International Journal of Economics and Financial Issues

ISSN: 2146-4138

available at http: www.econjournals.com

International Journal of Economics and Financial Issues, 2017, 7(3), 760-767.

Cyberspace Enhanced Payment Systems in the Zimbabwean Retail Sector: Opportunities and Threats

Ishmael Mugari*

Bindura University of Science Education, 1020 Chimurenga Road, Bindura, Republic of Zimbabwe. *Email: ishiemugari@gmail.com

ABSTRACT

The cyberspace has revolutionised payment systems across the globe. The retail sector has also embraced cyberspace enhanced payment systems as an alternative or compliment to the conventional cash based payment systems. Whilst the cyberspace has brought positive results to the business environment, new criminal threats have also evolved. This study sought to explore the nature of cyberspace enhanced payment systems for the retail sector in Zimbabwe, as well as to document the nature of cyber threats to this sector. It was found out that use of debit cards, mobile money transfers and real time gross (RTGS) transactions top the list of cyberspace enhanced payment systems in the Zimbabwean retail sector. Dominant cyber threats to the retail sector include infection of computers with viruses and unauthorised access, whilst debit card fraud and fraudulent RTGS transactions infrequently occur in the Zimbabwean retail sector.

Keywords: Cybercrime, E-payments, Payment Fraud
JEL Classifications: E42, L81

1. INTRODUCTION

Business systems across the globe have undergone structural changes, which have been caused by rapid advancement in technology. To this end, business models in different sectors have been redefined, with technology now being regarded as a driver rather than an enabler in conducting business operations (Mugari, 2016). Retail business has become multichannel, driven by evolving technologies and interactive, customer- focused applications (Metcalf and Kirst, 2013). With the retail sector becoming increasingly virtual, new technology and interactive mobile devices are increasingly changing consumer shopping patterns, and radically redefining the business environment from an exclusively physical to an omnipresent virtual place (Metcalf and Kirst, 2013). The cyberspace revolution within the retail sector is summed up by Hataiseree, 2008. p. 265 as follows;

> "The use of e-payments in the market place for retail payments, including the electronic funds transfer at point of sale (POS), 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."

The growth in the electronic payments sector is accompanied by numerous economic and transactional benefits (Kathirvel, 2013). Electronic payments improve economic efficiency, make payments more secure and convenient, and provide the impetus for further economic and social development (Kathirvel, 2013. p. 172). According to (Lawrence and Tar, 2010), internet transactions provide great opportunities for business in terms of gaining access to markets across the globe, thus supporting economic growth. (Kunyaru and Kyalo, 2015) argue that businesses have migrated to online transactions in order to benefit from increased efficiency, reduced costs, and the ability to operate across various platforms in real time.

There has been a growing trend towards the use of cyber-enhanced non cash-based payment systems across the globe. According to the 2013 United States Federal Reserve Payments study, payments have become increasingly card-based and the number of debit card payments increased more than any other payment type from 2009 to 2012 (Federal Reserve System (FRS), 2013). In the same study, it was also revealed that about 2 thirds of consumer and business payments were made with payment cards (FRS, 2013). Similarly, the (Australian Payments Clearing Association [APCA], 2015. p. 6) reports that payment cards are the most common non-cash payment methods used by the Australian consumers. Cards are used for in-store purchases, withdrawals at automatic teller machines (ATMs), and increasingly, online shopping and mobile payments (APCA, 2015). In South America, (KPMG,2015) reports that Brazil has some of the highest number of ATMs, POS terminals and cards per capita in the world. It is important to emphasise that payment cards are now increasingly being used for card-not- present online transactions.

In Africa, several nations are also moving towards extensive use of cyber-enhanced payment systems. Mobile money, ATM payments, card payments (credit card and debit card), online payments and real time gross settlement (RTGS) settlement are the dominant non-cash based payment systems in Kenya (KPMG, 2015). In Nigeria, the dominant non-cash based payment systems include; POS, ATM, mobile and RTGS (KPMG, 2015). Similarly, South Africa, whose electronic payment transaction volumes continue to rise, has card payments, POS terminals, online payments, POS terminals and mobile payments as the dominant cyber-enhanced payment systems.

