Cybercrime - The Emerging Threat to the Financial Services Sector in Zimbabwe

Ishmael Mugari

Lecturer, Bindura University of Science Education, Zimbabwe; Email: ishiemugari@gmail.com

Shingirai Gona

Lecturer, Bindura University of Science Education, Zimbabwe; Email: sgona@buse.ac.zw

Martin Maunga

Lecturer, Bindura University of Science Education, Zimbabwe; Email: mmmaunga@buse.ac.zw

Rufaro Chiyambiro

Intern, CIMAS Medical Aid Society, Zimbawe; Email: rufarohope@gmail.com

Doi:10.5901/mjss.2016.v7n3s1p135

Abstract

The proliferation of Information and Communication Technology (ICT) has resulted in the change of different aspects of human life, bringing convenience and simplicity to our lives. It has taken domain in the different business sectors inclusive of the financial institutions. However it has come with its own share of problems, which have become a major concern to business organisations. This study, which was confined to four financial institutions in Harare, was aimed at investigating the prevalence of cybercrime in financial institutions. A total of 48 respondents drawn from four commercial banks were invited to participate using stratified random sampling and purposive sampling techniques, with the questionnaire and in-depth interviews as the key research instruments. The study revealed hacking, phishing, identity theft and malware to be amongst the types of cybercrime in banks. Though financial institutions are putting cyber security systems in place to curb the scourge, the preventive measures are being out- paced by technological advancement.

Keywords: *Cyber crime, information technology, identity theft*

1. Background

Over the past decade, the world has witnessed a great improvement in information and communication technology. The introduction of computers and various software programmes in the business environment has greatly improved business operations. This increased use of technological innovation devices such as computers, mobile phones, internet and other associated technologies is a path way which has yielded both positive and negative results. The rise in cyber crime is the major negative impact of the use of the modern information technology infrastructure.

Cybercrime is a serious threat to all the facets of any nation's economic activity and this threat is more pronounced in financial institutions. The use of non cash based payment systems around the globe has increased the risk of cybercrime in financial institutions. The current liquidity crisis in Zimbabwe has led to an increase in the use of facilities such as payment cards and Real Time Gross Settlement System (RTGS) (Mugari, 2016). These alternative payment systems have increased exposure of financial institutions to risks such as fraudulent RTGS payments and electronic card fraud (Mugari, 2016). However, it is still a challenge to control and prevent cybercrime in developing countries than in developed countries due to factors such as; the lack of awareness, ineffective legislation and policies, cost of anti-viruses, amongst others. Law enforcement agencies have not been able to deal with cybercrime effectively, especially in the developing countries because of the pace at which technology is changing (Sussmann, 1999).

Mobile banking is one of the most recent innovations introduced in the banking sector. It involves the customer and bank communicating online (Saini et al, 2014). Customers now prefer online services because they are convenient, cost saving and easier and faster to use (Vrancianu and Popa, 2010). There has also been the introduction of mobile money transfer through mobile networks (Mbiti, 2011) and in Zimbabwe, it is being administered through services such as

Ecocash, Telecash and One Wallet. Technology has thus made banking services reach many people by improving affordability and accessibility (KPMG, 2011). Despite mobile banking advantages, it has been noted that many smart phone based applications have not been developed with security in mind, and are often not compliant with best practices (Metcalf & Kirst, 2013).

The enhancement of technology and online banking services has come with its own share of problems. Cybercrimes are committed using online technologies to illegally remove or transfer money to different accounts and are tagged as banking frauds (Wall, 2007). Siddique and Rerman (2011) identified the following cybercrimes; credit card fraud, ATM frauds, money laundering, phishing, identity theft and denial of service. According to Symantec Cyber Crime Report (2012), 114 billion is lost to cybercrime globally and the cost spent to fight cybercrimes is double the amount lost. The laws and regulations available are unable to keep up with the pace at which cybercrime is spreading (Akuta et al, 2011). It is important to note that Zimbabwe does not have a specific law towards fighting cybercrime as yet (Jangara, 2014; Chimheno & Dehangah, 2012).

