INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Perspectives on Cyber Threats to the Retail Sector in Zimbabwe: A Case Study of East Gate Shopping Mall

Ishmael Mugari
Lecturer, Department of Intelligence and Security Studies, Bindura University of Science Education, Zimbabwe

Abstract:
Great strides have been made in the information and communication technology (ICT) arena in the past two decades. Whilst the cyberspace has brought positive results to the business environment, new criminal threats have also evolved. These threats are known as cybercrime. It is imperative for businesses to understand the threats posed by the technological environment. This study, which was conducted at Eastgate Shopping Mall (Harare, Zimbabwe), sought to explore the level of adoption of ICT infrastructure by the retail sector, as well as to document the nature of cyber threats to this sector. It was found out that the retail sector in Zimbabwe has greatly embraced the ICT in their operations, as evidenced by hardware, use of internet and adoption of ICT based payment systems. Dominant threats to the retail sector include infection of computers with viruses and unauthorized access to computers and computer networks. Debit card fraud and fraudulent RTGS transactions rarely occur in the Zimbabwean retail sector. Awareness campaigns, promulgation of new cyber crime laws, crafting of a national ICT policy and collaboration between retailers and banks are the recommended measures to deal with retail cyber threats.

Keywords: *Cyber threats, cyber security, retail sector*

1. Introduction

Worldwide business systems have undergone structural changes, which have been caused by rapid advancement in technology. Business models, both in the financial sector and other sectors have been redefined, with technology now being regarded as a driver rather than an enabler in conducting business operations. Retailing has become multichannel, driven by evolving technologies and interactive, customer- focused applications (Metcalf & Kirst, 2013). The retail sector is increasingly virtual, as new technology and interactive mobile devices are profoundly changing consumer shopping patterns, and radically redefining the business environment from an exclusively physical to an omnipresent virtual place (Metcalf & Kirst, 2013). The use of e-payments in the market place for retail payments, including the Electronic Funds Transfer at Point-of-Sale (EFTPOS), E-banking, telephone banking, internet banking, E-debit and E-money has become a common and well accepted practice in the advanced countries that have extensive and well developed telecommunication network and infrastructure (Hataiseree, 2008:265).

With the increasing benefits brought about by the introduction of ICTs in business, new threats have also emerged. While the use of computers and the internet may raise efficiency in the business operations, the potential benefits need to be weighed against the threats posed by the increasing use of the information and communication technology. Davis & Hutchison (1997) highlight that computers and the internet have brought an array of new crime and consequently, a series of new challenges in the fight against this new threat. With the increasing usage of the internet, the fears of privacy abuse become a top concern of most of the internet users (Raja, Velmurgan & Seetharamon, 2008). Though the internet is famed for its security and anonymity, there are however numerous situations in which customers' personal information has been compromised by cyber criminals (Wagenaar, 2014).

Given the global nature of the internet, business sites have become targets for external organized criminal groups, creating new information security requirements for retailers to address (Metcalf & Kirst, 2013). Connected organizations impose a risk on information systems that cut across organizational borders and subject an organization to additional risks (Wagenaar, 2014). For example, a retail outlet whose network is linked to a financial institution's network or to a parent company outside the country will face more cyber threats.

The threat of cyber crime also needs to be understood in the context of its effects to the business environment, as Wright (2015) highlights that cyber attacks lead to damage to reputation arising from loss of commercially sensitive information and reactive costs incurred in responding to data leaks as well as legal consequences such as monetary fines. Negative customer comments over the social media can also negatively affect brand loyalty. As Wagenaar (2014) highlights, customers are willing to engage with retailers through loyalty programs and personalized offers. However, this will be difficult due to internet data security concerns, thus

negatively affecting business growth and innovation. Information technology based innovations are thus prone to cyber attacks and this can interfere with future innovations.

