Global Scientific JOURNALS

GSJ: Volume 7, Issue 9, September 2019, Online: ISSN 2320-9186
www.globalscientificjournal.com

# CYBER THREATS AND CYBER SECURITY IN THE KENYAN BUSINESS CONTEXT

**Laureen Akumu Ndeda[1] and Collins Otieno Odoyo[2]***
[1]School of Informatics and Innovative Systems, Jaramogi Oginga Odinga University of Science and Technology, Bondo Town, Kenya
[2]School of Computing and Informatics, Masinde Muliro University of Science and Technology, Kakamega Town, Kenya
*Correspondence author
Email Address: laundeda@gmail.com , and odoyo08@gmail.com

## ABSTRACT

Cyber security is basically the process of ensuring the safety of cyberspace from known and unknown threats. The International Telecommunication Union states that cyber security is the collective application of strategies, security measures, plans, threats administration tactics, engagements, training, paramount practices, assurance, and expertize that can be used to guard the information system, organization and related assets. The motivation of writing this paper was therefore to establish through content analysis, the dominant cyber threats and cyber security measures in the Kenyan business context, and to further, illustrate their impact, on the business organizations. The source of information was majorly studies conducted by other scholars related on cyber threats and cyber security, and published in the various journals. The paper has gone ahead to highlight the major cyber threats common in the context of Kenyan Business Environment. The paper has also identified some of the commonly used cyber security measures used to handle the identified threats.

Key words: *Cyber Threats, Cyber Security, ICT, SMEs.*

## 1. INTRODUCTION

Cyber security is basically the process of ensuring the safety of cyberspace from known and unknown threats. The International Telecommunication Union states that cyber security is the collective application of strategies, security measures, plans, threats administration tactics, engagements, training, paramount practices, assurance, and expertize that can be used to guard the information system, organization and related assets (International Telecommunication Union, 2004). 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.

Organizations therefore need to protect their networks and websites with proper security measures as the threat of destructive denial of service attacks has increased significantly (Berkowitz and O'Brien, 2002).

In Kenya, the arrival of submarine fibre optic cable has improved bandwidth availability, and as a result, Kenyan organizations are using the increased bandwidth and ICT capabilities brought about by this technology to efficiently do businesses, deliver services and collaborate across organizational, social, and geographic boundaries (Government of Kenya, 2014). Many business organizations have also increasingly forged collaborations with their partners with the aim of controlling market share in their sectors. Such collaborations involves part of their networks, data etc. to be accessed by their partners and stakeholders in general. This has led to organizations becoming more exposed to the likelihood of their data and information getting misused or stolen. Further, cloud computing has put even more strain on what is left of enterprise network boundaries and also introduced new cyber risks and threats (Curry, 2013).

### 1.1. Cyber Threats

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).

### 1.2. Cyber Security

Cyber-security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also known as information technology security or electronic information security. Cyber security can also refer to the security of internet, computer networks, electronic systems and other devices from the cyber-attacks (Olayemi, 2014).

According to Carnagie Mellon University, (2016), the required protection involves the implementation of one or a matrix of countermeasures to the cyber threats. These cyber threat countermeasure can be defined as a mechanism that completely eliminates cyber threat attacks or reduces the effects of a cyber-attack. Such countermeasures may include training of employees on cyber security policy issues, access controls to ICT assets to counter insider and social media threats and patching software vulnerabilities to harden ICT Systems (Paula, 2014).

### 1.3. Purpose and Objective of this Paper

In view of the above, the motivation of writing this paper was therefore to establish through content analysis, the dominant cyber threats and cyber security measures in the Kenyan business context, and to further, illustrate their impact, on the business organizations.

## 2. LITERATURE REVIEW

In a study conducted by Baino (2001) in Australia which was on evaluation of security risks associated with networked information systems. The study established that a big portion of security lapses were as a result of system administrators not updating software patches as well as not keeping abreast with developments in their trade. He attributed this ineffectiveness of system administrators to culture and workload, stating that the systems administrators were in most cases responsible for taking care of numerous disparate systems. He also found out that the system administrators were also expected to be experts in increasingly complex systems comprising of various technologies, which were often beyond the comprehension of most of them.

