ELECTRONIC FRAUD (CYBER FRAUD) RISK IN THE BANKING INDUSTRY, ZIMBABWE

Shewangu Dzomira*

Abstract

The paper explores forms of electronic fraud which are being perpetrated in the banking industry and the challenges being faced in an attempt to combat the risk. The paper is based on a descriptive study which studied the cyber fraud phenomenon using content analysis. To obtain the data questionnaires and interviews were administered to the selected informants from 22 banks. Convenience and judgemental sampling techniques were used. It was found out that most of the cited types of electronic fraud are perpetrated across the banking industry. Challenges like lack of resources (detection tools and technologies), inadequate cyber-crime laws and lack of knowledge through education and awareness were noted. It is recommended that the issue of cyber security should be addressed involving all the stakeholders so that technological systems are safeguarded from cyber-attacks.

Keywords: Electronic Fraud, Cyber Fraud, Cyber-Crime, Internet Banking, Electronic Banking

* *Post-Doctoral Research Fellow, CEMS, Department of Finance, Risk Management & Banking, UNISA*
Email: Dzomis@unisa.ac.za or shewangu@yahoo.com

1. Introduction

In modern times banks are not so often robbed because money is not only kept in bank vaults. In modern computer technologies and data networks a lot of money exists in cyber space. Banks have to adapt to modern trends of doing business electronically and at the same time protect themselves against cyber-crimes. The first recorded "cyber-crime" took place in the year 1820! That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 BC in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage (Khan, 2011). In Zimbabwe almost all banks to date have implemented electronic banking and/or cyber banking in one way or the other.

According to Dube et al. (2009), the first visible form of electronic innovation in Zimbabwe was in the early 1990s when Standard Chartered Bank and the Central African Building Society (CABS) installed automated teller machines (ATMs). (Kass, 1994 cited by Goi, 2005). Electronic banking in Zimbabwe has grown significantly in recent years. According to Gono (2012), fifteen banking institutions have already introduced mobile banking products in partnership with mobile operators and the number of banking institutions venturing into mobile banking are on the increase. The, volume of mobile payment transactions and the volumes of internet transactions also increased substantially. However, according to Kadleck (2005), as more businesses and customers launch their money into cyberspace, opportunities for 21st century tech-savvy thieves also increase.

While on the one hand, financial institutions in Zimbabwe are coping with global developments in technology, on the other hand cyber fraud perpetrators are on the look-out. E-banking fraud is an issue being experienced globally and is continuing to prove costly to both banks and customers (Usman et al., 2013). According to Shinder (2002), e-commerce, on-line banking and related technologies have resulted in millions of dollars of financial transactions taking place across network connections and as banks expand their array of online services to clients, the risk of internet computer fraud (ICF) increases and the risk landscape changes. Financially motivated high-profile attacks have been observed across the globe with the growing patronage of e-banking services and its anticipated dominance in the near future. Some of the known factors that contribute to the acute problem of security must be addressed (Usman et al., 2013).

According to Mushowe (2009), the Zimbabwean government had plans to come up with legislation to curb cyber-crime in the country in view of its increasing threat to world economies. Given the threats posed to global economies by cyber-crime, there was a need to come up with measures to combat this crime. In addition to that, Kabanda (2012) posits that incidences of cyber-crime in Zimbabwe were on the increase and need to be quantified through research. The prevalence of cyber-criminals is a

worrying development as Zimbabwe grows more reliant on ICTs. More so, Moyo (2012) adds that, people cannot redefine fraud because it has been committed through cyberspace and further mentions that due to the fact that most victims of cybercrime are high-profile bank customers, they were reluctant to announce or admit in public that they have been successfully defrauded by some cyber-criminal.

The Zimbabwean criminal codification act does not, at any point mention computer aided crimes or cyber criminology directly as a crime but this does not mean that cyber criminology is exempted. While there is so much online activity masked in anonymity and plasticity, tracing online criminals can be impossible or arduous, Muleya (2012)).

Although research have been carried out on adoption and use of internet banking, and security strategies in terms of online banking in Zimbabwe, the author found no research that specifically addressed the cyber fraud and the challenges faced by banking institutions in trying to combat this kind of risk.

In view of the above background, the paper intends to attain the following objectives:

- to examine electronic frauds perpetrated in the banking sector in Zimbabwe; and
- to explore the challenges faced by banks in an endeavour to combat cases of electronic fraud in Zimbabwe.

The following sections of this article outline the literature review, methodology, analysis of the findings, conclusions and recommendations.

2. Literature Review

Electronic fraud (cyber fraud)

At global level ICT advancement has immensely contributed to economic development including finance and banking. The internet is one of the fastest-growing areas of technical infrastructure development. Today information and communication technologies (ICTs) are omnipresent and the trend towards digitization is growing (Gercke, 2012). Due to the pivotal roles of banks in the growth and economic development of any nation, it has become very necessary to protect these institutions from the antics of fraudsters (Ikechi & Okay, 2013). However, it is the same ICT systems used by the banks which are negatively utilized by perpetrators of fraud. The increased use of ICT such as computers, mobile phones, internet and other associated technologies are the routes which gave rise to lot of constructive work as well as destructive work. The destructive activities are considered as 'electronic crime' which includes spamming, credit card fraud, ATM frauds, money laundering, phishing, identity theft, denial of service and other host contributing crime (Siddique & Rehman, 2011; Bamrara, Singh & Bhatt, 2013). While straight-through-transaction processing has afforded new levels of efficiency for financial institutions and greater convenience for consumers, it also creates new opportunities for fraud, as transactions are faster, do not require any human intervention, and are often "anonymous" (Oracle, 2012). Due to the pivotal roles of banks in the growth and economic development of any nation, it has become very necessary to protect these institutions from the antics of fraudsters (Ikechi & Okay, 2013).