With this background, this study was conducted in Harare Central Business District. All the financial institutions in Zimbabwe have their headquarters in Harare hence the sample was considered by the researchers to be representative of other financial institutions around the country. The study sought to address the following research questions;

1. Which types of cybercrime are prevalent in the financial sector in Zimbabwe?
2. How effective are the current measures for curbing cybercrime in the financial sector in Zimbabwe?
3. What can be done to combat cybercrime in financial institutions in Zimbabwe?

2. Literature Review

2.1 Concept of Cybercrime

Current definitions of Cybercrime have evolved experientially and differ depending on the perception of both protectors and victims (Magutu et al, 2011). To support the above, Yar (2005) argued that the lack of a consistent and statutory definition for the activities that may constitute cybercrime make it difficult to analyse it (Yar, 2005). Despite Magutu et al (2011) and Yar (2005)'s perception on the cybercrime definition, the Council of Europe has defined it as any criminal offence against or with help of computer network (United Nations Office on Drug Crime, 2013). Cybercrime can also be regarded as "computer-mediated activities which are illegal or considered illicit by certain parties and which can be conducted through global electronic networks" (Douglas and Loader, 2000). Other authors define cybercrime as unauthorized entry into a computer system with the motive to delete, modify or damage of computer data (Sarrab et al, 2013; Broadhurst, 2006). The diverse definitions therefore imply that it a complex type of crime since it has various forms and motives (Sarrab et al, 2013).

In Europe, cybercrimes are commonly considered as falling into one of two categories: new offences committed using new technologies, such as offences against computer systems and data, dealt with in the Computer Misuse Act 1990; and old offences committed using new technology, where networked computers and other devices are used to facilitate the commission of an offence (United Nations Office on Drug Crime 2013). To support the above, KMPG (2011) revealed that cybercrime has been used to describe a wide range of offences, including offences against computer data and systems (such as hacking), computer-related forgery and fraud (such as phishing), content offences (such as disseminating child pornography), and copyright offences (such as the dissemination of pirated content).

2.2 Nature of cybercrime

2.2.1 Phishing

Roger (2008) cited in Boateng & Amanor (2014) defines phishing as attacks on individuals and organizations in order to obtain private information which will be used for fraudulent purposes. This was supported by the Europol (2014) who went further to describe it as fraud against businesses and financial institutions through stealing the customer identity. Phishing is also referred to as identity fraud (United Nations Office on Drug Crime 2010). Sarannia & Padma (2014) defined identity theft as the stealing of sensitive information for illegal use without the owner's acknowledgement. They went further to identify three types of phishing namely spear, clone and whaling (Saranni and Padma, 2014; Chandhary, 2014). In agreement to the above, KPMG (2012) highlighted that phishing is the most common type of identity theft.

Boateng and Amanor (2014) identified vishing and smishing as types of phishing. According to Sarannia and Padma (2014) smishing is phishing by SMS (or Short Message Service). In agreement to Sarannia and Padma (2014), Boateng and Amanor (2014) defined vishing as an attack done through the use of short message services. For example a fake short message services may be send to a person informing him/her that his/her account has fallen victim to a malware and to correct this they need to send their personal details for corrections. This information is then misused for the phisher requirements (Boateng & Amanor 2014).

2.2.2 Hacking

Hacking is one of the oldest computer crimes (Herselman and Warren 2010). Paget (2007) cited in Hedayati (2012) defined hacking as the unlawful access to systems or databases to obtain personal or organizational confidential information. The availability of personal information online has made it easier for perpetrators to steal from business organizations and individuals (Magutu et al, 2011).

Bawane and Stelke (2014) listed the hacking techniques such as denial of services, spoofing, sniffing, viruses and worm, key loggers, social engineers and fake messages. In support of key loggers, Broadhurst (2006) identified hacking tactics such as key stroking monitoring or transmission whereby software is installed on victim's computer which records the key being entered and they are recorded and used for identity theft, internet fraud, telecommunication fraud and economic espionage. Hackers target a computer system host that has large data base so as to obtain identity related data on a large scale. This was supported by (Magutu et al, 2011) who mentioned the increased crisis, especially in individual accounts, as one password is used for many accounts. This therefore means that in the event of an attack of such a victim, there will be a great loss experienced in different accounts through identity theft (Magutu et al, 2011).

