DIGITAL FORENSIC TECHNOLOGIES AS E-FRAUD RISK MITIGATION TOOLS IN THE BANKING INDUSTRY: EVIDENCE FROM ZIMBABWE

Shewangu Dzomira*

Abstract

The paper investigates digital analytical tools and technologies used in electronic fraud prevention and detection, used in the banking industry. The paper is based on a descriptive study which studied digital forensics and 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 fraud detection and prevention tools and technologies would be most effective way of combating e-fraud if they can be utilized. It is concluded that banking institutions should reshape their anti-fraud strategies to be effective by considering fraud detection efforts using advanced analytics and related tools, software and application to get more efficient oversight.

Keywords: Digital Forensics, Data Analysis, Analytical Tools, Cyber Fraud, Cross- Channel Fraud

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

1. Introduction

It is an endless game of “cat and mouse” between banks and cybercriminals. There is a virtual arms race taking place online between financial institutions and cybercriminals who as soon as the bank deploys a new process or technology to prevent online fraud, they find a weakness to exploit (ACI, 2013). Cyber banking has recently become a necessity rather than a “superfluity” service across the banking industry. As a result recent developments have shown that most of brick and mortar banks are evolving themselves by shifting their focus towards up gradation of their own e-banking capabilities (Kesharwani & Radhakrishna, 2013).

According to Bhasin (2013), Sherlock Holmes is considered to be the first forensic accountant (Kahan, 2004), the term coined by Peloubet in 1946 (Joshi, 2003). Kautilya, from India was the first economist to openly recognise the need of a forensic accountant after mentioning the famous forty ways of embezzlement during the ancient times. In the Egyptian times, 3300-3500BC, commercial transactions were recorded on clay tablets, which would be scaled and if later found to be tempered with, investigations would take place (Nurse, 2002), cited Bhasin (2013). He adds that any discovered employee crime attracted punishment of a fine, mutilation or death in some cases.

Today, the challenge of combating fraud directed against a business is increased by the diversity and deceptive nature of workplace fraud and a company may realize too late that it has been victimized (KPMG, 2006). Bailard et al. (2013) observe that fraudsters, hackers and cybercriminals are improving their methods for account takeover and compromised identities that target bank’s customers and employees. The growth of complexity and access to technology has made susceptibility to ‘hi-tech’ crime which is a threat to businesses in the financial domain where the risk is very high (KPMG, 2012). Also, cybercrime is on the rise; large-scale fraud attacks, consumer data breaches and politically motivated Distributed Denial of Service (DDoS) attacks on financial institutions are costing them billions of dollars annually (41ST Parameters, 2013).

According to Raghavan & Parthiban (2014), Information Communication Technology (ICT) has brought unintended consequences in form of different cybercrimes which have affected different industries and the banking sector is one of them which have witnessed debit/card fraud, phishing, funds transfer, account takeover, identity theft, DoS and many others. Crane (2013) posits that, one problem is that digital forensics is not just about computer any more – smart phones, tablets, thumb drives and more each present unique challenges in accessing data.

Although researches have been done on electronic banking in Zimbabwe, the author found no research that specifically addressed digital forensic technologies as a cyber-fraud risk mitigation tool in the banking industry.

In light of the above background, the paper aims to achieve the following objectives:

- to explore the possibility of reducing electronic fraud cases using digital forensics in the banking industry,
- to examine digital technologies being used on electronic fraud prevention and detection in the banking industry.

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

2. Literature review

Whilst no one can dispute the paradigm that technology in the financial domain has brought efficiency and convenience in the way business transactions are executed however, the challenge still remains on the adequacy of effective digital technologies and systems to mitigate the risk associated with digital transactions. Digital forensics tools have allowed for fast and reliable data acquisition and analysis, which is imperative in a world where information can disappear quickly (Crane, 2013). Computer forensics emerged in response to the escalation of crimes committed by the use of computer systems either as an object of crime, an instrument used to commit a crime or a repository of evidence related to a crime (Baryamureeba & Tushabe, 2004; Agarwal, et al, 2011).