According to the World Economic Forum's Global Risks (2014), cyberspace has proved resilient to attacks, but the underlying dynamic of the online world has always been that it is easier to attack than to defend. On that note, the contemporary approach at all levels on how to preserve, protect and govern the common good of a trusted cyberspace must be developed, since the growth of the information society is accompanied by new and serious threats. The rising of such threats at various stages is because of the explosion of online banking coupled with the acceptance by consumers to disclose sensitive information over internet. Electronic fraud is committed in different ways.

Types of e-frauds

Electronic fraud could be classified into two categories namely, direct and indirect frauds. Direct fraud would include credit/debit card fraud, employee embezzlement, and money laundering and salami attack. Indirect fraud would include phishing, pharming, hacking, virus, spam, advance fee and malware.

Credit card/debit card fraud and identity theft are two forms of e-fraud which are normally used interchangeably. It involves impersonation and theft of identity (name, social insurance number (SIN), credit card number or other identifying information) to carry out fraudulent activities. It is the unlawful use of a credit/debit card to falsely obtain money or belongings without the awareness of the credit/debit card owner. (Williams, 2007; Njanike, Dube & Mashanyanye, 2009; Saleh, 2013). Theft of someone's identity can be done through different ways. According to Barker, D'Amato & Sheridon (2008), skimming involves stealing information off a credit card during a legitimate transaction. This type of scheme usually occurs in a business where the patron's credit card is taken out of sight while the transaction is being processed. The fraudster will swipe the card through an electronic device known as a "wedge" or skimming device, which records all information contained on the magnetic strip (ACFE, 2007, p.1.104) cited by Barker et al. (2008). To obtain credit card details, offenders may employ sophisticated method such as hacking into merchants' databases or simply "engineering" the victims into giving their credit card details (Prabovo, 2011). However, Williams (2007) argued that whilst businesses and banks suffer losses from credit card

fraud which continue to increase exponentially, there is not sufficient legislation to enable the eradication of this crime entirely.

In an attempt to maximize the benefits from technology utilization most people end up being victims of technology. Cyber fraudsters design web pages to look like legitimate sites where victims enter personal information such as usernames, passwords and credit card details. Often emails are sent to recipients asking disclosure and/or verification of sensitive information, and upon disclosure of such information the offenders make online transfers (Barker et al., 2008; Gercke, 2008). "Smishing" and "vishing" are forms of phishing which are more sophisticated and uses phone text messages and phone calls to bait victims (Tendelkur, 2013; KPMG, 2012). This kind of fraud can also be used to target corporates and other merchants. E-commerce merchant sites have been a target as they normally contain valuable loyalty points or stored payment card information that can be used for fraudulent purchases and also a kind of mass-marketing fraud (McGuire & Dowling, 2013; 41STParameter, 2013)

Traditionally, fraud perpetrators targeting bank institutions used "pen and paper" to commit internal fraud. However, upon computerization of the transactions the same perpetrators shifted to computer fraud committing the same type of fraud. According to Shinder (2002), embezzlement, which involves misappropriating money or property for own use that has been entrusted to an employee (for example, an employee uses legitimate access to the company's computerized payroll system to change the data, or moves funds out of the company's bank accounts into a personal account). Moreover, a financial institution can allow trusted employees to access personal customer data that can be used to gain online access to customer accounts. In this way an employee can easily commit fraud (BITS, 2003).

In some cases fraudsters run a program known as the "salami technique" as an approach to steal money in small increments. The program makes micro-changes over an extended period, so that the changes are not easily noticeable. An example of this type of fraud is a program that deducts a few dollars per month from the accounts of many clients (Tendelkur, 2013; Marshall, 1995).

Fraudsters also run malicious codes and malware programs which take control of individual's computer to spread a bug. A computer virus is a program that causes an unwanted and often destructive result when it is run. A worm is a virus that replicates itself. A Trojan (or Trojan horse) is an apparently harmless or legitimate program inside which malicious code is hidden; it is a way to get a virus or worm into the network or computer (Shinder, 2002; 41STParameter, 2013; KPMG, 2012).

In the recent global recession period money laundering and/or cyber laundering has been a common unethical practice. It is a form of fraud that involves the electronic transfer of funds to launder illegally obtained money. The competence to transfer limitless amounts of money without having to go through strict checks makes cyber money laundering an attractive proposition. (Shinder, 2002; Ikechi & Okay, 2013; Siddique & Rehman, 2011). New technologies and cyberspace offer money launderers new opportunities and present new challenges to law enforcement and difficulties in the investigations of internet-based-money laundering techniques (SiongThye, 2002; Gercke, 2011).

Another type of fraud involves spamming where unsolicited emails or junk newsgroup postings are sent without the consent of the receiver and frequently being malicious and sometimes offenders pretend to be financial institutions or companies (Schjoberg, 2008; KPMG, 2012; Geeta, 2011). In light of that, according to Gercke, (2011), some experts suggest the only real solution in the fight against spam is to raise transmission costs for senders.

In certain instances victims are redirected from legitimate websites to fraudulent or phony websites which look very identical to real ones; however any personal information entered into the forms (passwords and credit card number) would be sent to the cyber-criminal (Tendelkur, 2013; 41STParameter, 2013; McGuire & Dowling, 2013).