2.2.3 Card fraud

Sharma and Nanda (2006) defined card fraud as a type of crime involving the illegal use of unauthorized account or personal information so as to misrepresent the account information. Sonepat and Sonepat (2014) agreed with Sharon & Nanda by defining credit card fraud as the use of an unauthorized personal account for operations not intended. KPMG (2012) went further to reveal that credit card fraud can only be administered after stealing the cards and the relevant information needed for the transaction to take place. There are two kinds of card fraud which are online and offline card fraud (Sonepat & Sonepat 2014). Offline card fraud involves stealing of physical card and online car fraud is committed through the internet, phone, shopping and web.

2.2.4 Malware

According to Uppal et al (2014) malware is when an unauthorized programme is installed into a computers system secretly with the intention of stealing information. In support, the United Nations Office on Drug Crime (2013) acknowledged that malware attacks are achieved through the perpetrator installing a malicious software which allows them to scam the hard drive to collect information needed, usually credit card numbers and social security numbers. Magutu et al (2011) supported this by highlighting that malware moves between computer and network systems so as to modify systems without the owner's permission. Roderic (2006) went further to mention that malicious software can be designed to intercept communication or log key board strokes, therefore recording entry made by the user and the information can be sifted electronically for password and related information.

Uppal et al (2014) identified two categories of malware which are the contagious and masked. Under the contagious, he described viruses and worms, and under the masked, he describes the Trojans. After an unauthorized entry of a virus in a computer, the virus replicates itself and in the process infecting the whole system, leading to denial of services. Worms operate independently and they are passed through storage devices such as USB and email, which will cause shortage of space. Trojan is malware which conceals itself to behave like a legitimate program, which will be then downloaded from the internet and used for stealing personal and confidential information. These are obtained through downloading information from the internet.

2.2.5 Identity theft

Cole and Pontell, (2006) consider identity theft as the fastest growing cybercrime in America. One of the primary reasons for the lack of reliable data on identity theft is that it is debatable amongst investigators since they do not all agree on how best to define it and what crimes should fall under this broad concept (McNally and Newman, 2008; Cole and Pontell, 2006). Despite difficulties to define identity theft, McNally and Newman (2008) defined it as using someone's personal information for fraudulent use.

There is online identity theft which includes hacking, phishing malware and online fraud and offline identity theft which includes trashing and old fashioned stealing (Hoofnagle, 2009). To support the view on identity theft, CIPPIC (2007) cited in Hedayati (2012) identified the type of personal information that identity thieves steal which are credit card number, social security number, date of birth, passwords and pins, home address and phone number.

2.3 Applying Criminological Theory to Cyber crime

2.3.1 Routine activity theory

Routine theory is based on the rational choice theory and it was developed by Cohen and Marcus in 1979. It states that crime is normal and it just requires opportunity. Routine activities theory requires that three elements be present for a crime to occur: a motivated offender with criminal intentions and the ability to act on these inclinations, a suitable victim or target, and the absence of a capable guardian who can prevent the crime from happening. These three elements must converge in time and space for a crime to occur.

Hutching and Hayes (2009) applied the routine activity theory to one of the most common types of cybercrime crime in banks which is phishing. Hutching and Hayes (2009) went further and explained the presence of a suitable offender to be associated with the increase in the number of people using the internet. This therefore means an increase in the people with the technological knowhow of commit phishing. The presence of a suitable target is found where there is an increase of number people with the behaviours of potential victims, for example, more people using the internet and internet banking. The Department of Broadband, Communications and Digital Economy (2008) identified that 77% of Australians had accessed the internet in 2006, compared with 64% in 2001. This therefore increased the risk of both the likely offender and the suitable target.