With this background, this study was carried out at Eastgate Shopping Mall, which is in Harare, the capital city of Zimbabwe. Eastgate shopping mall is a five storey shopping mall with diverse retail business such as clothing, household furniture, electrical appliances, food outlets and pharmaceuticals. With diverse retail outlets under one shopping mall, Eastgate Shopping Mall was considered as a Case Study which can guide the rest of the retail sector in Zimbabwe on the threats of cybercrime. The study sought to explore the level of adoption of Information and Communication Technology (ICT) infrastructure as well as to document the nature of the cyber threats to the retail sector. The study sought to address the following research questions;

a) What is the level of adoption of ICT infrastructure by the Zimbabwean retail sector?
b) Which ICT related payment systems are being used by the Zimbabwean retail sector?
c) Which cyber threats are prevalent in the retail sector?
d) To what extent has the retail sector been able to deal with cyber crime?
e) What strategies can be implemented to curb cybercrime?

2. Literature Review

2.1. Cybercrime

Cyber crime is any crime that is committed using a computer or a computer network. The Criminal Law (Codification and Reform) Act [Chapter 9:23] of Zimbabwe (herein after referred to as The Criminal Law Code) defines a computer as a device or apparatus or series of devices which by electronic, electromagnetic, electromechanical or other means, is capable of one or more of the following:

a) Receiving or absorbing data and instructions supplied to it;
b) Processing data according to rules or instructions;
c) Storing and additionally, or alternatively, reproducing data before or after processing the data.

It goes on to define a network as the interaction of one or more computers through-

a) The use of satellite, microwave, terrestrial line or other communication media; or
b) Computer terminals or a complex consisting of two or more interconnected computers, whether or not the interconnection is continuously maintained.

Davis and Hutchison (1997) state that computers, through the use of the internet, have brought an array of new crime nomenclature and consequently, a series of new challenges in the fight against this new threat. Cybercrime can be regarded as "computer-mediated activities which are illegal or considered illicit by certain parties and which can be conducted through global electronic networks" (Thomas and Loader, 2000). It differs from physical or "terrestrial" crime in four main ways: being easy to commit, requiring minimal resources for great potential damage, being committable in a jurisdiction in which the perpetrator is not physically present, and often, not being entirely clearly illegal (Aseef et al, 2005).

2.2. Nature of Cyber Threats

2.2.1. Malware

According to Uppal, Mehra & Verma (2014) malware is when an unauthorized programmed is installed into a computers system secretly with the intention of stealing information. By merging the words 'malicious' and 'software', the term malware is created. Most of malware enters the system while downloading files over the internet and it scans for vulnerabilities of the operating system (Gaikwad, Motwani & Shinde, 2015). Magutu et al (2011) supported this by saying that malware moves between computer and network systems so as to modify systems without the owner's permission. Roderic et al (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.

2.2.2. Hacking

Hacking is one of the oldest computer crimes and the unlawful access to systems or databases to obtain personal or organizational confidential information is referred to as hacking (Broadhurst, 2006). The availability of personal information online has made it easier for perpetrators to steal from business organizations and individuals (Magutu et al 2011). 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 systems host that has large data base so as to obtain identity related data on a large scale.

2.2.3. Card fraud

Stealing bank or credit card details is another major cybercrime (Chavan et al, 2011). Most of the retail outlets have point-of –sale terminals where clients can use debit and credit cards to make payments. However, as Metcalf & Kirst (2013) point correctly point out, Point of Sale (POS) attacks can result in credit and debit card information being stolen. Duplicate cards are then used to with draw

cash at ATMs or in shops. Section 167 of the Zimbabwe Criminal Law Code criminalizes unauthorized use or possession of debit cards.

2.2.4. Denial-of-Service (DOS)

It is an attempt to bring down a personal website, computers or networks, often by flooding them with messages (Chavan et al, 2008). These attacks flood business websites with internet traffic, rendering them unreachable by their customers for various lengths of time (Dhameja, Jacob & Porter, 2013). This slow down of internet activity will eventually result in reduced business for those businesses that mainly rely on the internet.