More so, hacking/cracking is one of the oldest computer related crimes which refers to unlawful access to a computer system and include breaking the password of password-protected websites and circumventing password protection. These spy hackers are usually sophisticated and use trail covering techniques like relay computers to make it seem like the attack originates locally and makes it harder to trace them. Hackers gain unauthorized access to large amounts of confidential data with the aim to cause monetary and reputational damages to the targeted entity (Gercke, 2011; Aseef et al., 2005; EMC, 2013),

In advance fee fraud, offenders send out scam emails asking for recipients' help in transferring large amounts of money to third parties and promise them a percentage, if they agree to process the transfer using their personal accounts. The dynamics of advance fee fraud is to trick prospective victims into parting with funds by persuading them that they will receive a substantial benefit, in return for providing some modest payment in advance (Gercke, 2011). In essence, advance fee fraud encompasses mass marketing frauds and consumer scams, including advance fee scams such as 419 frauds, inheritance frauds, fake charity or disaster relief frauds, fake lotteries and pyramid schemes (Chang, 2008; McGuire & Dowling, 2013).

These e-fraud types have caused serious threat to the banking industry especially in most emerging economies including Zimbabwe and there is a need to address these issues.

General challenges in combating e-fraud/cyber fraud

The challenges faced by banks mainly include technical disadvantages, lack of knowledge and awareness, and lack of legislation.

In emerging and developing economies the issue of fighting electronic fraud is a major problem owing to a number of reasons. Mostly, advances in technology are fast-paced, as are fraudsters, however organisations are often far behind and the easy availability of new technologies with high operational speeds, capacity and connectivity make unlawful activities easier to escape detection. Cyber users in Africa do not have up-to-date technical security measures like anti-virus packages, and many of the operating systems used are not regularly patched (Kritznger & Solms, 2012; Harry, 2002; PWC, 2011). Generally there is lack of resources to investigate cyber-crime and beef up required instruments to combat electronic fraud.

In the wake of ever increasing ICT advances banking stakeholders need to engage cyber fraud awareness and education. The lack of awareness among the general public of how to maintain a minimum level of security with regard to personal information or electronic property, and it is vital not only to educate the people involved in the fight against cybercrime, but also draft adequate and effective legislation (Harry, 2002; Gercke, 2011; Mwaita & Owor, 2013). This is a very risky situation and means therefore that there is a clear, but certainly not deliberate lack of cyber security awareness and education to make cyber users aware of all possible cyber threats and risks (Kritzinger & Solms, 2012).

Most law enforcement agencies lack the technical expertise as well as sufficient regulatory powers and automated equipment to investigate complicated evidence collection because of intangible nature of cyber space and prosecute fraudulent digital transactions (Harry, 2002; Gercke, 2011; Mwaita & Owor, 2013). Therefore lack of cyber space legal legislation provides a safe haven for cyber criminals.

In light of trying to protect corporate reputation, investor and public confidence most businesses are reluctant to report cyber-criminal activity (Harry, 2002).

3. Methodology

The research on which this paper reports pertains to electronic fraud (cyber-fraud) perpetrated within the banking sector in Zimbabwe. The study was based on descriptive research. Descriptive study is a study that sets out to describe a phenomenon or event as it exists, without manipulation or control of any elements involved in the phenomenon or event under study (Page & Meyer, 2000). The descriptive study is popular in research because of its versatility across management disciplines (Cooper & Schindler, 2011). The main purpose of descriptive research is to describe the status-quo of affairs as it exists. In descriptive research the problem is structured and well understood (Ghauri & Gronhaug, 2005). In this study electronic fraud types and challenges faced by the banking sector in an attempt to combat the risk, forms the phenomenon. The primary data was collected on the basis of self-completion questionnaires and interviews administered to various respondents from different banks. According to Bryman & Bell (2003), self-completion questionnaire, respondents answer questions by completing the questionnaire themselves.

4. Sampling

In this research the non-probability sampling technique has been applied. Purposive and convenience sampling techniques were used. Purposive sampling involves choosing people whose views are relevant to an issue because one makes judgment, and/or persuaded by collaborators, that their views are particularly worth obtaining and typify important varieties of viewpoint (Jankowicz, 2005). In a convenience sample, often termed an accidental sample, units that we find convenient for some reason are selected (Ghauri & Gronhaug, 2005). In this study both purposive and convenience sampling were applied and the researcher targeted all 22 banks, from where the participant sample was selected. Tables 1 and 2 below show architecture of Zimbabwe`s banking sector and the sample structure of CEOs, auditors, risk managers and BAZ members respectively.

Table 1. Architecture of Zimbabwe`s Banking Sector as of December 2012

Type of Institution	Number
Commercial Banks	16
Building Societies	3
Merchant Banks	2
Savings Banks	1
Total Banking Institutions	22

Source: RBZ Monetary Policy Statement issued on the 31st of January 2013 by G. Gono

Table 2. The sample structure of CEOs, Auditors, Risk Managers and BAZ members

Description for CEO	Number	Percentage %
Distributed questionnaires for CEOs	22	100
Total Response of CEOs	15	68
Uncompleted questionnaires returned	4	18
Usable questionnaires	11	50
Description for Auditors	Number	Percentage %
Distributed questionnaires for Auditors	66	100
Total Response of Auditors	36	55
Uncompleted questionnaires returned	6	9
Usable questionnaires	28	42
Description for Risk Managers	Number	Percentage %
Distributed questionnaires for Risk Managers	22	100
Total Response of Risk Managers	18	82
Uncompleted questionnaires returned	2	9
Usable questionnaires	15	68
Description for BAZ members	Number	Percentage %
Distributed questionnaires for BAZ members	5	100
Total Response of BAZ members	4	80
Uncompleted questionnaires returned	1	20
Usable questionnaires	3	60

Universe

All the bank institutions which were studied have their head offices situated in one geographical area, Harare and therefore it was convenient to the researcher in contacting the survey. The targeted respondents (CEOs, Risk Managers, Auditors, Bankers' Association of Zimbabwe (BAZ) members) of these banks were as well stationed at head offices and were selected on the basis of what they know about e-fraud.

