, cybercrimes are becoming more frequent, more sophisticated, and more widespread affecting crucial areas such as Telecommunications .These cybercrimes activated by; crackers, hackers, career criminals, pranksters, cyber terrorists, cyber bulls, salami attackers are increasingly having devastating impact to the information consumers as well organizations. Organizations have suffered immense losses in form of unwarranted access to confidential information, lack of data integrity, and exposure to obscene and financial losses. The financial losses due to cybercrime are enormous and damaging.

According to Communications Authority's of Kenya first quarter report for 2018/19, National Cyber security Centre detected 3.82 million cyber threats, a rise from 3.46 million reported from the last quarter. Within the review period, the banking sector remained the most targeted industry followed by government institutions (County Governments such as Uasin Gishu). Latest statistics from National Kenya Computer Incident Response Team Coordination Centre (2014).

A total of 123 cybercrime cases were reported in Uasin Gishu in the year 2018-2019 as compared to 72 cases in 2016-2017, according to National Police Crime Situation Report (2017). This increase was attributed to reckless abuse of the social media during the electioneering period. Arrests were made as a result of use of intelligence and monitoring. There has been a rise of computer related frauds targeting banks, mobile money transfers services and SACCOs. The methods employed include identity theft, hacking, denial of services, intrusion and manipulation of computer systems.

Empirical and contextual studies have shown that even with the presence of cyber security framework, the dent causedby cybercrime is widening day by day. Conducted a study, which reveals that financial institutions in Kenya need to guard themselves against cybercrime. As the study concludes that there are emerging challenges of cyber threats in Kenya Banking sector, the study reported a monthly of increase of 100% in cybercrime. However, these studies have not significantly sought to examine factors contributing to cyber security framework in Kenya Telecommunication industry, a gap the present study sought to fill. This study sought to determine the effects of Cyber Threats on Information Communication Technology Security in Uasin Gishu County, Kenya.

1.2 Purpose of the Study

The purpose of the study was to find out the effects of Cyber Threats on Information Communication Technology Security in Uasin Gishu County, Kenya.

II: LITERATURE REVIEW

2.1 Cyber Threats in information Communication Technology Security

In the present day, the term is solely used to characterize data security matters. Since it is difficult to imagine how advanced sign traversing a wire can speak to an assault, we have taken to picturing the computerized world as a physical one.

As indicated the exponential development of the Internet interconnections has prompted a critical development of digital assault episodes regularly with heartbreaking and heinous outcomes. Malware is the essential decision of weapon to complete malignant aims in the internet, either by misuse into existing vulnerabilities or use of interesting attributes of developing innovations. The improvement of increasingly creative and powerful malware resistance instruments has been viewed as a pressing prerequisite in the digital security network. To help with accomplishing this objective, we first present a review of the most abused vulnerabilities in existing equipment, programming, and system layers (Alfawaz, 2008). This is trailed by studies of existing best in class relief systems as why they do or don't work. We at that point examine new assault designs in rising advances, for example, online networking, distributed computing, cell phone innovation, and basic foundation. At long last, we portray our theoretical perceptions on future research bearings. Digital security report 2015, the open division (government and related parastals) were positioned first levels. Impacts of digital security disappointment prompts the loss of protected innovation, direct money related misfortune from cybercrime, loss of touchy business data, (for example, arranging methodologies), Other expenses incorporate extra expense of tying down systems and uses to recoup from digital assaults, reputational harm to the hacked organization (Brenner, 2002).