2.2.5. Viruses and Worms

A computer virus refers to a small program with harmful intent and has ability to replicate itself and it may spread from an infected computer to another through network or corrupted media such as floppy disks and USB drives (Gaikwad, Motwani & Shinde, 2015). It can also be defined as a computer program that affects the storage devices of a computer or network, which then replicate information without the knowledge of the user (O'Brien & Makaras, 2011). Section 164 of the Zimbabwe Criminal Law Code provides that, "Any person who, without authority from the owner of the computer or computer network, knowingly introduces or causes to be introduced any computer virus into any computer or computer network shall be guilty of deliberate introduction of a computer virus into a computer or computer network". Gaikwad, Motwani & Shinde (2015) define a worm as a self replicating program which uses network to send copies of itself to other systems invisibly without user authorization. Worms cause harm to the network by consuming the bandwidth.

2.2.6. Smart Phones and Mobile Applications Threats

Many smart phone based applications have not been developed with security in mind, and are often not compliant with best practices (Metcalf & Kirst, 2013). According to the McAfee National Cyber Security Alliance survey, 57 % of smart phone users in the United States have never backed up their devices, and 63 % have never installed protective security software. In Zimbabwe, two leading mobile phone operators, Ecocash and Telecel, have developed mobile money transfer services namely ecocash and telecash respectively.

Given the nature of the cyber threats and the magnitude of their impacts, it is imperative for the retail sector to take necessary precautions against the scourge of cyber crime. Organizations in the retail sector are increasingly accumulating data and will even more rely on data and IT systems in the future (Wagenaar, 2014). With the dependence on data and IT increasing, the impact of a cyber security incident becomes larger. The retail sector is fast moving towards online payments and these payment methods expose the sector to various cyber threats. Some of the costs which are incurred in the fight against cyber crime include; hiring external computer forensic experts, loss of customers whose private data would have been compromised, cost of civil suits for data breaches and impaired reputation.

3. Methodology

The study combined both quantitative and qualitative research designs, with questionnaires and in-depth interview guide as the key research instruments. Respondents were invited to participate using a systematic random sampling and purposive sampling techniques. Respondents comprised of employees as well as owners of retail outlets at Eastgate Shopping Mall. Quantitative data was coded and fed into SPSS software for analysis. Qualitative data was analyzed using content analysis and was used to complement quantitative data.

3.1. Demographic Data

Variable	Variable Description	Frequency	Percent
Gender of Respondents	Male	12	46.2
	Female	14	53.8
Respondents' age ranges	Less than 20 years	2	7.7
	20 -24 years	11	42.3
	25- 29 years	5	19.2
	30- 34 years	6	23.1
	35 years and above	2	7.7
	Total	26	100
Respondents' highest level of education	Ordinary level	4	15.4
	Advanced level	4	15.4
	Certificate/ Diploma	10	38.5
	Undergraduate degree	6	23.1
	Post graduate degree	1	3.8
	Other	1	3.8
	Total	26	100
Nature of respondent' s business	Clothing and footwear	9	34.6
	Furniture	4	15.4
	Household electrical appliances	5	19.2
	Computers, cell phones and accessories	4	15.4
	Other	4	15.4
	Total	26	100
Period in Employment	Less than 1 year	4	15.4
	1 - 2 years	7	26.9
	3 – 4 years	8	30.8
	5 years and above	7	26.9
	Total	26	100

Table 1: Demographic characteristics of respondents

The gender distribution of the respondents was almost even, with female respondents (53.8%) slightly surpassing their male counterpart (Table 1). The modal age range was 20-24 year age group, which constituted 42.3% of the total respondents. The age groups of below 20 years and above 35 years had the least numbers of respondents, contributing 7.7% apiece. Most of the respondents (38.5%) had a certificate or a diploma as their highest qualification, followed by undergraduate degree holders who constituted 23.1%. those with Ordinary level and Advanced level qualifications constituted 15.4% apiece. This shows that the bulk of the respondents was mature and qualified enough to comprehend important aspects of this study.