Despite the massive benefits that can and have been derived from the adoption of information technology (IT), as well as the inevitable trends towards adoption of cyber-enhanced payment systems across the globe, new threats to business have also emerged. While there is a general consensus that 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 (ICT). To this end, 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 fear of privacy abuse becomes a top concern of most of the internet users (Raja, et al., 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.

Several reports of reports of criminal activities relating to non-cash based payment systems have been reported across the globe. In the United States of America, the estimated annual number of unauthorised transactions in 2012 was 31.1 million, with a value of $6.1 billion, and payment cards had substantially higher total unauthorised transactions (FRS, 2013). According to APCA (2015), payment industry data for 2014 shows that fraud on Australian payment cards continues to increase in the card-not-present space. For the year 2014, the card fraud rate for Australia stood at 58.8% for every $1000 spent in Australia, while it stood at 75 pence for every $1000 spent in the United Kingdom (APCA, 2015). Schneider, as cited in Kunyaru and Kyalo (2015) argues that the level of fraud in online transactions is higher than telephone or in- person transactions. According to the South African Banking Risk Intelligence Centre, financial losses resulting from credit card fraud in South Africa increased by 53% between 2010 and 2011 (Budhram, 2012). Given the global nature of the internet, business sites have become targets for external organised criminal groups, creating new information security requirements for retailers to address (Metcalf and Kirst, 2013). The situation is compounded by the interconnectedness of business organisations, thus imposing a risk on information systems that cut across organisational borders and in the end subjecting organisations to additional risks (Wagenaar, 2014). Within the retail sector, 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 (Mugari, 2016). The threat of cybercrime also needs to be understood in the context of its effects to the business environment. Cyberattacks lead to reputation impairment 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 (Wright, 2015). Negative customer comments over the social media can also negatively affect brand loyalty (Mugari, 2016). Wagenaar (2014) highlights that customers are willing to engage with retailers through loyalty programs and personalised offers. However, this will be difficult due to internet data security concerns, thus negatively affecting business growth and innovation. IT based innovations are thus prone to cyber attacks and this can interfere with future innovations (Mugari, 2016. p. 180).

2. STUDY AIM AND OBJECTIVES

The study was aimed at exploring the nature and risks of cyberspace enhanced payment systems in the Zimbabwean retail sector. The specific objectives of the study are to: (*1*) Describe the ICTenhanced payment systems that are available in the Zimbabwean retail sector, (ii) highlight the threats that are peculiar to the ICT enhanced retail sector payment systems, and (iii) to determine the extent to which the retail sector is able to deal with cyber threats. The findings from this study will provide relevant context specific knowledge and important decision making information to both retail sector players and policy makers who are faced with the growing threat of cybercrime in a fast changing digital era. In addition, this study takes place during a period characterised by liquidity crises, coupled by the Reserve Bank of Zimbabwe's thrust towards moving the nation to a cashless society. This study therefore gives insights into the available non-cash based payment systems and the risks associated with the payment systems.

3. LITERATURE REVIEW

3.1. Cybercrime

The term cybercrime has been defined in many ways by different authors (Magutu et al., 2011) and it is difficult to come up with a single definition on the term. Yar (2005) also argues that the lack of a consistent and statutory definition for the activities that may constitute cybercrime make it difficult to analyse it. Perhaps a simpler definition is provided by the Council of Europe, who 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." (Thomas and Loader, 2000; Mugari et al., 2016). 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, with various forms and motives (Mugari et al., 2016). What is more common amongst different definitions is the central role of a computer and the computer networks in perpetrating cybercrime. The criminal law (Codification and reform) Act [Chapter 9:23] of Zimbabwe 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:

1. Receiving or absorbing data and instructions supplied to it
2. Processing data according to rules or instructions
3. 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
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; Mugari (2016. p. 181) state that computers and the internet have brought an array of new crime nomenclature and consequently, a series of new challenges in the fight against this new threat. Despite the divergent views on the concept of cybercrime, the term can precisely be defined as, “computer-mediated activities which are illegal or considered illicit by certain parties and which can be conducted through global electronic networks” (Mugari, 2016. p. 181). It differs from physical or “terrestrial” crime in 4main 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).