The absence of capable guardianship was associated with lack of awareness. The term capable guardian may include the owner of the property e.g. account holders, law enforcement, Computer Emergency Response Teams (CERTs), banks and financial institutions, or any other individual or agency that has the potential to discourage offenders (Yar, 2005). Their absence increases the risk of cyber attacks.

2.3.2 Rational choice theory

The theory was propounded by Cornish &Clarke in 1987. The theory states that offenders make a choice to commit offences after doing a cost benefit analysis. This means an offender weighs the benefits of the offence they want to commit, as well as the cost of being caught and punished. This was supported by (McQuade, 2006) who posits that offenders are rational people who weigh the benefits of engaging in a particular criminal behaviour against the risks associated with that behaviour. According to this theory, there is need to stress the implication of strict punishment as a control measure. In financial institutions, electronic mechanisms such as user ID, automated access control system and surveillance cameras can serve as deterrents because they increase the perceived risk of being apprehended (Wada and Odulaja, 2012). The fact that cybercrime is difficult to detect also increases the chances of choices to commit cyber crime. Hence, a rational cyber criminal will choose to commit cyber crime due to huge benefits, coupled by difficulties in detection.

2.3.3 Space Transition Theory

This modern day theory was propounded by Jaishankar (2007) and is an explanation about the nature of behaviour of the persons who bring out their conforming and non-conforming behaviour in the physical space and the cyberspace. Space transition involves the movement of persons from one space to another, for example, from the physical space to the cyberspace and vice versa. The theory also highlights that persons with repressed criminal behaviour in the physical space have a propensity to commit a crime in cyberspace which they not otherwise commit in the physical space, due to their status and position (Jaishankar, 2008; Wada, Longe & Danquah, 2012). Identity flexibility, dissociative anonymity and lack of deterrent factor in the cyberspace provide the offenders with the choice to commit cybercrime (Jaishankar, 2008). Intermittent ventures of offenders in the cyberspace and the dynamic spatio-temporal nature of cyberspace provides the chance for escape (Jaishankar, 2008). The theory can thus explain the rise in cybercrime in financial institutions, especially given the fact that the perpetrators are usually of high social standing.

3. Methodology

Respondents were selected from four commercial banks out of a total of 25 registered banks in Zimbabwe. Services for commercial banks in Zimbabwe are almost similar hence four banks were selected to avoid data saturation. The study was confined to Harare Metropolitan Area and all the registered commercial banks have their headquarters in the capital city, hence it was the most ideal area of study. A total of 48 respondents from the four commercial banks were invited to participate in this study using stratified random sampling as well as purposive sampling techniques. The respondents were drawn from four key categories namely; the IT department, the risk management department, the internal audit department and the operations and services section. The respondents were perceived to be key informants to the study due to their direct and indirect encounters with criminal activities in the financial services sector. Questionnaires and in-depth interviews were the key research instruments. Quantitative data was coded and fed into the SPSS software for analysis. Qualitative data from interviews was analysed using summative content analysis and it was used to support quantitative data.

4. Research Findings and Discussion

4.1 Types of cybercrime in financial institutions and their prevalence rate

Table 1. Types of cybercrime

N=36

Types of cybercrime	Non	Low	Average	High	Mean	SD	Skewness
	1	2	3	4			
Hacking	0%	8.3%	75%	16.7%	3.08933	.0500	.192
Identity theft	0%	16.7%	69.4%	13.9%	2.9722	.55990	-.015
Electronic card fraud	11.1	36.1	41.7	11.1	2.5278	.84468	-.092
Malicious software	0	30.6	52.8	16.7	2.8611	.68255	.180
Phishing	8.3	27.8	50	13.9	2.6944	.82183	-.344

Source: Primary data

The results on Table 1 seem to suggest that cybercrime is a challenge for financial institutions in Zimbabwe. Hacking, though in the average category seems to be the major challenge, with a mean of 3.08933, standard deviation of 0.0500 and a level of skewness of .912. Identity theft comes second, with a mean of 2.9722 also indicating an average prevalence rate. Malicious software attack had a mean of 2.8611, with a standard deviation of 0.68255 and a 0.180 level of skewness. Phishing and electronic card fraud have lower prevalence rates, with means of 2.6944 and 2.5278 respectively. Though a lesser proportion of respondents considered the cyber crimes to be high (hacking, 17%; Identity theft, 14%; electronic card fraud, 11%; phishing, 14%), the fact that most of the respondents indicated that the cybercrimes have an average occurrence rate is a cause for concern.