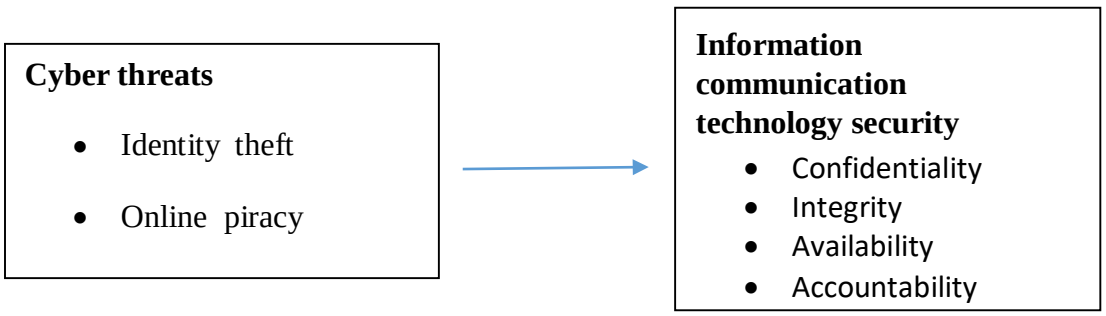
Creating nation governments are these days expected to be increasingly straightforward, share data with people in general and teach the populace on ongoing open advancements are hence putting intensely in e-government Unbound e-government frameworks won't just impede the persuade of administration conveyance to residents, yet may prompt twisted data prompting partners loss of framework certainty E-government security is pivotal for accomplishing a propelled phase of e-taxpayer supported organizations as it improves trust and unwavering quality of the administration conveyance. As the quantity of e-taxpayer supported organizations acquainted with the clients' expands, a more elevated amount of e-government security is required. There is have to assess variables prompting compelling digital security in e-taxpayer supported organizations which could be distinctive to the private segment as these two segments work in various condition and prerequisites (Chang ,2007).

Variables influencing security can for the most part be separated in two gatherings; inspiration or explanations behind the assailants of the framework and framework vulnerabilities or shortcoming abused by the aggressors for fruitful digital assaults. The qualification essentially indicates inspiration elements are for the most part outer to the association while frameworks' vulnerabilities are inner to the association however the order isn't totally select.

2.2 Conceptual Framework

A side from demonstrating the heading of the examination, through the applied system, the scientist can probably demonstrate the connections of the various develops that he needs to explore. The theoretical system communicates the connection between the autonomous and ward variable is demonstrated as follows.

Independent Variable **Dependent Variable**



Source: (Researcher, 2021)

111: RESEARCH METHODOLOGY

3.1 Research Design

This study was descriptive survey research design and explanatorily research design**.** Descriptive design involved gathering of quantitative information that can be tabulated along a continuum in a numerical form (Collis and Hussey, 2013). This design also entailed in gathering data that described events and then organized, tabulated, depicted and described the data collected.

Where description of the state of affairs of phenomena was done as it existed (Kombo and Tromp, 2011). The aim of this research design was to establish and give a report on the ways things are (Mugenda andMugenda, 2003). The descriptive design suitability to this study is due to its efficiency in gathering enough information which can be obtained from a selected target group of respondents within a given population set under the study.

Explanatory designs involved the study which the primary goal is to know and identify with the trait and mechanisms of the relationship and association between the independent and dependent variable. (Cooper and Schindler (2003), an explanatory study uses theories or hypotheses to account for the forces that caused a certain phenomenon to occur. And it goes beyond description and attempts to explain the reasons for the phenomenon. It involved series tests of significance for testing hypotheses in order to determine with what validity data can be said to indicate conclusions. It is also concerned with the estimation of population values. It is mainly on the basis of inferential analysis that the

This study employed both qualitative approach and quantitative approach, which helped clarify some sections of the study. Lieber and Weisner (2010) stated that the combination of both inductive and deductive reasoning by the mixed methods approach has helped in answering questions and providing comprehensive evidence for studying research problems than either of the approaches. According to Duo, mixed paradigm research have guiding principles for collecting and analysing data; which is termed as a research process of both the quantitative and qualitative in nature and which is a phase in conducting the research process. This has been in contention as being useful to the of the combination of these approaches which ensures understanding of a research problem under the study than using one of the two, however the mixed methods research provides strengths to both qualitative and quantitative research.

