Global Scientific JOURNALS

GSJ: Volume 6, Issue 3, March 2018, Online: ISSN 2320-9186

www.globalscientificjournal.com

KENYA METHODIST UNIVERSITY-KENYA

FACTORS CONTRIBUTING TO CYBER SECURITY FRAMEWORK IN KENYA: A CASE STUDY OF KENYAN TELECOMMUNICATIONS COMPANIES

Benson Muriuki Ngare(MIS-3-2621-2/2015)

ABSTRACT

The continuously rising cybercrime, in modern days, is being heavily being felt in developing countries and more so by the telecommunications sectors. Although Cyber security frameworks are also being developed to counter the same by the organizations, their objective has not been achieved to substantially, which demands for a cost-effective and responsive cybercrime framework in developing country to ensure security over telecommunications. Although research has been done on cyber security frameworks in the telecommunication sectors, it is not clear the factors contributing to cyber security framework in Kenya's Telecommunication industry. The study was therefore conducted to explore factors contributing to cyber security framework in Kenya's Telecommunication industry. The study, which adopted a descriptive research, had the 133 the telecommunications industry IT experts in Kenya as its target population and obtained a sample size of 100 respondents using the Slovin's formula. Data was collected using a structured questionnaire and analyzed using descriptive and inferential analysis to establish a study model. Based on the findings, the study established that at 0.05 (5%) level of significance, each of; personal data protection demands, computer use control, content exposure control, and data copyright structures are predictors of the cyber security framework in Kenyan telecommunications companies where 60.000% of variations in cyber security framework in Kenyan telecommunications companies is explained by these factors.

Key words: Computer use control, Content exposure control, Cyber security framework, Data copyright structures, Personal data protection demands

1. INTRODUCTION

Cybercrime, which often takes an international dimension, involves use of the computer over network as a platform for the commissioning crime. (Barret, *et al,* 2015). Accordingly, cybercrime investigations and cooperation between countries involved very important to address cybercirme (Jacob, Solms & Grobler, 2015). However, these formal agreements are complex and often time-consuming procedures, insignificantly covering computer-specific investigations. This renders the need to develop procedures for quick response to incidents, which are country specific as well as requests for international cooperation vital (Al-Ayoub, *et al*., 2015). Although there are existing global frame including; COBIT 5, ISO 27000, and NIST 800-53, and Westby, there is an urgent need to develop a frameworks to supplement information security though since these exhibit certain limitations (Westby 2004). The requirement to develop a comprehensive anti-cybercrime strategy and solutions for developing countries, which generally contains technical protection measures as well as legal instruments, is resulting threat of cybercrime being a major challenge.

Specifically, in Kenya, there is need to integrate protection measures into the roll-out of the Internet from the beginning. Although this might initially raise the cost of Internet services, the long-term gains in avoiding the costs and damage inflicted by cybercrime are large and far outweigh any initial outlays on technical protection measures and network safeguards (Mwai, 2015; Wekundah, 2015). The risks associated with weak protection measures could in fact affect the country more intensely, due to their less strict safeguards and protection (Nyawanga, 2015). The ability to protect customers, as well as firms, is a fundamental requirement not only for regular businesses, but also for online or Internet-based businesses (Nyawanga, 2015; Wekundah, 2015). Therefore, the country needs to bring its anti-cybercrime strategies into line with international standards from the outset, through the development of its cyber security framework and especially in the telecommunication industry.

Statement of the problem

Cyber security frameworks play an important role in the ongoing development of information technology in supporting or guiding the rapid developments of ICT infrastructure (Chang, Kuo & Ramachandrian, 2016). Despite the availability of cyber security frameworks, cyber crimes are becoming more frequent, more sophisticated, and more widespread affecting crucial areas such as Telecommunications (Saini, Rao, & Panda, 2012). These cyber crimes activated by; crackers, hackers, career criminals, pranksters, cyber terrorists, cyber bulls, salami attackers are increasingly having devastating impact to the information consumers as well organisations. Organisations have suffered immense losses in form of unwarranted access to confidential information, lack of data integrity, exposure to obscene and financial losses (Gercke. 2012). The financial losses due to cybercrime are enormous and damaging (Gercke. 2012; Saini *et al*., 2012). In the year 2007, the financial damage caused by cybercrime exceeded USD 100 billion in 2007, outsmarting the illegal trade in drugs (Gercke. 2012).