3.2. Nature of Cyber Threats

3.2.1. Card fraud

Given the fact that payment cards are amongst the dominant non-cash based payment systems across the globe (FRS, 2013; APCA, 2015), card fraud becomes a threat that business organizations have to grapple with. Card fraud entails fraudulent use of someone’s debit or credit card with the intention of obtaining money or paying for goods and services. Most of the retail outlets have POS terminals where clients can use debit and credit cards to make payments (Mugari et al., 2016). However, as Metcalf and Kirst (2013) point out, 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. A credit card, which provides the holder with credit to make purchases up to a limit fixed by the card issuer, is more prone to card fraud than debit cards. According to Budhram (2012), the enormous growth in the use of credit cards has resulted in high levels of credit card fraud. Technological advances have allowed the perpetrators to produce counterfeit cards that resemble the genuine card, thus making it difficult for shopkeepers, police and bank investigators to identify a fraudulent card (Budhram, 2012). The APCA (2015. p. 6) identifies five types of card fraud namely: Card-not-present; counterfeit/skimming; lost/stolen; never received; and fraudulent application. Card-not-present fraud entails unauthorized use of a consumer’s card details to purchase products or services in a non-face-to-face scenario, where the merchant has chosen to accept the transaction based on the card number alone. For counterfeit/skimming fraud, transactions are made with an altered or illegally reproduced card using details that have been obtained from an existing valid card. In a stolen/lost card fraud, a payment is made using a card that has been lost by or stolen from the rightful card owner. Never received card fraud involves transactions that are made on a card that was stolen before it was received by the rightful owner. Lastly, fraudulent application card fraud entails transactions that are made on a card where the account was established using someone’s identity or other false information (APCA, 2015).

3.2.2. Hacking and/unauthorised access

Hacking is one of the oldest computer crimes (Herselman and Warren, 2010) and involves trying to compromise a system’s security in order to gain unauthorized access (Easttom and Taylor, 2011). Hedayati (2012), Mugari et al. (2016. p. 137) 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). 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.

Closely related to hacking is unauthorized access, which Easttom and Taylor (2011. p. 12) define as a scenario in which a person accesses data that he or she has not been given permission to access. A common scenario is when someone who has legitimate access to some particular source of data chooses either to access data he or she is not authorized to access or to use the data in a manner other than how he or she has been authorized. In Zimbabwe, section 163 of the criminal law code seems to outlaw hacking by criminalizing unauthorized access to a computer network.

3.2.3. Viruses and worms

A computer virus refers to a small program with harmful intent and has ability to replicate itself (Mugari, 2016). It may spread from an infected computer to another through a computer network or corrupted media such as floppy disks and USB drives (Gaikwad et al., 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 andMakaras in (Mugari, 2016). 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 et al. (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 (Mugari, 2016).

3.2.4. Malware

Malicious software, which is commonly known as malware, is when an unauthorized programme is installed into a computers system secretly with the intention of stealing information (Uppal et al., 2014). Most of malware enters the system while downloading files over the internet and it scans for vulnerabilities of the operating system (Gaikwad et al., 2015). Subsequently, the malicious software moves between computer and network systems so as to modify systems without the owner's permission (Magutu et al., 2011). 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. Uppal et al. (2014), Mugari et al. (2016. p. 137) identified 2 categories of malware which are the contagious and masked. Under the contagious, he identifies viruses and worms, and under the masked, he identifies 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 (Mugari et al., 2016. p. 137).

3.2.5. Denial-of-service (DOS) attacks

A DOS attack is a category of non-access computer crimes. According to Easttom and Taylor (2011), a non- access computer crime encompasses a number of activities that can cause damage but do not involve the perpetrator actually gaining access to the target system. To this end, a DOS attack is an attempt to bring down a personal website, computers or networks, often by flooding them with messages (Chavan et al., 2008). Similarly, Easttom and Taylor, 2011 define a DOS attack as an attempt to prevent legitimate users from being able to access a given computer resource. These attacks flood business websites with internet traffic, rendering them unreachable by their customers for various lengths of time (Dhameja et al., 2013). Whilst there could be different motives for the attacks, this slow down of internet activity will eventually result in reduced business for those businesses that mainly rely on the internet (Mugari, 2016).