In another study by Kreicberga (2010) conducted in Sweden, on internal threat to information security countermeasures and human factor in small and medium enterprises (SMEs), established that formal policies that lack proper maintenance and awareness did not impact on employee behavior, whereas informal norms within organization have the greatest influence on information security behavior. Technological security countermeasures are more effective and undertaken seriously if their necessity was explained as a benefit to the end users.

A study by Tarimo (2006) carried out in Sweden on social and technical view of ICT security issues, trends and challenges towards a culture of ICT security, and further focused on the case of Tanzania. The study established that, to cultivate a culture sensitive to ICT security is not an easy task and it was not an issue that could be addressed solely by organizations. There were factors external to the organizations that also needed to be addressed when it comes to ICT security. For instance, when it comes to training and creating awareness for ICT security, aspects such the overall education system of a country and its support structures need to be put into consideration.

A study carried out by Makumbi (2012) entitled, an analysis of information technology security practices, a case study of Kenyan small and medium enterprises (SMEs) in the financial Sector. The objectives of the research were to establish the level of reliance Kenyan SMEs are on ICT, establish the most prevalent security threats among Kenyan SMEs, and to establish how Kenyan SMEs are protecting their computers, data, and networks from information security risks. The study established that there was awareness among the organizations investigated on the importance of information systems security and they had endeavored to put security measures in place based on their reliance on IT systems. With the nature of such organizations, financial fraud seemed to feature prominently among the incidents that were reported, loss of computer assets seemed to be a recurring problem and systems user threat was common among the organization studied. It was further established that, Firewalls were the common defense employed against hacking. The study went ahead to recommend that, such organizations should put various measures in place including segregation of duties, physical security controls and inventories of IT assets.

Nyamongo (2012) conducted a case study of private chartered universities in Kenya on information systems security management. The study established that institutions of higher learning in Kenya were ready to adopt and improve on their information systems security management by regularly updating management on security updates. Staff training on information systems security management would go a long way in improving the university's information security system management. Major challenges facing information security system management were found to be viruses, user errors, theft of computers, system and software errors. From this, it could be concluded that institutions of higher learning should rethink their ways of handling security of their most valued assets. Therefore, there was need for such institutions to adopt an effective strategy that would help them to achieve effective information security management.

In another study by Njiru (2013) carried out a study on a framework to guide information security initiatives for banking information systems, a case study of the Kenyan banking sector. The aims of this study were to identify common vulnerabilities affecting the banking information systems, to analyze existing frameworks used to evaluate security programs and initiatives of banking systems, to define the gaps in the existing security investment frameworks, to develop a framework that will be used for evaluating security programs for banking industry and to validate the security investment framework. The study established that people were the largest threat to information systems while lack of proper communication, lack of skilled labor and security awareness by customers were also cited as major obstacles to security effectiveness. Further, fraud, careless or unaware employees and internal attacks were also cited as threats that had increased banks' risk exposure. The study concluded that leadership and the alignment of people, processes and technology was the most important aspect in the transformation of information security.

## 3. METHODS AND MATERIALS

This paper used qualitative research approaches. The paper depended on secondary data that were obtained from other related studies that were published online. They were retrieved and the based on their relevance to the theme of this paper. Contents were analyzed using thematic analysis.

## 4. FINDINGS AND DISCUSSIONS

This paper involved combing through a series of related studies that others scholars had conducted and published in various journals as well as cyber security threats and countermeasures reports by various organizations such as Serianu and Governments. These findings are listed and further discussed in the subsections that follows;

### 4.1. Cyber Threats

According to Bulgurcu, Cavusoglu, and Benbasat (2010), any successful attack would definitely compromises the confidentiality, integrity, and availability of an ICT system and the information it hampers in an organization. Cyber theft can result in an exposure of economic, proprietary, or confidential information from which the intruder can gain from, whereas the legitimate organization losses revenue or patent information.

The following cyber threats according to the Kenya Cyber security report 2014 were found topping the list of the cyber threats facing Kenyan organizations. They include; insider threats, VOIP PBX Fraud, social media, denial of service (DoS), botnet attacks, online and mobile banking fraud, mobile money fraud and cyber espionage (Paula, 2014).

### 4.1.1. Insider Threats

This threat is characterized by employees deliberately attacking the organizational cyberspace assets. High level access users, for example system such as administrators look for system loop holes so as to gain unauthorized access, ride on other users' access privileges without their authority to attack the organizational systems for several reasons ranging from disgruntlement, revenge and blackmail (Paula, 2014).