The clothing and footwear business provided most of the respondents, with 34.6% of the respondents being engaged in the business. Those who deal with household appliances and furniture constituted 19.2% and 15.4% respectively. Computer, cell phones and accessories business provided 15.4% of the respondents. Other business also provided 15.4% of the total respondents. Other business included restaurants and pharmaceutical businesses. The modal period in employment was 3 - 4 years, with 30.8% of the total respondents. Only 15.4% of the total respondents had been in the retail business for less than a year. These statistics indicate that the key retail sector businesses were well represented in the study, with most of the respondents having vast experience in the retail business.

4. Research Findings and Discussion

4.1. ICT Infrastructure and Usage

4.1.1. Hardware and Software

Respondents were asked to indicate the availability and use of ICT infrastructure and network at their workplaces. For the purpose of data coding, the responses were numbered 1 to 4, with the numbers denoting; 1- Not available, 2- Available with low usage, 3- Available with moderate usage, and 4- available with high usage. The resultant statistics are shown on Table 2.

Variable description	Not Available	Available with low usage	Available with moderate usage	Available with high usage	Mean	Standard deviation
	1	2	3	4		
Availability and use of computers	0%	0%	3.8%	96.2%	3.9615	0.19612
Availability and use of intranet	26.1%	13.6%	0%	60.9%	2.9565	1.36443
Availability and use of the internet	3.8%	19.2%	15.4%	61.5%	3.3462	0.93562

Table 2: Availability and use of hardware and network

All the respondents indicated that computers are present at their work places. An overwhelming majority (96.2%) indicated that there is high usage of computers. The mean statistic of 3.9615 and a standard deviation of 0.19612 pointed to high usage of computers. Internet is also being widely used, with 61.5% indicating high usage. The mean statistic for internet use was 3.3462 with a standard deviation of 0.93562. Slightly above a quarter (26.1%) of retail shops did not have intranet facilities. Interesting though, 60.9% indicated high usage of the intranet, while none indicated moderate usage.

All the retail outlets that were visited for data gathering had computers and this was also confirmed by all the interview respondents. Most of the interviewees highlighted that their customers' data as well as all information pertaining to the business transactions is stored in the computers. Most of the retail outlets have access to the internet through both network cables and wireless frequency (WIFI). With most of the retail outlets being branches, intranet is mainly used to communicate with other branches though out the country. The researcher however noted during the in depth interviews that some of the interviewees could not distinguish between intranet and internet. These statistics are supported by Wagenaar (2014), when he opines that organizations in the retail sector are increasingly accumulating data and will even more rely on data and IT systems in the future. The availability of computer hardware, as well as the wide usage rate of the internet implies that cyber security is a critical issue for retail outlets.

4.1.2. Payment Systems

Respondents were also asked to indicate the availability and usage rate of the given payment systems. The statistics are tabulated as follows;

Variable description	Not Available	Available with low usage	Available with moderate usage	Available with high usage	Mean	Standard deviation
	1	2	3	4		
Availability and use of debit card facility	30.8%	7.7%	30.8%	30.8%	2.6154	1.23538
Availability and use of credit card facility	88.5%	3.8%	7.7%	0%	1.1923	0.56704
Availability and use of ecocash/ telecash facilities	0%	19.2%	57.7%	23.1%	3.0385	0.66216
Availability and use of RTGS facility	44.0%	24.0%	20.0%	12.0%	2.0000	1.08012

Table 3: Available payment system and extent of their usage

From the above statistics, cell phone payment systems (Ecocash and telecash) are the dominant ICT based payment systems in the retail sector. A total of 80.8% of the respondents considered the payment method's usage to be moderate (57.7%) or high (23.1%), with a mean statistic of 3.0385 and a standard deviation of 0.66216. Debit card payments are also high, with 30.8% apiece indicating the payment method as either moderate or high. The mean statistic for debit card payments was 2.6154, with a standard deviation of 1.2354. There seems to be low usage of RTGS facility as indicated by a mean statistic of 2.0000 and a standard deviation of 1.08012. Credit card facilities are not yet available in the retail sector in Zimbabwe, as denoted by a mean statistic of 1.1923 and a standard deviation of 0.56704.