3.2.6. 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 and 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 (Mugari, 2016). In Zimbabwe, 2 leading mobile phone operators, ecocash and telecel, have developed mobile money transfer services namely ecocash and telecash respectively (Mugari, 2016).

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 (Mugari, 2016).

4. DATA

Data was collected between April 2016 and October 2016 from retail businesses within Harare central business district. The study combined both quantitative and qualitative research designs, with questionnaires and in-depth interview guide as the key research instruments. A total of 176 respondents were invited to take part in the study, out of which 156 respondents provided data through questionnaires, whilst in-depth interviews were conducted on the remaining 20 respondents. Respondents were invited to participate using systematic random sampling and purposive sampling techniques. The distribution of the respondents is depicted on Table 1.

Quantitative data was coded and fed into SPSS version 16 software for analysis. Qualitative data was analysed using content analysis and was used to complement quantitative data.

5. RESEARCH FINDINGS AND DISCUSSION

5.1. Payment Systems

Card payment systems, RTGS transfer payments and mobile money transfer payments are some of the cyberspace enhanced payment systems that are available for the retail sector. To this end, respondents were asked to indicate the availability and usage rate of the given payment systems. The statistics are presented on Table 2.

From the above statistics, the debit card facility is the dominant ICT based payment system in the retail sector. A total of 88.5% of the respondents considered the payment method's usage to be moderate (42.3%) or high (46.2%), with a mean statistic of 3.3077 and a standard deviation of 0.78838. Mobile money transfer payment (Ecocash and Telecash) come closely 2nd, with

Table 1: Distribution of respondents

Category of respondents	Number of respondents
Questionnaires (retail shop employees and owners)	156
Interviews: Retail shop employees and owners	7
Customers	10
IT experts	3
Total	176

IT: Information technology

Table 2: Available payment system and extent of their usage (n=156)

Variable description	Not available 1 (%)	Available with low usage 2 (%)	Available with moderate usage 3 (%)	Available with high usage 4 (%)	Mean±SD
Availability and use of debit card facility	3.8	7.7	42.3	46.2	3.3077±0.78838
Availability and use of credit card facility	92.3	7.7	0	0	1.0769±0.27175
Availability and use of ecocash/telecash facilities	0	19.2	57.7	23.1	3.0385±0.66216
Availability and use of RTGS facility	28.0	36.0	24.0	12.0	2.2000±1.0000

SD: Standard deviation; RTGS: Real time gross settlement

a combined moderate to high usage rate of 80.8%. The mean statistic of 3.30385 for mobile money transfer payments indicates moderate usage for the payment platform. There seems to be low usage of RTGS facility as indicated by a mean statistic of 2.2000 and a standard deviation of 1.0000. Credit card facilities are not yet available in the retail sector in Zimbabwe, as denoted by a mean statistic of 1.0769 and an overwhelming 92.3% of the respondents indicating that the facility is not available in their respective businesses.

The above statistics point to the fact that the retail sector in Zimbabwe has embraced ICT based payment systems, with the debit card facility and mobile money transfer payments as the leading payment platforms. Most of the retail outlets have POS terminals to enable debit card payments. Also important to note is the fact that the ecocash mobile money is linked to the ecocash debit card, hence a customer can choose to transact using either the card or the mobile money transfer. This possibly explains the dominance of the debit card payment platform in the retail sector. The findings resonate with the trends in other African countries wherein KPMG (2015) highlights the dominance of card payments and mobile payments in Kenya, Nigeria and South Africa.

However, despite the dominance of the debit card facility, credit cards are not accepted for retail payments in Zimbabwe. All the interviewees also indicated that the credit card platform is not available in their respective businesses. More so, financial institutions in Zimbabwe are not issuing credit cards to customers. This is in sharp contrast with the global trends wherein credit cards are widely used in the United States (FRS, 2013), Australia (APCA, 2015), Kenya, and South Africa (KPMG, 2015). Though not a dominant payment platform, the RTGS facility also provides a good alternative to cash payment. Two shop owners who were interviewed indicated that retail products such as office furniture and appliances are mainly paid for through the use of RTGS facility, as most companies are reluctant to transact in cash.