3.1 Study Area

The study was carried out in Uasin Gishu County government ICT department which is in Eldoret Town .Uasin Gishu County Government is located on a plateau and has a cool and temperate climate. The researcher decided to choose Uasin Gishu County because it is affected by cybercrime each and every year.

3.2 Target Population

Kombo, 2011, in his investigation diagrams populace as a unit or a characterized gathering of individuals, fragments, and family units that are being contemplated. The investigation was led in Uasin Gishu County, Kenya. The examination applied Krejcie and Morgan equation of test assurance to create an example of 150 ICT staffs of County Government of Uasin Gishu Krejcie and Morgan table (1970).

3.3 Sample Size and Sampling Technique

An enumeration was led where by every one of the 150 ICT staffs of County Government of Uasin Gishu was inspected since the objective populace is little and sensible.

3.3.1 Sample size

3.3.2 Sampling Technique

The exploration utilized the system of stratified irregular testing; this is the point at which the objective populace was sub-separated into strata. The stratum involved Managers, Assistant directors, Section heads and Supervisors. Two arrangements of study units was required for the reasons for this investigation. This along these lines required utilization of a blend of testing systems. Stratified and straightforward arbitrary examining techniques was utilized to choose workers of Uasin Gishu County, Kenya (Creswell and Plano-Clark, 2011).

3.3.3 Data Collection

The investigation got the essential sources from Uasin Gishu County using an organized and semi-organized survey.

The investigation embraced surveys in gathering information has characterized poll as that arrangement of inquiries which has been arranged and confined in a way that is simpler to handle and utilized by the specialist in getting enough material for breaking down the information. Furthermore, polls were utilized due to their effectiveness, not costly and can be utilized when getting information from an a lot bigger example. In this investigation, the analyst planned surveys which were utilized to accumulate data from representatives since the sample size was huge. The survey was structured dependent on study destinations and was directed utilizing - drop-and-pick-later-strategy (Kothari (2013).

3.3.4 Informant Interview

This is a point by point talk with which is conveyed or led to witness people who have profound data on a given network, and knows regular events in the network. Key witness meeting were utilized to gather data from different scope of individuals; heads of offices and chiefs, who are accepted to have direct information about digital wrongdoing in Uasin Gishu County. The examination utilized key source meeting.

This included one on one meeting between the specialist and the sources utilizing open-finished inquiries questions. This strategy was gainful to the examination as it permited free-trade of thoughts, and fit posing progressively complex inquiries and getting increasingly point by point reactions.

3.4 Pilot Study

The pilot study was done in Moi Teaching and Referral Hospital ICT office. The members were urged to remark and make recommendations which was utilized to improve the exploration instruments to guarantee their legitimacy, unwavering quality and practicability.

3.4.1 Validity of the Research Iinstruments

According to Kabiru and Njenga (2009), Legitimacy as that way of degree in which the instrument estimates what it should gauge and this incorporates Content legitimacy and Construct legitimacy as a component of estimating instruments to be utilized in the examination. Content legitimacy was accomplished through introducing the instruments to managers together with counseling the specialists. After pilot study, the exploration accomplished develop legitimacy by the utilization of factor examination and make some correlation close by what Kaiser-Meyer-Olkin's proportion of 0.5 has demonstrated.

3.4.2 Reliability of instrument.

The consistence of instruments in getting similar results is what is alluded to as the dependability of research instrument (Orodho 2012).The research will receive a test-retest position in which survey instrument will be utilized more than once on similar respondents to test for the inner consistency. After pilot study, unwavering quality was resolved utilizing Cronbach Alpha coefficient. The two outcomes were connected and determined to check for the dependability file which on the off chance that it surpasses 0.7 shows satisfactory reliability. The unwavering quality record was set up by the Cronbach Coefficient Alpha recipe. Its primary intention is pre-trying the instruments to build up lucidity of importance and intelligibility of everything in the investigation instruments.

3.5 Data Collection Procedure

In the wake of being cleared by the college experts on composing, printing and guarding the proposition the analyst obtained a specialist letter for research. When the specialist gets an assent he searched for somebody to help him in dealing with the polls. Before managing the polls, they will initially be checked for precision, consistency and fulfillment.