Tools for analysis

In this study a qualitative analysis was done using content analysis of data. Content analysis involves analyzing text with respect to its content, with the factors of interest most often relating to meaning, or how many times (frequency with which) particular phrases/terms appear (Page and Meyer, 2000). Its breadth makes it a flexible and wide ranging tool that may be used as a stand-alone methodology or as a problem-specific technique (Cooper and Schindler, 2011). Once the data has been analyzed and the units categorized and measured, the researcher can then seek to identify themes and relationships between the observed frequency, for example, of the units (Crowther and Lancaster, 2009). Graphical displays and observed frequencies were used in this study. As with descriptive statistics, the appropriate graphical analysis depends upon the measurement scale for the variable that is being analyzed (Page and Meyer, 2000).

Findings

All the 28 respondents at least had passed Ordinary level and joined their respective institutions having acquired that qualification. A number of them (86%) had passed their Advanced Levels. Few of the respondents (43%) had bank related qualifications, such as Institute of Bankers Certificate or Diploma (IOBZ), while none had professional digital forensic qualification. Out of the total respondents, 82% indicated that they had undergone an orientation course in digital forensic auditing. It was discovered that 86% of the total respondents were ex-police officers, particularly from the Serious Fraud Unit of the Criminal Investigations Department.

Table 3. Profile of Responding Auditors

Academic and Professional Qualification	Frequency (n)	%
Ordinary Levels	28	100
Advanced Levels	24	86
Professional Digital Forensic Qualification	0	0
Other Banking Qualifications	12	43
Auditing Related Qualification	10	36
Orientation Courses	23	82
Other Background Experience e.g. police	24	86

Frequency

Figure 1 and table 4 shows the response rate for the questionnaires. The questionnaires were distributed to 22 CEOs; Auditors; 22 Risk Managers and 5 BAZ board members with 57 being returned and considered usable for analysis. Of these, 19% (11 respondents) were from CEOs; 49% (28 respondents) were from Auditors; 26% (15 respondents) were from Risk Managers and 5% (3 respondents) were from BAZ members.

Figure 1. The Response rate

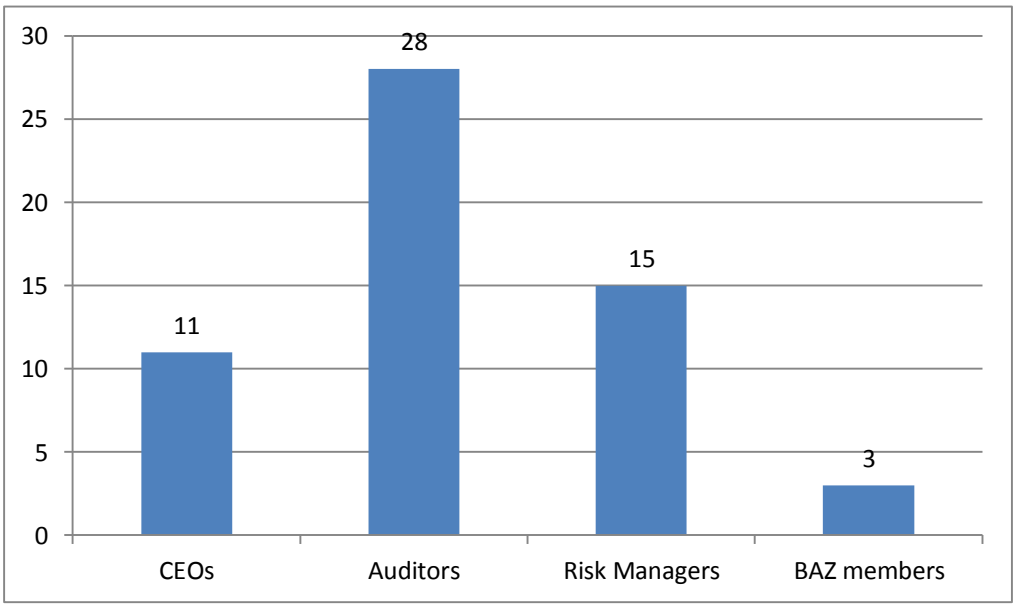


Table 4. Types of fraud experienced and prepared to be prevented

Fraud scheme	Response (%)
Accounting fraud (internal financial fraud including payroll, vendor, procurement, skimming)	76%
Money transfer (electronic funds transfer/wire transfer)	70%
Identity theft (credit/debit card fraud)	68%
Other	67%
Mobile banking	67%
Money laundering	55%
Hacking/cracking	45%
Phishing	43%
Pharming	34%
Spy software	27%
Computer virus (worms, Trojans)	17%
Scams	12%
Wire tapping	10%

Table 4 shows the response rate on each and every fraud type committed in the banking sector. From the ranking, accounting fraud is at the top with 76% indicating that the traditional ways of committing fraud are still being used but of late electronically (internal computer fraud). Followed by money transfer (70%), identity theft (68%), other (67%), mobile banking (67%) and money laundering (55%) forming the top six categories. A total of 67% of the respondents indicated that there are some other fraud types such as asset misappropriation, financial statement fraud, bribery and corruption Also being perpetrated are hacking/cracking with 45%, Phishing (43%), Pharming (34%), spy software (27%), computer virus (17%), scams (12%) and lastly wire taping with 10%.