Empirical and contextual studies have shown that even with the presence of cyber security framework, the dent caused by cyber crime is widening day by day. Nyambura (2013) conducted a study, which reveals that financial institutions in Kenya need to guard themselves against cybercrime. As the study by Nyawanga (2015) concludes that there are emerging challenges of cyber threats in electronic transaction technologies in Kenya Banking sector, the study by Munyua *et al*. (2010) reported a monthly of increase of 100% in cyber crime. The study by Munyua *et al*. (2010) established that number of incidents reported and their severity indicated a serious threat on government and privately owned information, communications and technology systems.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 take a different dimension of bridging the existing gap in order to establish factors contributing to workable frameworks aimed at containing cyber security in Kenya.

Research Objectives

The general objective of the study was to assess the factors contributing to Cyber security Framework in Kenya.

The study was guided by the following specific objectives

i. To establish the effects of personal data protection demands on cyber security framework in Kenyan telecommunications companies.
ii. To determine the influence of computer use control on cyber security framework in Kenyan telecommunications companies.
iii. To determine the effects of content exposure control on cyber security framework in Kenyan telecommunications companies.
iv. To establish the influence of data copyright structures on cyber security framework in Kenyan telecommunications companies.

Research Hypotheses

H_{10}: Personal data protection demands do not significantly contributes to cyber security framework in Kenyan telecommunications companies

H_{20}: Computer use control does not significantly influences cyber security framework in Kenyan telecommunications companies

H_{30}: Content exposure control does not significantly contribute to cyber security framework in Kenyan telecommunications companies

H_{40}: Data copyright structures do not significantly influence cyber security framework in Kenyan telecommunications companies

2. LITERATURE REVIEW

Theoretical Reviews

Cybersecurity Information Sharing Theory - Inserra and Rosenzweig (2014) - The theory involves the requirements that administrators must explain what information sharing is and how it works to address real privacy concerns overcoming lack of trust (Inserra & Rosenzweig, 2014). Information sharing between organization in order to flow rapidly and in both directions between the government and the private sector. It provides that the private sector should be provided with legal, freedom of information, and regulatory protections for sharing information. It advocates for broad information sharing to ensure government agencies have the information they need in order to prevent cybercrime and attacks (Inserra & Rosenzweig, 2014).

Cyber-terrorism IR Theory – Petallides (2012) -This theory involves understanding that the internet is a realist security model which is ungoverned (Petallides, 2012). It explains how to safeguard networks in an environment where allies cannot be fully trusted. It advocates for finding of better methods of storing important data through concentrating on mitigation of data breaches and cyber-attacks (Petallides, 2012). The theory analyzes impacts of the information revolution on cybersecurity and clarifies the challenges of the revolution (Eriksson & Giacomello, 2006). These pertinent questions are initially addressed by a critical review of past research. The theory pays attention to ICT-related security issues and scrutinizes realism, liberalism, and constructivism schools of thought in regard to what they can say about cybersecurity in this modern digital age (Eriksson & Giacomello, 2006). The theory suggests pragmatism as a bridge to the gap between theory and practice, and to overcome the dualistic, contending nature of international relations theories.

The Willie Sutton Theory of Cybersecurity - Derived from interview response of William Francis 'Willie' Sutton, a bank robber to whom the statement that he robs 'banks because that where the money is' is attributed (Bamrara, Jamba, & Rathore, 2015). Servers and storage devices that manage and safeguard the vast bulk of a company's or government agency's data are targeted because of the data in them. This involves a three-step process for better segmentation of high-value assets through; comprehensively understanding your computer environment, creating a segmentation model that ring-fences high (value assets), and creating a zero-trust model for high-value assets

Empirical reviews

The study by Saini et al. (2016) established that cyber security should be part of virtual infrastructure. An empirical study by Okuku et al. (2015) concludes that Kenya's growth in Internet use has been facilitated by high proliferation and adoption of mobile communications and that he role of governmental cyber security strategy is important for improving public awareness of mobile Internet threats. The study by Okuku et al. (2015) proposed that future research in this area be carried out to specifically measure the effectiveness of cyber security awareness approaches in countries with vibrant mobile Internet societies that have implemented awareness drives.