In concurrence to the questionnaire findings, seven of the ten interviewees from the retail business indicated that most of their loyal customers prefer to use debits cards and mobile phone transfers rather than transacting in cash. This was also supported by 6 out of 10 customers who indicated that they would rather use payment cards and mobile money transfers than to transact in cash. One of the customers had this to say, “I would rather use non cash based payment methods whenever possible than risk losing my hard earned cash to robbers.” Ironically though, non cash based payment systems are also prone to criminal activities. As (Metcalf and Kirst,2013) concur, the adoption of internet and mobile phone based payment systems inevitably expose the retail sector to cyber threats. In the end, it will be a matter of choosing a payment system with fewer risks.

The dominance of cyber-enhanced payment systems in Zimbabwe should be understood in the context of the prevailing economic environment, which of late has been characterised by a biting liquidity crunch. The liquidity crunch has led to cash shortages in the banks, with all banks resorting to limiting the maximum cash withdrawal amounts (Mugari, 2016. p. 184). The cash shortage has also negatively impacted on the retail sector, with businesses that mainly rely on cash transactions being the most affected. Commenting on the liquidity crunch and its impact on the payment systems, respondents had the following sentiments;

“The cash shortage has seriously impacted on our sales. Sales have dropped to alarming levels. We have since shifted our policy on payment methods and we have since embraced non cash payment methods. As you can see, we now have the ecocash facility and we have since increased our POS terminals for card transactions” (Retail sector employee).

“I think it’s high time we have to do away with cash payments and move to plastic money. This is the only viable way of dealing with the cash shortages. Here, most of our transactions are card based and we also accept RTGS payments” (Retail sector employee).

“I spend 5 h in a queue at a bank (name supplied) only to be given $50. I would rather use my card to buy groceries and reserve my cash for other pressing commitments” (Customer).

In light of the above sentiments, it can therefore be argued that the use of non- cash based payment systems is inevitable given the prevailing liquidity crunch. Moreover, the monetary authorities have also taken a leading role in lobbying for the use of plastic money as a way of circumventing the cash crisis. Another issue worth noting is the fact that Zimbabwe does not have its own currency and the Zimbabwean dollar was phased out in the year 2010, following a hyperinflationary period. According to Berger (2008), the inflation rate for the year 2008 had reached an unprecedented level of 231 million percent. The nation adopted a multi-currency regime, with the United States Dollar as the major trading currency, among other currencies such as the South African Rand, Botswana Pula, British Pound and the Chinese Yuan. Absence of the local currency and lack of control over the United States Dollar supply are some of the reasons for cash shortages in Zimbabwe. This scenario could also be an impetus for the adoption of non-cash based payment systems in Zimbabwe.

5.2. Types of Cyber Threats

Respondents were asked to indicate the prevalence rate of specified cybercrimes in their organisations. Their responses were coded as follows: (1) Doesn't occur, (2) rarely occurs, (3) common, (4) very common. Table 3 shows the responses, as well as the means and standard deviation.

As depicted by Table 3, infection of computers with viruses seems to be the dominant cyber threat in the retail sector, with an overwhelming 88.5% considering it to be either common (65.4%) or very common (23.1%). Moreover, the mean of 3.0769 and a standard deviation of 0.68836, indicate that the threat is common. Almost a third of the respondents (34.6%) indicated that unauthorised access is common, and this threat had a mean of 2.0769, pointing to the fact that this threat rarely affects the retail sector. Malicious software attacks, as represented by mean of 1.800, are a rare phenomenon, with 40% apiece considering the threat as not occurring or rarely occurring in their businesses. Majority of the respondents were of the opinion that debit card fraud is either rare (30.8%) or doesn't occur at all (65.4%). A mean of 1.3846 indicates that debit card fraud is a very rare phenomenon in the retail sector. Majority of the respondents (72%) also 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, a clear indication that credit cards are not in use in Zimbabwe.

The high prevalence of infection of computers with computer viruses is mainly attributed to the ease with which the threat can affect computer systems. A computer technology expert noted that most of the computer viruses emanate from the internet, while other viruses are transferred through use of removable storage devices. Regarding the latter, another information and computer technology expert jokingly remarked that almost every employee has at 1point been a culprit for this kind of threat. He further pointed out that most of the incidents involving infection of computer systems with computer viruses through removable storage devices are unintentional, though impacts can be disastrous. Laxity of access controls was also noted as a contributory factor to the rise in the threat of computer viruses.