Singh, et al (2013) in India Risk Survey found out top six fraud categories at global level as physical theft of assets with 25%, followed by information theft (23%), management conflict of interest (21%), vendor procurement (20%) internal financial fraud (19%), and corruption and bribery (19%). However, Kroll (2011/12) in Economist Intelligence Unit Global Fraud Survey found out and ranked fraud types as follows, information theft (50%), theft of physical assets (46%), vendor, supplier or procurement fraud (42%), IP theft (40%), internal financial fraud (38%) and money laundering (25%).

This was based on the proportion of companies describing themselves as highly or moderately vulnerable to such frauds.

Whereas Singleton, (2013) found out top five cyber-crimes (cyber fraud) ranked as follows, tax refund fraud (electronically perpetrated through phishing, personal information theft in filing the returns) at the top followed by corporate account takeover (electronic funds transfer). The third one is identity theft (credit/debit card fraud) followed by theft of sensitive data (cracking/hacking) and lastly theft of intellectual property.

In contrast to literature findings the fraud incidences in Zimbabwe are only different in terms of incurrence ranking but the nature and type of cyber frauds are almost the same.

Fraud incurrence and banks' preparedness in fighting the fraud menace

About 67% of the respondents cited "lack of oversight by line managers or senior managers on deviations from existing electronic process/controls" as one of the major cause followed by "current business pressure to meet set targets" and "difficult business scenario" as other causes for rising fraud cases. About 40% of the respondents revealed that there was collusion between employees and external parties.

The current perception of fraud and fraud incidents encountered by the banks

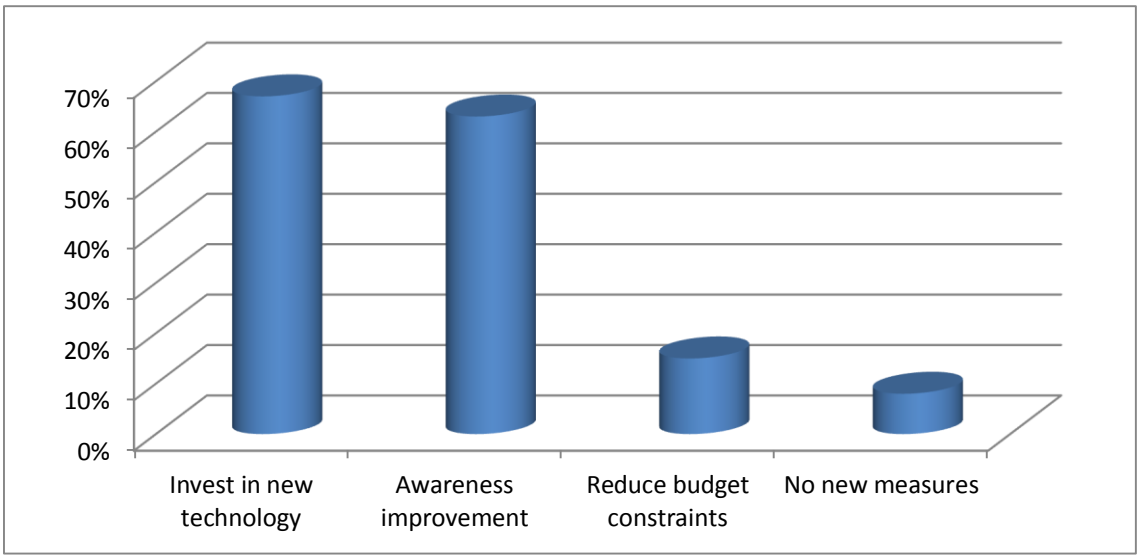
The retail banking sector has encountered the maximum number of fraud incidents followed by the corporate banking division. A number of the respondents who are involved in priority banking sector have also faced significant fraud cases number in this area. Cases of fraud in personal banking are attributed to "identity theft" and "misuse of power of attorney/account takeover".

Table 5. Challenges with regard to prevention

Challenges	Response (%)
Budget constraints and personnel and lack of resources	53%
Lack of fraud detection tools and technologies	49%
Lack of awareness and education	35%
Challenge in law enforcement, legislation and crime investigation	24%

Table 5 shows a total of 53% of the respondents indicated that they lack sufficient resources, 49% showed that there is lack of fraud detection tools and technologies whilst 35% of the total respondents indicated that a fragmented fraud prevention approach is a challenge and 24% of the respondents indicated that difficulty investigating crimes across borders is a challenge.

Figure 2. Reduction of fraud vulnerability



From Figure 2, a total of 67% of the respondents indicated that there is a need for investment in new technology. 63% said that there is a need for awareness improvement, 15% of the total respondents revealed that increase in budget/staff should be considered and 8% of the respondents indicated that no new measures are required.