3.6 Data Analysis

The examination study technique which was utilized for this situation is of subjective and quantitative investigation strategies in nature and for breaking down the information the scientist utilized unmistakable measurement which incorporated frequencies, rates, implies (which demonstrates the normal pace of study factors), and the standard deviation which told the best way to discover a lot of scores all things considered.

The inferential insights which were embraced were Regression Model of relationship to get the noteworthy and factual connection between the factors.

The empirical model is as follows;

$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \varepsilon$

Y- Cyber crime
β_0= Constant

β_1- β_5 - Coefficient

X_1 –Cyber Threats

X_2-Network Crimes

X_3 – Access Crimes

X_4 – Abetting Crimes

ε –Error

3.7 Ethical Consideration
The examination embraced the accompanying moral contemplations:

Totally deliberate interest was looked for as nobody is constrained to respond to addresses they would prefer not to. There are some moral worries that was considered before embraced on the investigation. Educated assent regarding all members was guaranteed by requesting that they use where vital coding as opposed to utilizing their names or some other individual data in surveys. The researcher provide adequate information concerning the study, adequate opportunity for the respondent to consider all options regarding the study, and assure them that they were not compelled to participate in the study. The participants were not coerced to sign the consent form. So as to accomplish this, the respondents were permitted to just tick where proper. This exploration was secret and was kept by the scientist alone. There was an introductory letter from Mount Kenya University, National Commission for Science Technology and Innovation (NACOSTI), Ethical Review Committee (ERC) demonstrating the reason with respect to why the examination is being directed to the investigation and how he plans to secure the data of the respondents so as to keep away from stresses and in this way making the respondents to unreservedly take an interest in filling polls.

IV: DISCUSION OF FINDINGS

4.1 Cyber-threat on Information Communication Technology Security
The study sought the responses on the assertion that cyber-threat on Information Communication Technology Security are as presented on table 4.14 below.

Table 4.1 Cyber-threat on Information Communication Technology Security

Statements	SD	D	UD	A	SA	Total
Identity theft is rampant in internet materials	6(5.5 %)	24(21 .8%)	15(13 .6%)	55(50 %)	10(9. 1%)	110(1 00%)
Online piracy always scan all removable storage devices like USB Flash Disk before using them on the computers.	9(8.2 %)	54(49 .1%)	13(11 .8%)	23(20 .9%)	11(10 %)	110(1 00%)
Computers are regularly scanned for malware programs (for example viruses).	10(9. 1%)	53(48 .2%)	13(11 .8%)	34(30 .9%)	0(0.0 %)	110(1 00%)
One can only access specific websites from the establishment‘s internet connection	6(5.4 %)	16(14 .5%)	65(59 .2%)	20(18 .2%)	3(2.7 %)	110(1 00%)
The county uses CCTV to monitor departments using computers.	11(10 %)	59(53 .6%)	2(1.8 %)	12(11 %)	26(23 .6%)	110(1 00%)
Departments using computers are accessible by authorized employees only.	13(11 .8%)	4(3.6 %)	3(2.7 %)	60(54 .5%)	30(27 .2%)	110(1 00%)

Each employee has to have a user name and password to use a computer.	11(10%)	54(49.1%)	2(1.8%)	17(15.5%)	26(23.6%)	110(100%)
Each password and user name is unique to every employee	16(14.5%)	22(20%)	5(4.5%)	52(47.2%)	15(13.6%)	110(100%)
The county wireless internet is password protected	12(11%)	18(16.4%)	8(7.2%)	62(56.4%)	10(9.1%)	110(100%)
There is a strict county policy concerning computer misuse.	3(2.7%)	15(13.6%)	54(49.1%)	33(30%)	5(4.5%)	110(100%)

(*Source*: Researcher, 2021)

The first objective of the study sought the study responses on the effect of cyber-threat on Information Communication Technology Security, based on the first statement that identity theft is rampant in internet material, the study results revealed that 5.5% of the respondents strongly disagreed, 21.8% disagreed, 13.6% were undecided, 50% agreed and 9.1% strongly agreed. From the study findings we can imply that the majority of the respondents were in agreement that identity theft as a cyber-threat on information communication technology was rampant in internet materials in Uasin Gishu County.