The study by Casey (2011) concludes that issues experience in the telecommunications industry include; breaches to data confidentiality, integrity and availability of computer data Crimes related to data include data exfiltration, unauthorized encryption and lose, unwanted data infiltration, deletion, alterations.Another study by Faiz and Maqsood (2008) in an effort to examine better understanding of mobile telephony security against information security threats from the developers' perspective established that most developer had very little security awareness as they also lacked enough security conscious attitudes. Therefore, a secure mobile phone services can be developed with the balance of security and usability.

The study by Rieke, et al. (2013) established that cyber computer fraud; MPESA hacking, computer-based forgery, identity theft such as taking customer data and using computer for illegal purposes and misuse of devices for criminal purposes were common complaint against mobile companies in Kenya. The study by Magutu et al. (2011) revealed that there is extreme content-related exposure of images and texts, such as pornography and other content-related offensive messages.From the argument by the Magutu et al. (2011) the present may conclude that the content

exposure might be beyond the boundaries of the telecommunications companies since the companies only protect information being consumed by their clients and they do not control the internet access

Magutu et al. (2011) documented the copyright related offences as; stealing of trade-marks and copyright theft

3.RESEARCH METHODOLOGY

This study used a descriptive research design in soliciting information in the area of research of to assess the factors contributing to Cyber security Framework in Kenya. Target population was the 120 IT experts in the telecommunications industry in Kenya. A sample size of 92 respondents was obtained using the Slovin's formula (Tejada & Puntalan, 2012) given by:

$$n = \frac{N}{1 + Ne^2}$$

Where

N= population size;

e= margin of error; take as 5% or 0.05.

For a total population of N=120

$$n = \frac{120}{1 + (120 * 0.05^2)}$$

=92.32

Sample size n = 92

The study adopted proportionate stratified random sampling to select respondents form each company (Palinkas, *et al*., 2015).

Data was collected fro primary sources using a structured questionnaire, administered using drop and pick method. The research tool was tested for reliability and validity before administration.

The study analysed the data using descriptive analysis to produce descriptive statistics; especially, means, frequencies, and standard deviation to help establish patterns, trends and relationships, and to make it easier for the researcher to understand and interpret implications of the study. The study carried out inferential statistics, correlation and multiple regressions, to estimate dependent variable (response; Cyber security framework in Kenya) in terms of the independent variable (predictor; personal data protection demands, computer use control, content exposure control, and data copyright structures). The study tested the hypotheses using Analysis of Variance (ANOVA), at 0.05 level of significance **(**p-value <=.05).

4. RESULTS AND DISCUSSIONS

Table 1: Analysis by study objectives

Cyber Security Framework In Kenya	Mean	Std. Dev.
The Cyber security framework enhances management of system risk	3.11	0.640
Appropriate safeguards ensure delivery of critical infrastructure services.	3.06	0.704
Cyber security framework activities identify occurrence of cyber security	3.43	0.558
Appropriate activities are developed using Cyber security framework	3.51	0.616
The Cyber security framework development of resilience plans	3.17	0.741
Overall Cyber Security Framework In Kenya	**3.26**	**0.652**
Personal Data Protection Demands		
Need for confidentiality contributes to the Cyber security framework	3.15	0.755
data integrity necessitates Cyber security framework development	3.46	0.663
Data security is the key contributor to Cyber security framework	3.43	0.661
Development of Cyber security framework is occasioned by data safety	3.42	0.682
The demands for a propriety database led to Cyber security framework	2.83	0.720
Overall Personal Data Protection Demands	**3.26**	**0.696**
Computer Use Control		
Cyber security framework developed to ensure money transfer security	2.66	1.050
Computer user authenticity drive Cyber security framework development	3.02	0.838
Need for Integrity codes largely contributes to Cyber security framework	2.80	1.019
Cyber security framework is developed to provide electronic evidence	2.74	0.796
Desire to track computer usage demands for Cyber security framework	2.85	1.019
Overall Computer Use Control	2.81	0.944
Content Exposure Control		
Cyber security framework is for ensuring tracking of share information	3.15	1.004
Cyber security framework provides transmitted contents authentication	3.14	0.882
Content blocking/ firewalls necessitates Cyber security framework	3.41	0.791
Source identification demands for developing Cyber security framework	3.09	0.805
Availability of Proprietary software requires Cyber security framework	2.60	0.787
User awareness of transmitted content requires Cyber security framework	2.60	0.581
Overall Content Exposure Control	**3.00**	**0.808**
Data Copyright Structures		
Cyber security framework is introduced to enact Copyright laws	2.35	1.037
Trade-marks and Logos contributes towards Cyber security framework	2.29	1.195
Patenting shared contents demands for Cyber security framework	2.25	1.173
Service provider liability contributes towards Cyber security framework	2.55	1.031
Cyber security framework is required for cooperation share information	2.78	1.053
Overall Data Copyright Structures	**2.44**	**1.098**