### 4.1.2. VOIP / PBX Fraud

This type of fraud involves parties external to the organization making unauthorized calls through the organization's VOIP/PBX systems at the expense of the organization. The external parties hack into the organization's VOIP/PBX phone system and make money by using the phone system to make calls to premium rate numbers, and leave the owner organization to pay the bills of the hackers' calls (Paula, 2014).

### 4.1.3. Social Media

This type of threats include online fake offers that are designed to trick users to give away their access credentials. Complex online malware install buttons that are availed to user with the ultimate aim of gaining access to the user's computer or system. The hackers may provide fake plug-ins posing as legitimate internet extensions to trick users to download them and therefore infect their computer and steal information from it (George, 2015).

### 4.1.4. Denial of Service (DoS)

Most of the time denial of service (DoS) attacks come from compromised ICT systems at hosting service providers sites especially the ones that are slow to respond to malware attack clean ups and also from installations that cannot be reached by international authorities. DoS attacks present themselves in various forms. Some attack the ICT infrastructure at a site, while others take advantage of vulnerabilities in applications and network communication protocols in use at a site. Such attacks are intended to make websites, servers and ICT infrastructures unavailable to their legitimate users (Blagov, 2015).

### 4.1.5. Botnet Attacks

Botnet attacks originates from compromised computers, generally referred to as botnets, in cyberspace. The increasingly usage of high speed internet exposes more computers, routers and other ICT gadgets to the world-wide-web and on the same regard, expanding the quantity of computers, routers and other ICT gadgets that can be compromised by cyber criminals especially if these gadgets are not properly secured.

The compromised gadgets can be utilized to spread viral infections, produce spam and carry out different sorts of online crime and fraud. The assailants then use this very distributed system to launch attacks on targets such as, monetary establishments and government institutions with the aim to defraud, cripple or steal information (Leder and Martini, 2009).

### 4.1.6. Online and Mobile Banking Fraud

According to Mukinda (2014), many Kenyans who have subscribed to mobile banking services run the risk of exposing their money to fraudsters. The growing implementation and use of online and mobile banking services has brought to the fore a new frontier of cyber threats to financial institutions and their customers. This is as a result of the fact that most of these financial institutions are implementing already vulnerable web and mobile applications.

In a study by Paula (2014) on online banking applications, it was revealed that out of the thirty three online banking applications sampled, only two online banking sites had adequate online security deployed on their web applications. Most of the online applications studied lacked strong encryption and were prone to phishing attacks.

### 4.1.7. Mobile Money Fraud

The popularity of mobile money usage in Kenya and the East Africa region in general has already attracted cyber criminals who have shifted their focus to this new money transfer service. The criminals in this sector are getting sophisticated and are fast in finding exploitable vulnerabilities in new controls implemented by mobile money merchants, financial institutions and individual users (Paula, 2014).

### 4.1.8. Cyber Espionage

Cyber espionage is the theft of secret or confidential information stored digitally on computers and ICT networks. Cyber criminals financed by states or organizations deploy high level and carefully crafted techniques to access networks and steal information in a stealthy manner. Cyber espionage is being advanced by the ongoing political and economic changes in most countries in the world. Also, competing organizations are using cyber espionage attacks to obtain strategic information from their competitors (Lotrionte, 2015).

### 4.2. Cyber Security and Countermeasures

Cyber threat countermeasure can be viewed as an action, process, technology, device or system that serves to prevent or mitigate the effects of a cyber-attack against a computer, server, and network or associated device (Carnagie Mellon University, 2016).

#### 4.2.1. Countermeasures to Insider Threats

Measures commonly used under this category of threats include awareness training for employees, so that they are able to identify phishing and other social media threat techniques (US Government, 2014). It is therefore recommended that regular training should be offered to employees to maintain high levels of knowledge skills and abilities which in turn prevent or mitigate insider threats and to improve risk perception.

The training also help in raising the level of employee knowledge on how they can guard themselves against becoming unintentional threats. Adequate security practices such as two-factor authentications for system login and inculcate employee culture that highly resonates with organizational information security mission is highly encouraged (US Government, 2014).