4.1.1 Hacking

With the majority (75 percent) indicating hacking to be in the average category, the finding is in tandem with the study conducted by Raghavan & Parthiban (2014) and Siddique & Rehman (2010), who identified hacking to be amongst the types of cybercrimes most prevalent in the banking sector. Analysing the results of the study and that of past studies, it can be established that hacking is a persistant crime, as it was identified in the studies by Siddiqie & Rehman (2010); Raghavan & Parthiban (2014) and Mugari (2016). This to some extent shows the difficulty of fighting it as it keeps on being amongst the prevalent types of cybercrime in banks.

The interviews also identified hacking amongst the types of cybercrime present in their institutions. Amongst the respondents, one of them revealed that financial institutions possess a large amount of their customer's data due to the nature of services they offer. This has made financial institutions to be amongst the major targets for hackers as they extract personal information of the customers for fraudulent purposes. This was in the same view with Magutu et al (2011) who affirm that hackers target computer systems that have large databases such as that of banks to obtain identity related data on a large scale.

4.1.2 Identity theft

The finding shows that identity theft is amongst the worrisome types of cybercrime in the financial sector. The interviewees also cited identity theft as one of the most prevalent type of cybercrime in Zimbabwe's' financial institutions. Some interviewees however identified hacking, phishing and malicious software to be the major forms of identity theft. KPMG (2011) also categorised phishing, hacking and malicious software to fall under the identity theft type of crime. It is also noteworthy to point out that identity theft proved to be the centre of every other type of cybercrime in the financial institutions as it is the major aim of the offender to steal personal information of customers which will then be used to steal.

4.1.3 Malicious software

With slightly above half (53%) of the respondents considering malicious attacks to have an average occurrence rate, the prevalence rate is also worrisome for financial institutions. This finding complimented the studies which were conducted by Siddique & Rehman (2011) and KMPG (2011) who also identified malicious software as a type of cybercrime common in banks. Majority of the interviewees concurred that malicious software is prevalent in Zimbabwe's financial institutions but much of its exposure for the risk is emanating from services such as e-banking. This is due to the use of unsafe devices to access personal information. This was supported by Uppal, Mehra & Verma (2014) who revealed that e-banking is at risk of masked malwares such as Trojans which conceals its self to behave like legitimate programmes.

4.1.4 Phishing

Table 1 shows that half of the respondents considered prevalence rate of phishing to be average, whilst only 14 % considered it to be high. However, slightly above a third (36.1%) were of the view that the crime is either low (27.8%) or nonexistent (8.3%). Basing on the statistics, it is also safe to opine that phishing is a common type of cybercrime in the financial institutions in Zimbabwe. The crime was also cited by half of the interview respondents. The study findings are in tandem with the studies conducted by the Europol (2014) and Wada & Odulaja (2012) who listed phishing as one the major threats against individual and organizational private information in the financial sector.

4.1.5 Electronic card fraud

Though 41.7% of the respondents considered its prevalence rate as average, a significant percentage (47,2%) considered it to be either low (36.1%) or non-existent (11.1%). This shows that the threat is as significant as other threats. This can be explained by the fact that the Zimbabwean banking sector has not embraced the use of credit cards, though there is wide use of the debit cards. In other developed countries, the widespread use of the credit card results in an upsurge of electronic card fraud.

4.2 Current measures to combat cybercrime and their level of effectiveness

This was an open ended question which required the respondents to list the measures they have put in place within their organisations as a way to fight cybercrime. The respondents identified education and training through seminars and workshops, tight IT security, constant change of ICT technology to meet up with the changes, installation and constant updating of security measures such as anti-viruses, firewalls and firewalls data recovery sites. These all fall under the three broadways to overcome cybercrime which are cyber laws, education and policy making as suggested Saini and Rao (2012).