Stressing on the impacts of computer viruses on the business in general and electronic payment systems in particular, a computer technology expert had this to say;

"Nowadays important business information and customer data is stored in centralised databases. Some of the computer viruses can compromise confidential information within the databases, and in the worst case scenario, personal customer data can be lost. In the end, it would be risky for the businesses to transact using electronic payment systems."

Given the serious effects that viruses can have on important businesses, it becomes imperative for businesses to put in place sound security measures to protect important business data. In light of the view that most of the viruses emanate from the internet, installation of firewalls and up-to- date anti-virus software were viewed by the ICT experts to be amongst the effective ways of dealing with internet related viruses.

Two of the retail shop supervisors who were interviewed admitted that their systems had once been hacked and customer data was compromised, though they were reluctant to provide finer details on the incidents. Closely linked to computer viruses are malicious software and DOS attacks. Whilst malicious software attacks and denial of service attacks were not considered to be dominant by the respondents, both threats can emanate from 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 could possibly be due to DOS attacks.

Despite the near moderate usage of debit cards as a form of payment in the retail sector, the findings suggest that debit card fraud is a rare occurrence in the sector. This could possibly be due to the security features of a debit card payment system as opposed to a credit card payment system. Card related fraud, as (Metcalf and Kirst,2013) is mainly pronounced with credit cards than debit cards. The security issue for debit cards is further supported by the finding from all the interviewee retail operators that they only accept card- present transactions, hence minimising the prevalence rate of debit card fraud. On the other hand, card-not-present transactions, which are found in most developed world, are susceptible to fraudulent activities. The low usage rate of the RTGS system can possibly explain why fraudulent RTGS payments are a rare phenomenon. One interviewee who deals with electrical goods however highlighted a single incident in which he lost goods through a fraudulent RTGS pay.

5.3. Retail Sector's Ability to Deal with Cybercrime

Majority of the respondents (57.8%) were inclined to disagree with the fact that their organisations are able to deal with cyber threats (Table 4). Moreover, only 23% of the respondents were inclined to agree to the fact that their organisations had the

Table 3: Types of cybercrime and their prevalence (n=156)

Variable description	Doesn't occur 1 (%)	Rarely occurs 2 (%)	Common 3 (%)	Very common 4 (%)	Mean±SD
Unauthorised access	26.9	38.5	34.6	0	2.0769±0.79614
Infection of computers with viruses	3.8	7.7	65.4	23.1	3.0769±0.68836
Malicious software attack	40.0	40.0	20.0	0	1.800±0.76376
Debit card fraud	65.4	30.8	3.8	0	1.3846±0.57110
Credit card fraud	100	0	0	0	1.0000±0.0000
Fraudulent RTGS transaction	72.0	28.0	0	0	1.2800±0.45826
Denial of service attack	54.2	41.7	4.2	0	1.5000±0.58977

SD: Standard deviation, RTGS: Real time gross settlement

Table 4: Response on whether respondent's organization is able to deal with cyber threats

Response	Frequency (%)
Strongly disagree	24 (15.5)
Disagree	66 (42.3)
Neutral	30 (19.2)
Agree	30 (19.2)
Strongly agree	6 (3.8)
Total	156 (100.0)

ability to deal with cyber threats, whilst another 19.2% was undecided.

Given the availability of cyber threats, majority of the respondents' view that they are not able to deal with these cyber threats seems to compound the vulnerability of the retail sector. Whilst most retail outlets have improved their cyber security through strict access controls, use of antivirus software and installation of firewalls, most interviewees admitted that their systems are still vulnerable. Another retail operator raised an important point when she remarked that;

"With the global reach of the internet, you wouldn't know where and when the next attack will come from but that's the risk that you have to accept when you accept non cash based payment systems. So it's either you take the risk (of accepting non cash based payment systems) and prosper or you do away with the risk and perish."

Such opinion makes sense in the current Zimbabwean business environment, which is characterised by liquidity crunch. Monetary authorities are encouraging use of plastic money as an alternative to cash based payment systems.