#### 4.2.2. Countermeasures to VOIP /PBX Fraud

For this category of fraud an organization needs to use virtual LAN (IEEE 802.1Q) to segregate voice and data traffic (Wei, 2012). Further, there is need to also implement quality of service to give priority to voice traffic over data traffic. This design prevents internal hackers from sniffing voice traffic. The network administrator could also monitor traffic on individual voice ports on the Ethernet switch. If a voice port has unusual traffic spike, it would trigger a security alert for further investigation. Other countermeasures include disabling non-service related ports, restricting international calls to designated phone numbers and constantly monitor call detail records (CDRs) to identify unusual usage patterns (Yu, 2015).

#### 4.2.3. Countermeasures to Social Media Threat

For social media cyber security threats, countermeasures that could be implemented comes from two fronts, the people front and the policy front. People front involves awareness training for employees on how to handle the various social media cyber threat related crimes when online (Wilcox, 2015). From the policy perspective, countermeasures applied included measures in the organizational security policy on how to handle social media threats such as phishing and social engineering while online (Wilcox, 2015).

#### 4.2.4. Countermeasures to Denial of Service

A DoS attack being a network based attempt to make a website, a service or a complete infrastructure unavailable to users by mostly attacking victims from several compromised systems. To counter such attacks, detective security in the form of continuous monitoring of system capacity and traffic type of critical infrastructure, and services like firewalls with a view to improving detection capabilities of cyber-attack must be put in place.

According to European Broadcasting Union (2015), strengthen the detective security measures with preventive security measures such as segmentation of internal to external networks, of any network containing critical broadcast systems, automation of the scanning and patching of potential DoS vulnerabilities in internet facing services and load balancing and defining a DoS protection agreement with the internet service provider (ISP).
Network based countermeasures could also be considered such as; black holing, blocking attackers IP addresses, stopping IP announcing, domain name service (DNS) reconfiguration and isolation (disconnect from internet access) (European Broadcasting Union, 2015).

#### 4.2.5. Countermeasures to Botnet attacks

Botnet attacks countermeasures can be classified into two, namely; classical and offensive countermeasures. Classical countermeasures entails identifying a central weak point in the botnet infrastructure which is then manipulated, disrupted or blocked to incapacitate the botnet. Cooperation with an ISP is required so as to access and shut down the central component of the botnet, which then leads to the owner losing control of the botnet (Leder and Martini, 2009).

Offensive countermeasures can be categorized into three: mitigation, manipulation and exploitation.

Mitigation entails technical methods that slow botnets down by restricting the bandwidth available to it. Manipulation strategies make use of the command interface to issue commands that will cripple or disrupt the botnet. The likely solution here is to remove the DoS commands as well as the download and execute programs commands so as to allow the cleaning of infected computers. Exploitation involves finding vulnerabilities or bugs in the botnet then use them to cripple or shutdown the botnet (Leder and Martini, 2009).

#### 4.2.6. Countermeasures to Online Banking and Mobile Money Fraud

A common countermeasure to online and mobile banking fraud is two-factor authentication. Two-factor authentication entails an identification name and a password consisting of a known and fixed part and an additional piece of information that is dynamically generated and used once with each session. The dynamically generated part can be a session code or a set of single use identifiers sent at regular intervals to each customer or automatically generated at the time of logon into a session. Some financial institutions use session codes sent to user mobile phone while others issue hardware tokens that generate random codes which customers then use in their logon sessions. Still others provide bank card reading devices which first require users to use a personal identification number (PIN) to generate confirmation codes. In most cases the codes are needed when making money transactions (Ferguson, 2015).

#### 4.2.7. Countermeasures to Cyber Espionage

At government levels cyber espionage is being countered using legislation and diplomatic cooperation. As for business organizations, they have to defend themselves against persistent threats to their private data and intellectual property. Advanced tools such as threat analyzer provide enterprises with the protection they need to keep cyber threats at bay, protect their data and keep their reputations intact (Threat Track Security Inc, 2013).

## 5. CONCLUSION

From the related literature review, it could be concluded in this paper that the major cyber threats in the Kenyan business context included; insider threat, VOIP / PBX Fraud, social media, denial of service attacks, botnet attacks, online and mobile banking fraud, mobile money fraud and Cyber Espionage. Dealing with these cyber threat is not simply a question of reviewing your security systems. To respond appropriately, an organization need to have the flexibility to act quickly, gather the facts and assess the true impact of the loss.