Figure 3. Adjustment of resources dedicated to fraud prevention

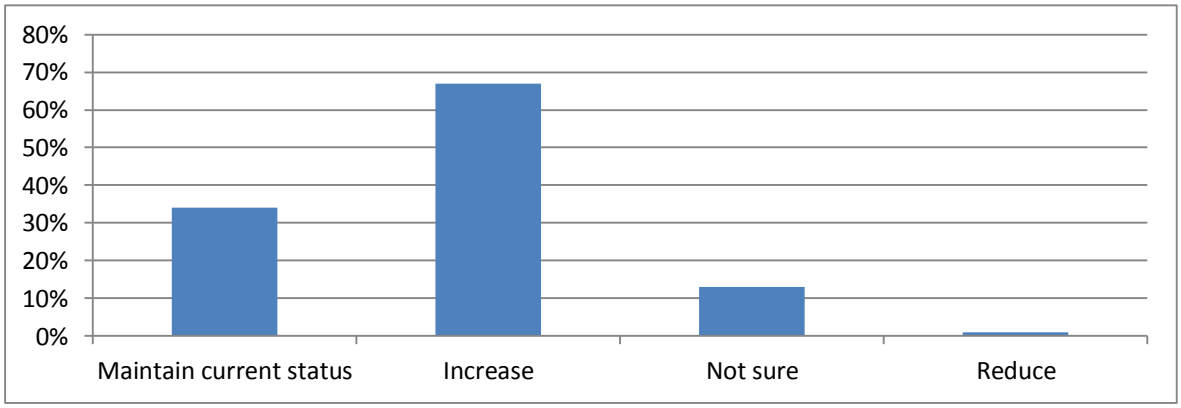


Figure 3 shows that of the total respondents, 34% indicated that there should be no change. 67% of the respondents showed that the resources should be increased for fraud prevention whilst 13% showed that there were unsure and only 1% indicated that they should be reduced.

Kritzinger & Solms (2012) found out that a number of cyber factors led Africa to becoming a cybercrime hub and identified the following challenges; lack of cyber security awareness, ineffective legislation and policies, and lack of technical cyber security measures. More over PWC (2011) in Global Economic Crime Survey found out that there is less chance of law enforcement being able to identify the perpetrator or find out where they were based when they committed and makes it harder to identify arrest and prosecute them by traditional means. The current laws are not mature enough to prosecute cyber criminals with any impact. They also found out that technological advancements are fast-paced, which means the development of cybercrime is too.

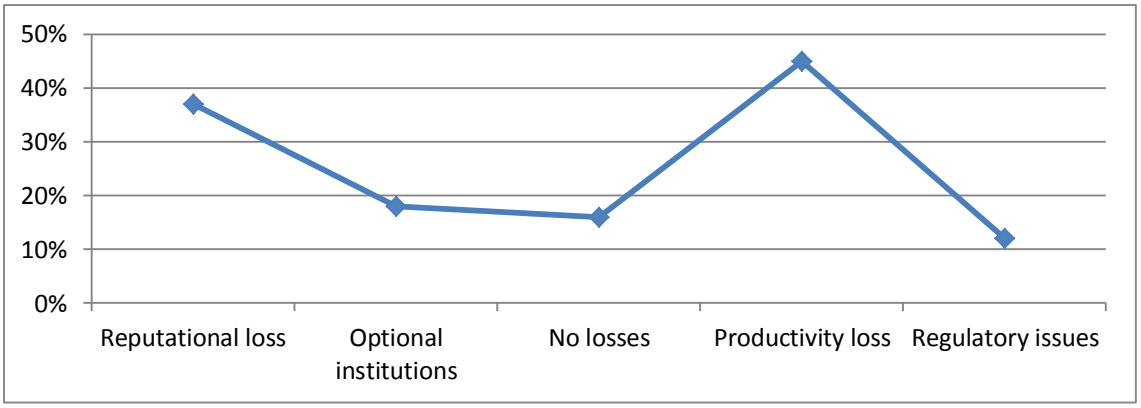
All in all, these other findings in the literature tend to corroborate the findings in the Zimbabwean context.

As indicated by more than 80% of the respondents, fraud risk management is being discussed at the board level at least every quarter. About 75% of the respondents revealed that they had a fraud risk management framework in place with a chief risk officer for managing fraud risk. A total of 50% of the respondents indicated that they are moving towards implementation of digital fraud analytics solution, and 60% of these respondents appear to be more satisfied and comfortable with the move. The core issue with those who have not yet taken the move to implement digital fraud analytics tools is "data integration from current internal systems issues" or insufficiency of data.

PWC (2011) in Global Economic Crime Survey found out that organisations that have performed fraud risk assessments have detected and reported more fraud. A total of 50% of the respondents named Chief Information Officer or Technological Director with ultimate responsibility for dealing with cybercrime and 21% indicated CEO or the Board. Only 36% of respondents said the CEO and the Board review these risks at least once a year, and almost a quarter said they only review them on an ad hoc basis.

However, in Zimbabwean context the Chief Risk Officer is in charge of fraud risk management and the board sits almost four times a year.

Figure 4. Non-financial losses suffered as a result of incidents of fraud



From Figure 4, about 37% of the respondents indicated loss on corporate reputation, 18% showed that customers opted for other institutions. Furthermore, 16% of the respondents indicated that there were no losses as a result of fraud incidents, while 45% of the total respondents indicated that they suffered losses on productivity and 12% of the respondents indicated that they suffered regulatory or other compliance issues.

However,(2011) in Global Economic Crime Survey found out that 40% of the respondents indicated that apart from financial losses suffered of more than us$5million in one in ten of those who reported fraud, reputational damage was the biggest fear. Comparing with the Zimbabwean situation most respondents put more emphasis on productivity loss.

Conclusion

From the above one can conclude that the most frequently occurring type of fraud is still the "traditional" fraud committed by employees in the banks. Identity theft also constitutes a large percentage of fraud. Other forms of fraud such as spam/scam, phishing, pharming, and money laundry represent a portion that is expected to rise, owing to the ever advancing development of technology. Retail banking has been noted as the major contributor to fraud, because retail banking is more a process, and also volume driven and decentralized. In the priority banking sector banks need to consider the risks involved in priority sector lending and develop risk mitigation strategies.