Though some retail outlets may claim to be safe from cyber threats as of now, it can be argued that perpetual safety cannot be guaranteed. This is supported by an IT expert who argued, "Any business that uses computer applications and the internet is and will always be prone to cyber attacks. You may claim to be safe now, but as new e-business applications are inevitably developed, new threats will always emerge". Similarly, e-payment platforms are continuously changing as businesses embrace innovative ways of transacting. Such changes often bring new threats, which may not be prevented by the prevailing security systems. This therefore calls for the need for the retail sector cyber security systems to keep up with the pace of technological advancement in both business operations and payment systems.

The retail sector's preparedness to deal with cyber threats should also be interrogated in light of the Zimbabwean legal framework. Cybercrime is dealt with under Chapter VIII of the Zimbabwean Criminal Law (Codification and reform) Act [Chapter 9: 23]. Specifically, the following sections deal with cybercrime:

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

Whilst the legislative authorities should be applauded for at least recognising the threat of cybercrime, most of the interviewees were of the opinion that the laws are inadequate. One IT expert had this to say;

"Given the global trends towards use of the internet and cyberspace based payment systems, one would expect a nation to have a comprehensive piece of legislation on cybercrime, rather than to just have 2 pages on cybercrime, as is the case with our criminal law code."

It is also important to highlight that the current criminal law code was promulgated in 2004, when the nation had not yet widely embraced ICT. Moreover, during the processes which led to the adoption and the subsequent promulgation of the criminal law code, electronic payment systems had not yet been widely embraced in Zimbabwe. To this end, it can be argued that the current provisions within the criminal law code fall short in addressing the current threats posed by the ever changing ICT discourse. In what seems to be an admission that laws to deal with cyber crime are inadequate, the legislative authority in Zimbabwe is currently working on the cybercrime bill which if passed into law will address some of the inadequacies of the criminal law code.

Another possible pitfall of the criminal law code in addressing emerging cyber threats is that it is too general and does not specifically address the threats within the retail sector ICT based payment systems. Whilst it may be difficult to craft laws that specifically address retail sector cyber threats, a policy framework on retail payment systems would be another viable option.

Other interviewees bemoaned lack of requisite investigative skills on the part of law enforcement agents, and these sentiments were echoed by those who had at 1point reported a cybercrime to the police. Indeed a comprehensive piece of legislation can be promulgated to deal with cybercrime, but it can fall short on implementation, especially where the law enforcement officials are incapacitated. There is therefore need for continuous training of police officers for them to keep up with the pace of change in the technological environment.

6. CONCLUSION

As expected and in line with the global trends, Zimbabwean retail sector has greatly embraced cyberspace enhanced payment systems, with use of debit card and mobile money transfer systems topping the list of non-cash based payment systems. Though at a lower rate, RTGS transactions are also being used by retailers, especially those dealing in office furniture and electrical appliances. The biting liquidity crunch and lobbying by the monetary authorities have been the major push factors for the adoption of cyberspace based payment systems. However, despite some benefits, ICT based payment systems are prone to threats. Chief among the threats are infection of computers with viruses and unauthorized access, whilst there have also been reported incidents of debit card fraud and fraudulent RTGS payments. The presence of these threats, coupled with the perceived inability to effectively deal with the threats compounds the vulnerability of cyber-enhanced payment systems in the Zimbabwean retail sector. Despite the current measures to deal with cybercrime in the retail sector, the measures seem to be inadequate.

Based on the findings of this study, it can be concluded that cybercrime will remain the major threat to cyberspace enhanced payment systems in the Zimbabwean retail sector and the threat will be compounded by the swift pace at which technology is advancing. There is therefore an urgent need for the relevant policy makers and retail sector players to come up with comprehensive measures to deal with cyber threats.

REFERENCES

Aseef, N., Davis, P., Mittal, M., Sedky, K., Tolba, T. (2005), Cyber-Criminal Activity and Analysis. White Paper, Fall. Available from: https://www.courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/team2-whitepaper.pdf. [Last accessed on 2015 Sep 30].

Australian Payments Clearing Association (APCA). (2015), Australian Payments Fraud. Available from: http://www.apca.com.au/docs/fraud/Australian-payment-fraud-details-and-data-2015.pdf. [Last accessed on 2016 Aug 25].