## 6. REFERENCE

[1]. IT Governance Ltd. (2015). what-is-cybersecurity.aspx. Retrieved from http://www.itgovernance.co.uk : http://www.itgovernance.co.uk/what-iscybersecurity.aspx

[2]. Government of Kenya. (2014). Cyber Security Startegy. Ministry of Information Communications and Technology. Nairobi: Govenment Press.

[3]. Curry, S. e. (2013). Big data fuels intelligence driven security. Security Division. San Diego: EMC Corporation.

[4]. Robinson N. L. (2013). Cyber-security threat characterization, a rapid comparative analysis. Stockholm: RAND Corporation

[5]. Saulius, P. (2012). What factors explain why there is not a common and comprehensive global response to cyber threats? Leiden University.

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

[7]. Carnagie Mellon University. (2016). CERT Division. Retrieved from http://www.cert.org/

[8]. Paula, E. A., (2014). Kenya Cyber Security Report 2014, Rethinking Cybersecurity, "An Integrated Approach: Processes, Intelligence and Monitoring.". Nairobi: Serianu Limited.

[9]. Baino, P. (2001). Evaluation of Security Rrisks Associated with Networked Information Systems. Melbourne: Royal Melbourne Institute of Technology University.

[10]. Kreicberga, L. (2010). Internal Threat to Information Security-Countermeasures and human factor within SME. Kiruna: Lulea University of Technology.

[11]. Makumbi E. A., (2012). An Analysis of Information Technology (IT) Security Practices: A Case Study of Kenyan Small and Medium Enterprises (SMEs) in the Financial Sector. Nairobi: University of Nairobi.

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

[13]. Njiru, S. W. (2013). A Framework to Guide Information Security Initiatives for Banking Information Systems, Kenyan Banking Sector Case Study. Nairobi.

[14]. George, T. (2015, October). Next Big Cybercrime Vector: Social Media. Retrieved from Security Week: www.securityweek.com

[15]. Blagov, M. (2015). What is a Distributed Denial of Service (DDoS) Attack:DoS and DDoS Explained: Incapsula. Retrieved from www.incapsula.com: https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html

[16]. Leder, F., & Martini, W. (2009). Proactive Botnet Countermeasures an Offensive Approach. Bonn: Institute of Computer Science IV, University of Bonn, Germany.

[17]. Mukinda, F. (2014). Fraudsters find easy cash in mobile banking. Nairobi: DAILY NATION Newspaper.

[18]. Lotrionte, C. (2015). Countering State-Sponsored Cyber Economic Espionage under International Law. Journal of Law Cyber Warfare, 443 - 540.

[19]. US Government. (2014). Combating the Insider Threat. New York: National Cybersecurity and Communications Integration Centre.

[20]. Wei, X. K. (2012). Security Implementation for a VoIP Server. Conference on Computer Science & Service System, (pp. 983 -985).

[21]. Yu, J. (2015). Prevention of Toll Frauds against IP-PBX. International Conference on Security and Management, (pp. 259 - 254). Chicago.

[22]. Wilcox, H. M. (2015). Countering Social Engineering through Social Media: An Enterprise Security Perspective. Sydney: Charles Sturt University, Australia.

[23]. European Broadcasting Union. (2015). Mitigation of Distributed Denial of Service (DDoS) (DDoS) Attacks. Geneva: The European Broadcasting Union.

[24]. Ferguson, R. (2015). The Word Is Not Enough – Online banking fraud. Cork, Ireland: Trend Micro Incorporated.

[25]. Threat Track Security Inc. (2013). Enterprises Must Prepare to Combat Cyber Espionage. Clearwater, Florida: hreat Track Security, Inc.

[26]. International Telecommunication Union (2004). Understanding Cybercrime: A Guide for Developing Country.

[27]. Olayemi, O. J. (2014) A socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria, International Journal of Sociology and Anthropology, 6(3), 116-125.

[28]. Tarimo, C. (2006): ICT Security Readiness Checklist for Developing countries: A Social-Technical Approach. Ph.D thesis. Stockholm University, Royal Institute of Technology.

[29]. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, MIS Quarterly34 (3), 523-548.

[30]. Berkowitz, J., & O'Brien, J (2002). How accurate are value-at-risk models at commercial banks. Finance 57:1093–1111. Retrieved from: https://doi.org/10.1111/1540-6261.00455