Cyber security framework in the Kenya's mobile telephony companies is highly enhanced management of cyber security risk to systems, assets, data, and capabilities (Mean = 3.11; std. dev. = 0.640) and that these companies develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services using their cyber security framework (Mean =3.06; Std. Dev. = 0.704). Kenya's mobile telephony companies has very effectively developed and implemented the appropriate activities to identify the occurrence of a cyber security event through the cyber security framework (Mean =3.43; Std. Dev. = 0.558) and the cyber security framework very highly enhances development and implementation of the appropriate activities to take action regarding a detected cyber security event (Mean =3.51; Std. Dev. = 0.616). The cyber security framework highly ensures that Kenya's mobile telephony companies develop and implemented the appropriate activities to maintain plans for resilience and to restore any capabilities or services that are impaired due to a cyber security event (Mean = 3.17; Std. Dev. = 0.741). Overall, the mobile telephony companies has very strong influence on Cyber Security Framework in Kenya (Mean =3.26; Std. Dev. = 0.652).

Overall, the personal data protection demands would very highly contributes to development of the cyber security framework (Mean = 3.26; Std. Dev. = 0.696). The need for confidentiality of personal very highly contributed to the cyber security framework (Mean = 3.15; Std. Dev. = 0.755) and that the cyber security framework in Kenyan telecommunications companies should actually developed due to requirement for data integrity as strongly supported by the results (Mean = 3.46; Std. Dev. = 0.663). The data security is the key contributing factor to Cyber

security framework in their firms (Mean = 3.43; Std. Dev. = 0.661) and that the development of the cyber security framework should be strongly (majorly) occasioned by the need for data Safety (Mean = 3.42; Std. Dev. = 0.682). The demands for a propriety database are some the key reasons leading to cyber security framework development in the Kenyan telecommunications companies (Mean = 2.83; Std. Dev. = 0.720).

Overall, the computer use control was shown to highly influence the adoption of cyber security framework in Kenyan telecommunications companies (Mean = 2.81, Std. Dev. = 0.944). The cyber security framework in the in Kenyan telecommunications companies should be developed to ensure money transfer security (Mean = 2.66, Std. Dev. = 1.050) and that computer user authenticity is one of the main contributing factors to the cyber security framework development (Mean = 3.02, Std. Dev. = 0.838). The need for integrity codes largely contributes to the cyber security framework (Mean = 2.80, Std. Dev. = 1.019) while the cyber security framework in the firms should be developed to provide electronic evidence (Mean = 2.74, Std. Dev. = 0.796). Further the desire to track the computer usage demands for cyber security framework (Mean = 2.85, Std. Dev. = 1.019).

Overall, the Content Exposure Control is one of the main factors affecting cyber security framework development in Kenyan telecommunications companies (Mean = 3.00; Std. Dev. = 0.808). This is where the Kenyan telecommunications companies should develop cyber security framework to ensure tracking of information being shared within the systems (Mean = 3.15; Std. Dev. = 1.004) while the cyber security framework in these firms should be introduced to provide authentication of the contents being transmitted (Mean = 3.14; Std. Dev. = 0.882). The need for content blocking highly and desire to install firewalls demands for cyber security framework development Mean = 3.41; Std. Dev. = 0.791). Meanwhile, the need to only avail proprietary software is a key driver to the cyber security framework development (Mean = 2.60; Std. Dev. = 0.787) while the demand for user awareness on content being transmitted highly necessitated the cyber security framework development (Mean = 2.60; Std. Dev. = 0.581).