The above statistics point to the fact that the retail sector in Zimbabwe has embraced ICT based payment systems, in addition to cash based payments. This could possibly be due to the liquidity crunch which is affecting all the sectors of the economy. The liquidity crunch has at times led to shortage of cash in the banks, with some banks resorting to limiting the maximum withdrawal amounts. Three of the 8 interviewees indicated that most of their loyal customers prefer to use debits cards and mobile phone transfers rather than transacting in cash. As Metcalf & Kirst (2013) concurs, the adoption of internet and mobile phone based payment systems inevitably expose the retail sector to cyber threats.

4.2. Cyber Threats

4.2.1. Level of Knowledge on Cyber Threats

Respondents were asked to indicate their level of knowledge on cyber threats. Their responses were coded as follows; 1- no knowledge, 2- Little knowledge, 3- Average knowledge, 4- Very common.

Variable	No knowledge	Little knowledge	Moderate knowledge	Vast knowledge	Mean	SD
	1	2	3	4		
Level of knowledge on cyber threats	11.5%	26.9%	46.2%	15.4%	2.6538	0.89184

Table 4: Respondents' level of knowledge on cyber crime

The above statistics indicate that most of respondents (46.2%) had moderate knowledge on the cyber threats, while 38.4% either had little knowledge or no knowledge. The mean statistic of 2.6538 and a standard deviation of 0.89184 pointed to the fact that most of the respondents had little knowledge about cyber threats. However, with the rate at which the retail sector is adopting ICT applications, one would have expected an exponential rise in the level of knowledge of cyber threats.

4.2.2. Types of Cyber Threats

Respondents were asked to indicate the prevalence rate of specified cybercrimes in their organizations. Their responses were coded as follows; 1- Doesn't occur, 2- Rarely occurs, 3- Common, 4- Very common. Table 5 shows the responses, as well as the means and standard deviation.

Variable description	Doesn't occur	Rarely occurs	Common	Very common	Mean	SD
	1	2	3	4		
Unauthorized access to computers and networks	19.2%	30.8%	50.0%	0%	2.3077	0.78838
Infection of computers with viruses	3.8%	3.8%	53.8%	38.5%	3.2692	0.72430
Malicious software attacks	32.0%	36.0%	32.0%	0%	2.0000	0.81650
Debit card fraud	57.7%	34.6%	7.7%	0%	1.5000	0.64807
Credit card fraud	100%	0%	0%	0%	1.0000	0.0000
Fraudulent RTGS transactions	64.0%	36.0%	0%	0%	1.3600	0.48990
Denial of service attacks	54.2%	41.7%	4.2%	0%	1.5000	0.58977

Table 5: Types of cyber crime and their prevalence

As depicted by Table 5, infection of computers with viruses seems to be the dominant cyber threat in the retail sector. This is depicted by the mean of 3.2692 and a standard deviation of 0.72430, indicating that the threat is common. Half of the respondents indicated that unauthorized access to computers and networks is common, and this threat had a mean of 2.3077 and a standard deviation of 0.78838. Debit card fraud and denial of service attacks had a mean of 1.500 apiece, indicating that their prevalence rate is insignificant. Majority (64.0%) indicated that fraudulent RTGS transactions do not occur at their work places. All the respondents indicated that credit card fraud does not occur at their work places. This gives credence to the fact that financial institutions in Zimbabwe are hesitant to issue credit cards.