Berger, S. (2008), Zimbabwe Inflation Hits 231 Million Percent. UK: Telegraph.

Broadhurst, R. (2006), Developments in the global law enforcement of cyber-crime policing. An International Journal of Police Strategies and Management, 29(2), 408-433.

Budhram, T. (2012), Lost, stolen or skimmed: Overcoming credit card fraud in South Africa. SA Crime Quarterly, 40, 31-37.

Chavan, P., Aggawal, R, Bajaj, K., Agrawal, N. (2011), Cybercrime: A Financial Sector View. India: KPMG Publishers.

Davis, R.W.K., Hutchson, S.C. (1997), Computer Crime in Canada. Toronto: Carswell.

Dhameja, S., Jacob, K., Porter, R.D. (2013), Clarifying Liability for Twenty-First-Century Payment Fraud. Federal Reserve Bank of Chicago. Economic Perspectives No. 3Q/2013.

Easttom, C., Taylor, J. (2011), Computer Crime, Investigation, and the Law. Boston: Cengage Learning.

Federal Reserve System. (2013), Federal Reserve Payments Study. Available from: https://www.frbservices.org/files/communication/pdf/research/2013_payments_study_summary.pdf. [Last accessed on 2016 Aug 25].

Gaikwad, P., Motwani, D., Shinde, V. (2015), Survey on malware detection techniques. International Journal of Modern Trends in Engineering and Research, 21(7): 1-25.

Hataiseree, R. (2008), The Development of e-Payment and Challenges in Thailand. Available from: http://www.seacen.org/au1/pdf/publication/research_prj/2008/rp71/Chapter10.pdf. [Last accessed on 2015 Oct 07].

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

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

Kathirvel, K. (2013), Credit card frauds and measures to detect and prevent them. International Journal of Marketing, Financial Services and Management Research, 2(3), 172-179.

KPMG. (2015), Payments Developments in Africa. Vol. 1.South Africa: KPMG.

Kunyaru, P.M., Kyalo, J.K. (2015), Factors affecting online transactions on the developing countries: A case of E-commerce business in the Nairobi county, Kenya. Journal of Educational Policy and Entrepreneurial Research (JEPER), 2(3), 1-17.

Lawrence, J and Tar, U. (2010), Barriers to ecommerce in developing countries. Information, Society and Justice, 3, 23-35.

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 and Cyber Security, 1, 1-20.

Metcalf, R., Kirst, K., editors. (2013), Cyber Security and the Retail Consumer Sector. Retail and Consumer Insights 2/2013. Available from: http://www.newsletter.pwc.in/inxmail9/images/R&Cinsights/IssuesApril2013/PwC,R&CInsights1,2013,corr.pdf. [Last accessed on 2015 Oct 25].

Mugari, I. (2016), Perspectives on cyber-threats to the retail sector. A case study of East gate shopping mall. International Journal of Innovative Research and Development, 5(3), 180-187.

Mugari, I., *et al*. (2016), Cybercrime-the emerging threat to the financial services sector in Zimbabwe. Mediterranean Journal of Social Sciences, 7(3), 135-143.

Raja, J., Velmurgan, M., Seethyaraman, A. (2008), Epayment: Problems and prospects. JIBC, 13(1), 1-17.

Roderic, G. (2006), Cyber-Crime: The Challenge in Asia. USA: University of Washington Press.

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).

Thomas, D., Loader, B., editors. (2000), Cybercrime: Law enforcement, Security and Surveillance in the Information Age. UK: Cambridge University Press.

Uppal, D., Mehra, V., Verma, V. (2014), Base survey on malware analysis, tools and techniques. International Journal on Computational Sciences and Applications, 4(1), 103-112.

Wagenaar, J. (2014), Collaborative Cyber Security in the Retail Sector. Masters Thesis. Netherlands: University of Twente.

Wright, T. (2015), Retailers Need to Tackle Inevitable Cyber Threats. New York: Pillsbury.

Yar, M. (2005). The Novelty of Cybercrime: An Assessment in light of Routine Activity Theory. European Journal of Criminology, 2(4), 407-427.