On average, data copyright structures highly influences the development of cyber security framework for Kenyan telecommunications companies (Mean = 2.44; Std. Dev. = 1.098). in which case, enacting of copyright laws moderately influences the development of cyber security framework (Mean = 2.35; Std. Dev. = 1.037) as trade-marks and logos contributed moderately towards the cyber security framework adoption Mean = 2.29; Std. Dev. = 1.195), and the requirement to Patents shared contents would as well moderately demands for Cyber security framework development (Mean = 2.25; Std. Dev. = 1.173). The demand for service provider liability highly contributes towards cyber security framework (Mean = 2.55; Std. Dev. = 1.031) while cooperation among concerns to share common information highly contributed towards introduction of cyber security framework in Kenyan telecommunications companies (Mean = 2.78; Std. Dev. = 1.053).

The Pearson's correlation analysis results, at 5% level of significance, shows that all the Independent variables (IVs); personal data protection demands (r = .538, p-value = .000), computer use control (r = .722, p-value =.000), content exposure control (r = 648, p-value =.000) and data copyright structures (r = .104, p-value = .041) were significantly related to cyber security framework in Kenyan telecommunications companies, since the p-value for each was less than 0.05. The relationship between each of; computer use control (r = .722), content exposure control (r = 648) and that of cyber security framework in Kenyan telecommunications companies was high since the correlation coefficient (r) for each comparison was greater than 0.6. The relationship between personal data protection demands (r = .538) and cyber security framework in Kenyan telecommunications companies was moderate since the correlation coefficient (r) was between 0.3 and 0.6. However, the relationship between data copyright structures (r = .104) and cyber security framework in Kenyan telecommunications companies was very low since the correlation coefficient (r) was less than .03 and almost turning towards zero.

The ANOVA analysis indicate that the observed p-value = .000, since p-value less than 0.05 (F=25.022, p-value=.000), then we reject then null hypothesis and accepted the alternative hypothesis. So, at the 5% significance level (i.e. $\alpha = 0.05$, level of significance), there exists enough evidence to conclude that at least one of the predictors; personal data protection demands, computer use control, content exposure control, and data copyright structures, is useful explaining cyber security framework in Kenyan telecommunications companies.

He regression results show that; personal data protection demands, computer use control, and content exposure control had positive coefficients, implying they were directly proportional to cyber security framework in Kenyan telecommunications companies. So, an increase in any of IVs; personal data protection demands, computer use control, and content exposure control leads to increase in cyber security framework in Kenyan telecommunications companies and vice versa. However, data copyright structures had a negative coefficient, implying that it was indirectly proportional to cyber security framework in Kenyan telecommunications companies. So, an increase in any of IVs; data copyright structures leads to decrease in cyber security framework in Kenyan telecommunications companies and vice versa.

The model summary results show that the coefficient of determination was .600, an indication that 60.000% of variation in cyber security framework in Kenyan telecommunications companies is explained by personal data protection demands, computer use control, content exposure control, and data copyright structures.

5. CONCLUSION

The study concludes that personal data protection demands had moderate positive significant effects on (contribution towards) development of the cyber security framework in Kenyan telecommunications companies as occasioned by; the need for confidentiality of personal; requirement for data integrity, data security, need for data Safety and the demands for a propriety database. These are the main factors of personal data protection demands leading to cyber security framework development in the Kenyan telecommunications companies.

The study concludes that the computer use control has strong significant positive influences the development and adoption of cyber security framework in Kenyan telecommunications companies as indicated by; ensuring money transfer security, enhance computer user authenticity, activate utilisation of integrity codes, and provide electronic evidence, and track the computer usage.

The study concludes that the content exposure control has a strong significant positive effect on cyber security framework development in Kenyan telecommunications companies as indicated by; ensure tracking of information being shared within the systems, provide authentication of the contents being transmitted, necessitate content blocking, satisfy the desire to install firewalls, satisfy the demand for source identification. The key drivers to the cyber security framework development are the need to only avail proprietary software and the demand for user awareness on content being transmitted.

The study concludes that data copyright structures has low significant positive influences on the cyber security framework and is characterised by; support enacting of copyright laws, protect trade-marks and logos, patents shared contents, support the demand for service provider liability, ensure cooperation among concerns to share common information.

In conclusion, all the four IVs personal data protection demands, computer use control, content exposure control, and data copyright structures) could significantly predict the DV (cyber security framework in Kenyan telecommunications companies.