To add on, the interviewees responded to the same question and identified measures such as protection of the banking sector through access control measures, installation of biometric security and use of smart cards. They also suggested separating critical banking applications from the web through firewalls. This was in support of the study by Siddique & Rehman (2011) which recommended the following protection measures; hardware identification, access control software and disconnecting critical banking application from the web.

4.3 Effectiveness of Current Measures

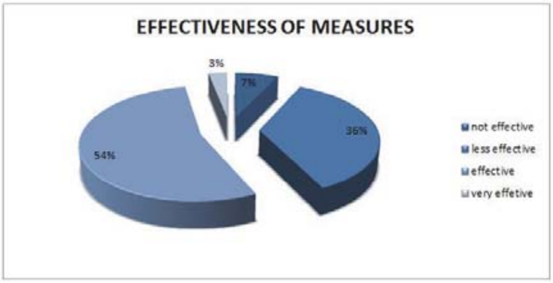

Figure 1: Effectiveness of measures

From the total respondents, 57% considered current control measures as either effective (54%) or very effective (3%) (Fig 1). The other 43% considered the measures as either less effective (36%) or not effective (7%). However, the statistics seem to be at tangent with the findings on the prevalence rate, with the prevalence rate pointing to inadequacies on the current preventive measures. Interestingly though, most of the interviewees indicated that the current control measures are not very effective and they admitted that it will be difficult to outwit the cyber criminals.

5. Conclusion

From the above findings, it can be concluded that cybercrime is prevalent in the financial institutions, with hacking, identity theft and malicious software as the most prevalent cyber threats. Whilst the literature survey pointed out the severity of cybercrime in developed nations, the findings point out that the scourge is also rampant in developing nations like Zimbabwe. Control measures such as training, updating of anti-viruses and firewalls top the list of current strategies to curb cyber crime. Despite the presence of these control measures to protect banks from being victims, keeping their security systems up to date is difficult, as it is being outpaced by the changes in technology itself. Based on the findings of this study, it can be concluded that cybercrime will remain the major threat to financial institutions and the challenge will be compounded by the swift pace by which technology is advancing. Admittedly, the financial services sector is the back bone of the economy in any nation, hence the glaring need for dealing with the threat.

6. Recommendations

- Education of employees is the best defence against many threats. However, this is most effective when organisations break away from traditional security awareness models to employ creative and immersive techniques, and deploy technologies that can influence user behaviours.
- Multi-layer security, including firewalls, secure sign-on, dual authentication with triangulation of access and real- time business event monitoring helps protect against data failings from external attacks
- Improved real-time tracking and business intelligence will alert institutions to any security breach. The ability to monitor every transaction across global operations will be the key to protecting against internal and external threats.
- New technologies, such as mobile banking applications or payment, need to be considered within the overall security framework. This will be critical from a cost and resource perspective. Applications, procured through line of business functions, can operate outside of the core infrastructure which will impact on the security and risk posture of the organisation.

References

Adelaja, O., (2012) Catching Up With The Rest Of The World: The Legal Framework Of Cybercrime In Africa

Akuta, E., A., M., Ong'oa, I. M., & Jones, C.R., (2011) Combating Cyber Crime in Sub-Sahara Africa; A Discourse on Law, Policy and Practice Journal of Research in Peace, Gender and Development Vol. 1(4) pp. 129-137, May 2011

Albrecht, W., S., Hill, N. C., & Albrecht, C. C. (2006). The ethics development model applied to declining ethics in accounting. Australian

Accounting Review, 16(1), 30-40.

Almarri, S., and Sant, P., (2014) Optimised Malware Detection in Digital Forensics. International Journal of Network Security & Its Applications (IJNSA), Vol.6(1).

Arcuri, M., C., Brogi, M., & Gandolfi. G., (2012) Effects Of Information Security, JBreaches on Stock Returns: Is cybercrime a threat to firms?