Based on the second statement that online piracy always scan all removable storage devices like USB Flash Disk before using them on the computers, the study results reveal that; 8.2% of the respondents strongly disagreed that online piracy always scan all removable storage devices like USB Flash Disk before using them on the computers, 49.1% disagreed, 11.8% were undecided, 20.9% agreed that online piracy always scan all removable storage devices like USB Flash Disk before using them on the computers and 10% strongly agreed with the statement. From the study findings the majority 49.1% disagreed that online piracy always scans all removable storage devices like USB Flash Disk before using them on the computers, the findings implies that online piracy as a cyber threat on ICT security in Uasin Gishu does not scan all removable storage devices like USB flash disk before using them on the computers.

Based on the statement that computers are regularly scanned for malware programs (for example viruses), the study results are as follows; 9.1% strongly disagreed that computers are regularly scanned for malware programs (for example viruses), 48.2% disagreed, 11.8% were undecided and 30.9% disagreed that computers are regularly scanned for malware programs (for example viruses). As indicated by most of the employees 48.2%, the computers in the County Government of Uasin Gishu are not regularly scanned for malware program which makes them vulnerable to cyber-attack.

Based on the fourth statement that one can only access specific websites from the establishments internet connection, the study results reveal that 5.4% of the respondents strongly disagreed that one can only access specific websites from the establishments internet connection, 14.5% disagreed, 59.2% were undecided, 18.2% agreed and 2.7% strongly agreed. From the study findings its evident that the majority 59.2% were undecided on whether one can only access specific websites from the establishments internet connection while only 2.7 strongly agreed with the assertion. The study findings implies that most of the employees in Uasin Gishu were not certain whether they can only access specific website from the establishments internet connection.

Based on the fifth statement that the county uses CCTV to monitor departments using computers, the study results revealed as follows; 10% of the respondents strongly disagreed that county uses CCTV to monitor departments using computers, 53.6% disagreed that county uses CCTV to monitor departments using computers while 1.8% were undecided, 11% agreed that county uses CCTV to monitor departments using computers and 23.6% strongly agreed that county uses CCTV to monitor departments using computers. The study findings can be interpreted to mean that the county does not actually use the CCTV to monitor departments using computers.

Based on the sixth statement that departments using computers are accessible by authorized employees only, the study findings revealed as follows; 11.8% of the respondents strongly disagreed that departments using computers are accessible by authorized employees only, 3.6% disagreed, 2.7% were undecided, 54.5% agreed that departments using computers are accessible by authorized employees only and 27.2% strongly agreed that departments using computers are accessible by authorized employees only. As indicated by the majority 54.5%, in most departments using computers in Uasin Gishu County Government, computers are only accessible by authorized employees, this helps in safeguarding against cyber threats on ICT security.

On the statement that each employee has to have a user name and password to use a computer, the study findings revealed as follows; 10% of the respondents strongly disagreed that each employee has a user name and password to

use a computer, 49.1% disagreed, 1.8% were undecided, 15.5% agreed that each employee has a user name and password to use a computer and 23.6% strongly agreed that each employee has a user name and password to use a computer. From the study findings, we can infer that most employees in Uasin Gishu County 49.1% disagreed that they have a username and password to use a computer.

On the assertion that each password and user name is unique to every employee, the study findings revealed as follows; 14.5% strongly disagreed that each password and user name is unique to every employee, 20% disagreed, 4.5% were undecided, 47.2% agreed that each password and user name is unique to every employee and 13.6% strongly agreed that each password and user name is unique to every employee. The study result implies that the majority 47.2% were in agreement that each and every employee in Uasin Gishu has a unique password and user name. This helps in countering cyber threats on ICT security in Uasin Gishu County.