Though infection of computer systems with viruses was cited as the dominant cyber threat, most of the citizens are not aware of the seriousness of this threat. Malicious software attacks and denial of service attacks are both serious dimensions of the effects of computer viruses.

Though some interviewees were not conversant with malicious software attacks and DOS attacks, they however indicated that they sometimes witness unusually slow connectivity. Such slow connectivity can however emanate from virus attacks. Debit card fraud is a rare occurrence possibly due to the security features of a debit card as opposed to credit cards. Very few banks in Zimbabwe offer debit cards for which card-not-present transactions can be performed, hence minimizing the prevalence rate of debit card fraud.

The above cyber threats are summed up under Chapter VIII of the Zimbabwean Criminal Law Code as follows;

- Section 163. Unauthorised access to or use of computer or computer network.
- Section 164. Deliberate introduction of computer virus into computer or computer network.
- Section 165. Unauthorised manipulation of proposed computer programme.
- Section 167. Unauthorised use or possession of credit or debit cards.
- Section 168. Unauthorized use of password or pin-number.

4.3. Retail Sector's Preparedness in Dealing with Cyber Threats

Table 6 shows that only 32% of the respondents were inclined to agree to the fact that their organizations had the ability to deal with cyber threats. Other respondents were neutral (28.0%) or were inclined to disagree (32.0%) with the fact that they can deal with cyber

threats. The mean statistic of 2.8400 points to the fact that majority of the retail outlets are not yet prepared to deal with the threat of cyber crime.

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean	SD
	1	2	3	4	5		
Ability of organization to deal with cyber threats	12.0%	20.0%	28.0%	28.0%	4.0%	2.8400	1.1060

Table 6: Respondent organizations' ability to deal with cyber threats

The retail sector in Zimbabwe is not yet prepared to deal with cyber threats. This lack of preparedness, coupled with inadequate knowledge on the nature of cyber threats leaves the retail sector vulnerable.

5. Strategies to Deal with Cyber Threats

5.1. Awareness Campaigns

With the ICT revolution upon us, the general population needs to be educated on both the benefits and the risks of adopting ICT. With the statistics pointing to the fact that the retail sector players have little knowledge on cyber threats (Table 4), the panacea for this knowledge gap would be to provide them with the requisite information. Workshops and seminars should be arranged for all retail sector players to educate them with the threats posed by adopting ICT.

Table 7 shows that most of the respondents had no knowledge (53.8%) or little knowledge (30.8%) about the laws that deal with cyber threats. The mean statistic of 1.6154 and a standard deviation of 0.75243 pointed to the fact that the majority of the respondents had little knowledge on cyber threats.

	No Knowledge	Little Knowledge	Moderate Knowledge	Vast Knowledge	Mean	SD
	1	2	3	4		
Level of knowledge on laws which deal with cyber threats	53.8%	30.8%	15.4%	0%	1.6154	0.75243

Table 7: Respondents' level of knowledge on laws which deal with cyber threats

Though the laws dealing with cyber threats have been promulgated, most of the players in the retail sector are not aware of the specific provisions that relate to the threat. When the researcher highlighted some of the statutory provisions that deal with cyber crime to the interviewees, some of the interviewees concurred that some of the cyber crimes were happening frequently at their work places. The general public should also be informed of these important statutory provisions and this can be achieved through publication in the local daily newspapers.

5.2. Promulgation of New Cyber Crime Laws

The current Criminal Law Code was promulgated in 2004, when the nation had not yet widely embraced ICT. The current provisions fall short in addressing the current threats posed by the ever changing ICT discourse. Though the issue of promulgating new cyber laws has been discussed in Parliament, there is need for the lawmakers to move with speed as these cyber threats do not only affect retail businesses but also other key economic sectors. In addition to the relevant laws, there is also need for a national cyber crime policy which can be crafted by leading academics as well as representatives from law enforcement agents. Such a policy will guide all economic players on all issues pertaining to ICT.