Bamoriya, P., Bamoriya.H ., & Singh P., (2014) Perceptual mapping of electronic banking channels in India: A Multidimensional Scaling approach. International Journal of Research Studies in Management 2014 April, Volume 3 (1), 17-26

Bamrara, A., Singh,G., and Bhatt. M., (2013), Cyber-attacks and defense strategies in India: An empirical assessment of banking sector, International journal of cyber criminology, Volume 7(1) pp49-61.

Bawane, M.S., and Shelke, C.J., (2014) Analysis Of Increasing Hacking And Cracking Techniques. International Journal of Application or Innovation in Engineering & Management Volume 3(2), February 2014

Boateng ,E.O., & Amanor P.M., (2014) Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices. Journal of Emerging Trends in Computing and Information Sciences Vol. 5, No. 4 April 2014

Broadhurst, R. (2006) Developments in the global law enforcement of cyber-crime Policing: An International Journal of Police Strategies and Management29(2) : pp. 408-433.

Chaudhary, G., K. (2014) Development Review on Phishing: A Computer Security Threat International Journal of Advance Research in Computer Science and Management Studies Volume 2, Issue 8, August 2014 pg. 55-64.

Chimheno, R., M., & Dehgantanha, A. (2014), Framework for cybercrime law implementation in Zimbabwe.

Cole, S.A., & Pontell, H. (2006). Don't below hanging fruit: identity theft as moral panic. In T. Monahan (Ed.), Surveillance and security (pp. 125−147). London: Routledge

Cornish, D. B., and Clarke, R. V. G., (1987). The Reasoning Criminal: Rational Choice Perspectives on Offending, New York: Springer-Verlag.

Douglas, T., & Loader, B. D. (2000). Cybercrime: Security and surveillance in the information age, UK: Routledge

Europol. (2014). 'The Internet Organised Crime Threat Assessment'. The Hague: Europol.

Ghosh. S., & .Turrini. E., (2011). Cybercrimes: A Multidisciplinary Analysis. Springer-Verlag Berlin Heidelberg, 2011.

Hassan, B., A., Lass, F., D & Makinde, J. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. ARPN Journal of Science and Technology VOL. 2, NO. 7.

Hedayati, A. (2012) An analysis of identity theft: Motives, related frauds, techniques and prevention. Journal of Law and Conflict Resolution Vol. 4(1), pp. 1-12, January 2012.

Herselman, M. & Warren, M. (2010). Cyber Crime Influencing Businesses in South Africa Issues in Informing Science and Information Technology.

Hutcchings. A. & Hayes, H. (2009) Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the 'Net'? Current Issues in Criminal Justice Volume 20 Number 3 .

Jangara, T., B. (2014). Cyber Threats and Cyber Solutions: managing the growing incidents of fraud in business. 1st Internal Control Institute Congress for Africa 30 – 31 October 2014pp 1-22

Jaishankar, K. (2008). Space Transition Theory of cyber crimes. In Schmallager, F., & Pittaro, M. (Eds.), Crimes of the Internet. (pp.283-301) Upper Saddle River, NJ: Prentice Hall.

KPMG (2011). Cyber Crime – A Growing Challenge for Governments July 2011, Volume 8.

KPMG (2012). Cybercrimes: A Financial Sector Review. Government and Public Sector.

Kritzinger, E. and Von Solms, S. (2012) A Framework for Cyber Security. Africa Journal of Information Assurance &Cybersecurity Vol. 2012 (2012)

Magutu, P., O., Ondimu, G., M & Ipu, C., J. (2011) Effects of Cybercrime on State Security: Types, Impact and Mitigations with the Fiber Optic Deployment in Kenya. Journal of Information Assurance & Cyber security Vol. 2011.

Mbiti, I., & Weil. D., N. (2011) Mobile Banking: The Impact Of M-Pesa In Kenya. National Bureau Of Economic Research Working Paper 17129 http://www.nber.org/papers/w17129.

McNally, M., & Newman, G. (2008). Perspectives on identity theft. Monsey, NY: Criminal Justice Press.

McQuade, S. (2006) Understanding and Managing Cybercrime, Boston: Allyn & Bacon.