Further, on the statement that the county wireless internet is password protected, the study finding were as follows; 11% strongly disagreed that the county wireless internet is password protected, 16.4% disagreed that the county wireless internet is password protected, 7.2% were undecided, 56.4% agreed that the county wireless internet is password protected and 9.1% strongly agreed. As revealed by most of the respondents 56.4%, we can infer that the county wireless internet is password protected which makes it hard for cyber crime to occur.

Finally, on the statement that there is a strict county policy concerning computer misuse, the study results revealed as follows; 2.7% of the participants strongly disagreed that there is a strict county policy concerning computer misuse, 13.6% disagreed that there is a strict county policy concerning computer misuse, 49.1% were undecided, 30% agreed that there is a strict county policy concerning computer misuse and 4.5% strongly agreed that there is a strict county policy concerning computer misuse. From the study findings we can infer that the majority were not sure whether there is a strict county policy concerning computer misuse, this implies that there is need for the county government to enlighten its employees on policies concerning computer misuse.

The rapid growth of information and communication technologies (ICT) has resulted in a number of new areas of opportunities and efficiencies for organizations, more especially business organizations and private sector in general, in Kenya and even globally. Although, these new technologies have brought these benefits, they have also brought unprecedented cyber threats (IT Governance Ltd, 2015). Organizations therefore need to put in place ICT infrastructures consisting of networked computers and other communication systems and security measures, in order to exploit the mentioned ICT benefits. These networked computers, which include Local Area Networks (LANs) and internet, organizations globally continually face challenges that are related to maintaining their information systems and data in the cyberspace environment. Intrusion into corporate networks by hackers have increased tremendously and new forms of computer viruses that are used by hackers to launch cyber-attacks are continually being released. According to Robinson, 2013 Cyber threats are those actors or adversaries exhibiting the strategic behavior and capability to exploit cyberspace with an intention of harming life, information, operations, the environment and or property.

Cyber threats have a huge potential to cause serious harm because cyber applications have found application in many places which include governments, vital infrastructure, businesses and also private space. These threats may be classified broadly into two, namely; cyber warfare and cybercrime. Cyber warfare is the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes (Saulius, 2012). Cyber-crime on the other hand can be defined as any criminal activity that involves a computer, networked device or a network (Jethwani and Surbhi, 2015). While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials (Jethwani and Surbhi, 2015).

V: SUMMARY OF THE FINDINGS, CONCLUSION AND RECOMMENDATION

5.1 SUMMARY OF THE FINDINGS

Based on the first objective, the study confirms that 50% agreed that identity theft as a cyber threat on information communication technology was rampant in internet materials in Uasin Gishu County, 49.1% disagreed that online piracy always scans all removable storage devices like USB Flash Disk before using them on the computers. As indicated by most of the employees 48.2%, the computers in the County Government of Uasin Gishu are not regularly scanned for malware program which makes them vulnerable to cyber attack. 59.2% were undecided on whether one can only access specific websites from the establishments internet connection while 53.6% disagreed that the county

government uses CCTV to monitor departments using computers, 47.2% were in agreement that each and every employee in Uasin Gishu has a unique password and user name, 56.4% agreed that the county wireless internet is password protected and 49.1% were not sure whether there is a strict county policy concerning computer misuse, this implies that there is need for the county government to enlighten its employees on policies concerning computer misuse.

5.1 Conclusion

Based on the first objective the study concludes that; Identity theft as a cyber threat on information communication technology was rampant in internet materials in Uasin Gishu County, online piracy does not always scans all removable storage devices like USB Flash Disk before using them on the computers. Computers in the County Government of Uasin Gishu are not regularly scanned for malware program which makes them vulnerable to cyber attack. Most employees can only access specific websites from the establishment's internet connection. County government does not use CCTV to monitor departments using computers, each and every employee in Uasin Gishu has a unique password and user name and county wireless internet is password protected Although most were not sure whether there is a strict county policy concerning computer misuse, this implies that there is need for the county government to enlighten its employees on policies concerning computer misuse.