REFERENCES

Al-Ayyoub, M., Jararweh, Y., Benkhelifa, E., Vouk, M., & Rindos, A. (2015, June). Sdsecurity: a software defined security experimental framework. In *2015 IEEE International Conference on Communication Workshop (ICCW)* (pp. 1871-1876). IEEE.

Bamrara, A., Jamba, L., & Rathore, A. (2015). Information Security: Exploring the Association between IT Receptivity and Cyber Crime Victimization. *FIIB Business Review, 4*(1), 55-63.

Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems, 57*, 24-41.

Computer Hope (2017). *Free computer Help and Information*. Salt Lake City, Utah: Computer Hope.

Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations:(IR) relevant theory*?*. *International political science review*, *27*(3), 221-244.

Faiz, A. & Maqsood, M (2008). *Information Security Threats Against Mobile Phone Services (Developer´s Perspective)*. Unpublished Master Thesis: Lulea: Lulea University of Technology.

Gercke. M. (2012). *Understanding cybercrime: Phenomena, challenges and legal response*. Geneva, Switzerland: International Telecommunication Union. Retrieved from www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Inserra, D. & Rosenzweig, P. (2014). *Cyber security Information Sharing: One Step toward U.S. Security, Prosperity, and Freedom in Cyberspace Heritage.org/Backgrounder #2899 on National Security and Defense.* Retrieved from http://www.heritage.org/research/reports/2014/04/cybersecurity-information-sharing-one-step-toward-us-security-prosperity-and-freedom-in-cyberspace

Korten, D. C. (2015). *When corporations rule the world*. Berrett-Koehler Publishers.

Manjula, R. P., & Shanmugan, D. R. (2016). A Study on Customer Preference Towards Cyber Crime With Banking Industry. *International Journal of Multidisciplinary Research and Modern Education, 2*, 597-603.

Metheny, M. (2013). *Federal cloud computing: The definitive guide for cloud service providers*.

Mwai, M. N. (2015). *Factors Contributing To Occurrence Of Cybercrime On E-Banking In Commercial Banks In Kenya* (Doctoral dissertation, United States International University-Africa).

Nyawanga, J. O. (2015). *Meeting the challenge of cyber threats in emerging electronic transaction technologies in in Kenyan banking sector* (Doctoral dissertation, University of Nairobi).

Ochola, M. A. (2013). *Outsourcing Strategies Adopted by Telecommunication Vendor Companies in Kenya* (Doctoral Dissertation, University of Nairobi).

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research, 42*(5), 533-544.

Petallides, C. J. (2012). "Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat." *Inquiries Journal/Student Pulse*, *4*(03). Retrieved from http://www.inquiriesjournal.com/a?id=627

Prinz, M. (2015). Investigation of the Impact of National Culture on IT-Governance: An Explorative Study Contrasting German and Japanese National Culture.

Saini, H, Rao, Y. S. & Panda. T.C. (2012). Cyber-Crimes and their Impacts: A Review. *International Journal of Engineering Research and Applications (IJERA)* 2(2), 202-209. Available online at: www.ijera.com

Smith, R. (2016). *The NIST Cybersecurity Framework (CSF) Unlocking CSF - An Educational Session.* University of California

Stewart, P. (2015). Trading cybercrime for jobs and commerce or paying pp: Using the WTO to combat cybercrime. Geo. *Washington International Law Review*, *48*, 475.

Stokes. J. (2007). Insides the Machine. An Illustrated Introduction to Microprocessor and Computer Architecture. san Francisco: No Starve Press.

Taylor, S. J., Bogdan, R., & DeVault, M. (2015). Introduction to qualitative research methods: A guidebook and resource. John Wiley & Sons.

Thompson, K. (2015). TE Challenge.

Tropina, T., & Callanan, C. (2015). *Self- and co-regulation in cybercrime, cyber security and national security*.

Wasike, S. N. (2011). Analysis of ICT Policies and regulations in the mobile sector in Kenya: Interpretive study of mobile banking service.

Weber, R. H., & A. Darbellay (2010). *Legal issues in mobile banking,' Journal of Banking Regulation, 11*(2), 129 – 145.

Wekundah, R. N. (2015). *The effects of cyber-crime on e-commerce; a model for SMEs in Kenya* (Doctoral dissertation, University of Nairobi).

Westby, J. R. (2004). *International guide to cyber security*. Chicago, Ill.: ABA Publ. Information System Audit and Control Association (ISACA, 2015).