McQuade, Samuel.(2008) "Cybercrime." In The Oxford Handbook of Crime and Public Policy, by Michael Tonry. Oxford: Oxford University Press, 2011.

Metcalf, R. & Kirst, K. (Eds) (2013). Cyber security and the retail consumer sector. Retail and Consumer insights 2/2013 [Online], Available from: newsletter.pwc.in/inxmail9/images/R&Cinsights/IssuesApril2013/PwC,R&CInsights1,2013,corr.pdf. Accessed on 25/10/2015.

Mugari, I. (2016). Perspectives on Cyber- Threats to the Retail Sector. A Case Study of Eastgate Shopping Mall. International Journal of Innovative Research And Development Vol 5 (3), 180- 187.

Quarshie, H.,O. & Odoom, A., M., (2012) Fighting Cybercrime in Africa. Scientific and Academic publishing Vol.2, No.6, October 2012.

Raghavan, A., R. & Parthiban, L. (2014). The effect of cybercrime on a Bank's finances. International Journal of Current Research & Academic Review; Volume-2 Number 2 173-178.

Roderic, G. et al. (2006). 'Cyber-crime: The Challenge in Asia,'" University of Washington Press, USA.

Roger, E.,S. (2008) Rogers Communications Inc, 2008 Annual Report.

Saini, H., Rao, Y.,S, Panda, T.,C (2012) Cyber-crime and their Impacts: A Review International Journal of Engineering Research and

Applications: Vol. 2, Issue 2, Mar-Apr 2012, pp.202-209 .

Sarannia, A. & Padma, U., R. (2014) Prevention Model For Phishing Attacks In Web Applications Using Linkguard Algorithm. International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 1.

Sarrab, M., Aldabbas, H.,& Elbasir, M. (2013) Challenges of Computer Crime Investigation In North Africa's Countries. The International Arab Conference on Information Technology (AaCIT'2013).

Sauser, W. (2007). Employee theft: Who, how, why, and what can be done. S.A.M. Advanced Management Journal, 72(3), 13-25.

Sharma, A.,K & Nanda, G., L. (2006). "Frauds in Credit Card Business", Banking Finance, July , Volume, Issue no.7.

Siddique, M., I., Rehman, S. (2011). Impacts of Electronic crime in Indian Banking Sector .

Sonepat, R. & Sonepat, S. (2014) Analysis on Credit Card Fraud Detection Methods. International Journal of Computer Trends and Technology (IJCTT) – volume 8 (1).

Soni, R., R & Neena (2013). An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks.

Sussmann, M., A. 1999, 'The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium', Duke J. of Comp. & Int'l L., 9:451.

Symantec (2012). Internet Security Threat Report 2011 Trends. Mountain View, CA:Symantec Corporation.

Symantec (2013). Internet Security Threat Report 2013. Mountain View, CA: Symantec Corporation.

United Nations Office on Drug Crime. (2013). Comprehensive study on Cybercrime ,United Nations UK.

Uppal, D., Mehra, V. & Verma, V. (2014). Basic survey on MalwareAnalysis,Tools and Techniques. International Journal on Computational Sciences & Applications (IJCSA) Vol.4.

Vrancianu, M., & Popa, L. A. 2010. Considerations Regarding the Security and Protection of E-Banking Services Consumers Interests. The Amfiteatru Economic Journal, 1228: 388-403.

Wada, F., & Odulaja, G. O. (2012). Assessing Cyber Crime and its Impact on E-Banking in Nigeria Using Social Theories. African Journal of Computing & ICT, 5, 69-82.

Wada, F., Longe, O., & Danquah, P. (2012) Action speaks louder than words- Understanding cyber criminal behaviour using criminological theories. Journal of Internet banking and Commerce Vol 17(1).

Wall, D. (2007). Cybercrimes and the Internet. Crime and the Internet.

Yar M, (2005). 'The novelty of "cybercrime": An assessment in light of routine activity theory'. European Journal of Criminology, Vol 2 (4) pp 407-427.

Yassir, A. & Nayak, S. (2012) Cybercrime: A threat to Network Security International Journal of Computer Science and Network Security Vol.12 (2).