With regard to the incurrence of fraud and the preparedness of the banks to fight menace, it was noted that lack of oversight by line managers or senior managers on deviations from existing electronic process/controls was one of the major causes, followed by the "current business pressure to meet set targets" and a "difficult business scenario" as other causes of fraud cases to rise. An additional factor was the collusion between employees and external parties.

It can be concluded that inadequacy of resources to keep abreast of advanced technology and lack of knowledge and awareness on cyber fraud are major problems. In addition to that digital investigative challenges were identified coupled with lack of cyber fraud detection tools and technologies, and qualified personnel to carry out the investigations. Furthermore, it was noted that there is insufficient legislation and law enforcement to address and tackle e-fraud cases.

Recommendations

Institutions should implement shielded authentication that is not vulnerable to spoofing of web. There is need for implementation of fingerprint authentication merged with graphical models that should include one-time authentication mechanisms which would be effective against both offline and online attacks from spoofing.

Constant educational programs for electronic banking need to be conducted to alert the users on how to always ensure secure online transactions. The Reserve Bank of Zimbabwe should further reduce electronic banking service costs as a method to cultivate increased usage by customers. If the afore-mentioned attributes are implemented in unison, the security strategies implementation will improve from being effective to a much more effective. This would boost the trust of clients and the confidence as well.

There is a need to have an industry wide framework on strong e-fraud governance and legislation and policies with specific emphasis on tackling electronic channel based fraud.

Organisations require a comprehensive enterprise-wide approach to fraud management that supports broader organizational compliance and risk management. The path to this approach includes an IT infrastructure that enables enterprise-wide, real time, and cross-channel monitoring and management capabilities. Bank institutions should work towards developing digital forensic auditors.

Further research

Further research should be done on digital forensics as a tool in preventing and detecting electronic fraud in the banking sector in Zimbabwe

References:

1. Ampratwum, E.F. (2009), Advance Fee Fraud "419" & Investor Confidence in the Economies of Sub-Saharan Africa (SSA), Journal of Financial Crime. Vol. 16 No. 1, pp. 67-79.
2. Aseef, N., Davis, P., et al. (2005), Cyber-criminal Activity and Analysis. White Paper.
3. Bamrara, A., Singh, G. and Bhatt, M. (2012), An Explorative Study of Satisfaction Level of Cyber-crime Victims with Respect to E-Services of Banks, Journal of Internet Banking and Commerce. Vol. 17 No. 3. pp.1-16
4. Bamrara, A., Singh, G. and Bhatt M., (2013), Cyber Attacks & Defense Strategies in India: An Emperical Assessment of Banking Sector, International Journal of Cyber Criminology. Vol.7(1), pp.49-61.
5. Barker, K.J., D'Amato, J. and Sheridon, P., (2008), Credit Card Fraud: awareness and prevention, Journal of Financial Crime. Vol. 15 No. 4, pp. 398-410.
6. BITS (2003), Fraud Prevention Strategies for Internet Banking, A Publication of the BITS Fraud Reduction Steering Committee, www.BITSINFO.ORG
7. Boateng, R., Olumide, L., Isabalija, R.S., and Budu, J. (2011), Sakawa – Cybercrime & Criminality in Ghana, Journal of Information Technology Impact, Vol.11 No. 2, pp. 85-100.
8. Bryman, A. and Bell, E. (2003), Business Research Methods, Oxford University Press.