5.3. Robust ICT Strategies by Retail Organizations

Given the nature of cyber threats, retail organizations should adopt a robust security strategy, based on an assessment of threats, vulnerabilities and business impacts. These should be tied to an effective security management regime which includes appropriate risk mitigation. Penetration testing should be carried out frequently to test the vulnerability of the ICT systems.

5.4. Collaboration

The retail sector should collaborate with the financial institutions when they implement their cyber security measures. This collaboration will reduce online payment and electronic card related risks. Wagenaar (2014) concurs that sharing and correlating information could help detecting those threats in an early stage. An example is an incident of debit card fraud, which calls for both the bank and the retail shop to collaborate during the investigations.

6. Conclusion

The Zimbabwean retail sector has greatly embraced the ICT, with most retail outlets using various computer applications in their daily duties. In addition to cash based payments, online and mobile phone based payments are also on the rise, with ecocash/telecash and

debit card payments toping the non- cash payment systems. Though at a lower rate, RTGS transactions are also being used by retailers. The adoption of ICT has created new threats to the retail sector, chief among them being infection of computers with viruses and unauthorized access to computer networks. Though there are laws which deal with cyber crime in Zimbabwe, the laws are inadequate, thus calling for the need for promulgation of new comprehensive cybercrime laws.

7. Abbreviations

- ATM- Automated Teller Machine
- ICT- Information and Communication Technology
- RTGS- Real Time Gross Settlement System
- DOS- Denial Of Service
- Malware- Malicious Software

8. References

i. Aseef et al. 2005. Cyber-Criminal Activity and Analysis. White Paper, Fall [Online]. Available on: https://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/team2-whitepaper.pdf. Accessed on 30/ 09/2015.
ii. Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime Policing: An International Journal of Police Strategies and Management 29(2): pp. 408-433.
iii. Chavan. P., Aggawal. R, Bajaj, K, Agrawal, N. (2011), Cybercrime: A financial sector view, KPMG publishers, India.
iv. Davis, R. W. K. & Hutchson, S. C. (1997). Computer crime in Canada, Carswell, Toronto.
v. Dhameja, S, Jacob, K & Porter, R. D. 2013. Clarifying liability for twenty-first-century payment fraud. Federal Reserve Bank of Chicago. Economic Perspectives 3Q/2013.
vi. Gaikwad, P., Motwani, D. & Shinde, V. (2015). Survey on malware detection techniques. International Journal of Modern Trends in Engineering and Research. Vol 2(1).
vii. Hataiseree, R. (2008). The development of e-payment and challenges in Thailand [Online] available from: www.seacen.org/au1/pdf/publication/research_prj/2008/rp71/Chapter10.pdf. Accessed on 7/10/2015.
viii. 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 .
ix. 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.Accessedon 25/10/2015.
x. O'Brien & Makaras. (2011). Management Information Systems, 10th Edition, McGrawHill, New York.
xi. Raja, J., Velmurgan, M. & Seethyaraman, A. (2008). Epayment: Problems and prospects. JIBC Vol 13 (1).
xii. Roderic, G. et al. (2006). 'Cyber-crime: The Challenge in Asia,'" University of Washington Press, USA.
xiii. Republic of Zimbabwe. (2004). Criminal Law (Codification and Reform) Act [Chapter 9:23]. Government Printers, Harare.
xiv. Thomas, D & Loader, B. (Eds). (2000). Cybercrime: Lawenforcement, security and surveillance in the Information Age, Cambrigde University Press, UK.
xv. Uppal, D., Mehra, V. & Verma, V. (2014). Basi survey on malware analysis, tools and techniques. International Journal on Computational Sciences and Applications, Vol 4(1)
xvi. Wright, T. (2015). Retailers need to tackle inevitable cyber threats, Pillsbury, New York.
xvii. Wagenaar, J. (2014). Collaborative Cyber Security in the Retail Sector. Masters Thesis, University of Twente, Netherlands.