5.2 Recommendation

There is a need for setting up a public facility (preferably with a presence on the internet) where victims can report incidences. The public need a lot of sensitization and training on what computer crimes are, in which forms they can manifest, how to detect them, what to do after detection and how to prevent and minimize them. The County Government should enact cybercrime laws that deal with harmonization and standardization of computer crime, as this would bring the county closer to attaining total justice to cybercrime victims.

REFERENCES

Alfawaz, S, May, LJ and Mohanak, K (2008) 'E-government Security in Developing Countries: a Managerial Conceptual Framework',Paper Presented to International Research Society for Public Management Conference, Queensland University of Technology, Brisbane, 26-28.

Bougaardt, G and Kyobe, M.(2011) "Investigating the Factors Inhibiting SMEs From Recognizing and Measuring Losses From Cyber Crime in South Africa" The Electronic Journal Information Systems Evaluation Volume 14 Issue 2, (pp167-178).

Brenner, S., W. (2002b). The Privacy Privilege: Law Enforcement, Technology and the Constitution. *Journal of Technology Law and Policy* 7 (2) 123-94.

Brenner, S.,W. (2002a) Organized Crime? How Cyberspace may Affect the Structure of Criminal Relationships. *North Carolina Law & Technology* 4 (1)

Brenner, S.,W. (2004). Toward a Criminal Law for Cyberspace, Distributed Security. Boston University *Journal of Science & Technology Law* 10 (2).

Bulgurcu, B, Cavusoglu, H., and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, *ISQuarterly* 34(3),523-548.

Chang and C-S. Lin (2007) "Exploring Organizational Culture for Information Security Management," Industrial Management &Data Systems,vol.107,no.3,pp.438- 458.

Chau, P. Y., Kuan, K. K., and Liang, T. (2007). Research on IT value: What we Have Done in Asiaand Europe. *European Journal of Information Systems,16*(3),196.

Cooper,D.R.,and Schindler,P.S.(2003).Business Research Methods.(8thed.).Boston: McGraw-HillIrwin.

Creswell, J. W. (2013). Qualitative Inquiry and Research Design: Choosing Among FiveApproaches. Sage.

Dacin, M. T., Goodstein, J. and Scott, W. R. (2002). Institutional Theory and Institutional Change:Introduction to the Special Research Forum. *Academy of Management Journal*, *45*(1), 45-56.

Dhillon, G. and Torkzadeh, G. (2006). Value-focused Assessment of Information Systems Security in Organizations, *Information Systems Journal* 16(3), 293- 314.

Einhorn, H. J. and Hogarth, R. M. (1981). Behavioral Decision Theory: Processes of Judgment andChoice. *Journal of Accounting Research*, 1-31.

Glenny, M. Glick, B., and Wainwright, R. (2010). Cybercrime, Cybersecurity and the Future of the Internet.

Herath, T.,and Rao, H. R. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations. *European Journal of Information Systems*18(2), 106- 125.

Hulme, G. V. (2011). SCADA Insecurity-Stuxnet Put the Spotlight on Critical Infrastructure Protection but

Will Efforts to Improve it Come too late? *Information Security Magazine*, 13(1), 38-44.
International Telecommunication Union (2004). Understanding Cybercrime: A Guide for DevelopingCountry.
Jin, X. Q. Z. G. C. (2006). Theoretical Trace and Framework of Overall Innovation Management. *Chinese Journal of Management*, *2*, 002.
Kankanhallia, A., Teo, H., Tan, B. and Wei, K. (2003). An Integrative Study of Information SystemsSecurity Effectiveness, *International Journal of Information Management* (23), 139-154.
Kimutai, J. K. (2014). Social Media and National Security Threats: a Case Study of Kenya(Doctoral dissertation, University of Nairobi).