9. Chang, J.J.S. (2008), An analysis of advance fee fraud on the internet, Journal of Financial Crime, Vol.15 No. 1. pp. 71-81.
10. Cooper, D.R. and Schindler P.S. (2011), Business Research Methods, McGraw-Hill/Irwin Series
11. Crowther, D. and Lancaster, G., (2009), Research Methods: A concise introduction to research in management and business consultancy, Elsevier Butterworth-Heinemann.
12. Detective Assistant Inspector Tom Muleya and Superintendent Moyo Ndabazihle - http://www.techzim.co.zw/2012/03/zim-police-join-the-cyber-warfare/
13. Diaz-Gomez. (no date). What You Need to Know About Cybercrimes, IT Capstone-Research Paper.
14. Dube, T., Chitura, T. and Runyowa, L. (2009), Adoption and use of Internet Banking in Zimbabwe: An Exploratory Study, Journal of Internet Banking and Commerce, Vol. 14 No.1, pp. 1-13
15. EMC, (2013), The Current State of Cybercrime 2013: An Inside Look at the changing Threat Landscape, www.rsa.com.
16. FBI, http://www.fbi.gov/about-us/history/famous-cases/willie-sutton.
17. Frost & Sullivan (*no date*), Key IT Anti-Fraud Challenges for Banking and Financial Institutions in Latin America. White Paper, www.frost.com.
18. Geeta, D. V. (2011), Online identity theft-an Indian perspective, Journal of Financial Crime, Vol. 18 No.3, pp. 235-246. Emerald Group Publishing Ltd.
19. Gercke, M. (2011), Understanding Cybercrime: A Guide for Developing Countries.ICT Applications and Cybersecurity Division.Policies and Strategies Department.ITU Telecommunications Development Sector 2nd Edition, www.itu.int/ITU-D/cyb/cybersecurity/legislation.html
20. Ghauri, P. and Gronhaug, K. (2005). Research Methods in Business Studies: A Practical Guide. Pearson Education Limited.
21. Gono, G. (2013), Monetary Policy Statement issued in terms of the Reserve Bank of Zimbbawe Act Chapter 22:15, Section 46.
22. Ikechi, K.S. and Okay O.E. (2013), The Nature, Extent and Economic Impact of Fraud on Bank Deposits in Nigeria, Interdisciplinary Journal of Contemporary Research in Business, Vol. 4 No. 9, pp. 253-265
23. Jankowicz, A.D. (2005), Business Research Projects, Thomson Learning.
24. Joyner, E. (2011), Detecting and Preventing Fraud in Financial Institutions. Enterprise wide Fraud Management, SAS Global Forum 2011, Paper 029-2011, www.sas.com.
25. Kabay, M.E. (2008), A Brief History of Computer Crime: An Introduction to students.
26. Kabanda, The Independent, April 12, 2012- http://www.theindependent.co.zw/2012/04/12/the-essence-of-cyber-security-it-governance/
27. Kadleck C. (2005), Banks battle against growth of electronic payment fraud. Crain's Cleveland Business 26. No.3, http://www.craincleveland.com/
28. Khan, A. (2011), http://www.scribd.com/doc/71120466/The-First-Recorded-Cyber-Crime-Took-Place-in-the-Year-1820
29. Kritzinger, E. and SH von Solms. (2012), A Framework for Cyber Security in Africa.Journal of Information Assurance and Cibersecurity, Vol. 2012 (2012), Article ID 322399, 10 pages.
30. Kroll. (2011/12), Global Fraud Report. Economist Intelligence Unit Survey Results. www.kroll.com
31. KPMG (2012), Cybercrimes: A financial sector overview, www.kpmg.com/in.
32. Marshall, R. (1995), Computer Fraud – What can be done about it? The CPA Journal; May 1995; 65, 5; Accounting & Tax pg. 30.
33. McGuire M. and Dowling, S. (2013), Cybercrime: A review of the evidence, Chapter 2: Cyber-enabled-crimes-fraud & theft, Home Office Research Report 75.
34. Mwaita, P. and Owor, M. (2013), Workshop Report on Effective Cybercrime Legislation in Eastern Africa, Dar Es Salaam, Tanzania.
35. NCPC (2012), Cybercrime, www.ncpc.org.
36. New York State, Department of Financial Services, (2014), Report on Cyber Security in the Banking Sector.
37. Njanike, K., Dube T. and Mashanyanye E. (2009), The Effectiveness of Forensic Auditing in Detecting, Investigating and Preventing Bank Frauds, Journal of Sustainable Development in Africa, Vol. 10 No. 4, pp. 405-425
38. Oracle (2012), Fraud Fight: Enterprise-wide Strategy Sets the Stage for Victory. Oracle Corporation, www.oracle.com.
39. Page, C. and Meyer D. (2000), Applied Research Design for Business and Management, McGraw-Hill Book Company Australia.
40. Prabowo, H.Y. (2011), Building our defense against credit card fraud: a strategic view, Journal of Money Laundering Control, Vol. 14 No. 4, pp. 371-386. Emerald Group Publishing Ltd.
41. Potter, M. (2000), Internet Banking and Fraud: making business less risky, Community Banker 9 No.7 JI 2000.
42. PWC (2011), Cybercrime: protecting against the growing threat. Global Economic Crime Survey, www.pwc.com/crimesurvey
43. Rajasthan, A. (2013), An Investigative Study of Banking Cyber Frauds with special Reference to Private and Public Sector Banks, Research Journal of Management Sciences, Vol. 2(7), pp. 22-27.
44. Reserve Bank of India, Department of Banking Supervision, Central Office, Mumba, Guidelines on Information Security, Electronic Banking, Technology Risk Management & Cyber Frauds.
45. Schjolberg, S. (2008), ITU Global Cybersecurity Agenda (GCA), High-Level Experts Group Global Strategic Report.
46. Shinder, D.L. (2002), Scene of the Cybercrime: Computer Forensics Handbook, Syngress Publishing.
47. Siddique, M.I. and Rehman, S. (2011), Impact of Electronic Crime in Indian Banking Sector – An Overview. International Journal of Business & Information Technology, Vol. 1 No. 2.
48. Singh, G., Sharma, A., Rampal, K., Kular, R., et al. (2013), India Risk Survey 2013. Pinkerton & Federation of Indian Chambers of Commerce & Industry (FICCI)
49. Singleton, T., (2013), The Top 5 Cybercrimes. American Institute of CPAs.
50. Tam Siong Thye (2002), Money Laundering and E-commerce, Journal of Financial Crime, Vol. 9 No. 3, pp. 277-285. Harry Stewart Publications.
51. Tan Harry S.K. (2002), E-fraud; current trends and International developments, Journal of Financial Crime, Vol. 9 No. 4, pp. 347-354.

52. Tendelkur, R. (2013), Cyber-crime, securities markets and systematic risk, Joint Staff Working Paper of the IOSCO Research Department and World Federation of Exchanges
53. Transport and Communication Minister Christopher Mushowe http://www.newzimbabwe.com/pages/email9.14180.html -11/12/2009
54. Usman, A.K. and Shah M.H. (2013), Critical Success Factors for Preventing e-Banking Fraud, Journal of Internet Banking and Commerce, Vol. 18 No. 2.
55. Williams, D.A. (2007), Credit Card Fraud in Trinidad and Tobago, Journal of Financial Crime, Vol. 14 No. 3.
56. Zakaria, S. (2013), The Impact of Identity Theft or Perceived Security and Trusting E-Commerce, Journal of Internet Banking and Commerce, Vol. 18, No.2.
57. Zimucha, T., Zanamwe N., Chimwayi K., et al. (2012), An Evaluation of the Effectiveness of E-banking Security Strategies in Zimbabwe: A Case Study of Zimbabwean Commercial Banks. Journal of Internet Banking and Commerce, Vol. 17 No. 3, pp. 1-16
58. 41STParameter (2013), The Growing Threats of Cybercrime, www.the41st.com