Today's business environment generates vast amounts of data and information and hundreds of billions of dollars are lost annually due to fraud, financial mismanagement or other malfeasance such as information deletion, policy violation or unauthorised access (Deloitte, 2013). Fraud detection and prevention is crucial to maintaining a successful web business and no merchant can afford to overlook the need for protection against fraud (Authorize.Net, 2006). In addition to that Bhasin (2013) cited that, forensic accounting has come into lime light due to rapid increase in financial frauds and white collar crimes.

Digital forensics has been defined by many authors as the use of scientifically derived and proven analytical techniques towards the preservation, collection/extraction, examination, validation, identification, analysis, interpretation, documentation and presentation of data from digital/electronic sources or magnetically stored/encoded for evidentiary purposes and root cause analysis (Baryamureeba & Tushabe, 2004; IIA, 2009; PWC, no date; Mercuri, 2005; Carrier, 2003). However, according to Garfinkel (2010), golden age of digital forensics is quickly coming to an end and increasingly organisations encounter data that cannot be analysed with today's tools because of format incompatibilities, encryption, or simply a lack of training. Given the inherent complexity of the online banking platform and the dramatic increase in mobile banking, preventing online fraud presents financial institutions with the number of highly complex challenges to overcome (ACI, 2013).

Moreover, digital crime has increased in frequency and inflicts immense damage to users and systems and the level of sophistication has been reached that makes it hard to track its sources of origins especially with the advancements in modern computer networks and the availability of diverse electronic devices (Selamat et al, 2013; Alharbi et al, 2011). In the modern era, digital forensics is an important tool for solving digital fraud crimes committed (for example phishing, money laundering and other bank frauds) as well as solving crimes where evidence resides in a computer (Garfinkel, 2010). A framework for digital forensics, therefore needs to be flexible enough so that it can support future technologies and different types of incidents (Carrier & Spafford, 2004).

While there is no fool proof way of preventing fraud, certain fraud prevention techniques have proven to be successful (PWC, no date). Cyber security is not a technology problem that can be "solved", it is a risk to be managed by a combination of defensive technology, astute analysis and informative warfare and a traditional diplomacy (KPMG, 2012). The primary reason of data analytics in tackling fraud is because a lot of internal control systems have serious control weaknesses and its key aspect is the ability for the technology to maintain comprehensive logs of all performed activities and electronic transactions fraudulent activity or heightened fraud risk. While it is important and a win to uncover fraudulent activity that has been going on for several years but identifying the issue before it is material serves the organisation immensely on financial damage (ACL, 2013; ACL, 2014). According to Usman & Shah (2013), fraud in e-banking services occur as a result of various compromises in security ranging from weak authentication systems to insufficient internal controls. However, to attain a better situation banks apply more rigorous technologies for identifying and tracking hostile devices and using more sophisticated link analysis tools that search for connections between seemingly disparate events (41ST Parameters, 2013).

Data analytics tools can mine through digital data and identify hidden relationships and red flags thereby enabling banks to proactively identify potential fraudulent transactions before they manifest themselves years down the line (Deloitte, 2013). More so, there is a spectrum of analysis that can be deployed to detect fraud, that ranges from point-in-time analysis conducted in an ad hoc context for one-off fraud investigation or exploration, through to repetitive analysis of business where fraudulent is likely to occur (ACL, 2014). To test and monitor internal controls effectively, organisations should analyse all relevant transactions against control parameters, across all systems and all applications and examining transactions at source level helps assure the integrity and accuracy of the information (IIA, 2009).

Common digital analysis would include media analysis, media management analysis, file system analysis, application analysis, network analysis, operating system analysis, executable analysis (intrusion investigations), image analysis, video analysis and memory analysis (Carrier & Apafford, 2004; Carrier, 2003). According to ACL (2014) & IIA (2009), analytical fraud detection techniques include the following: calculation of statistical parameters, classification, stratification of numbers, Benford's law (digital analysis), joining different diverse sources, duplicate testing, gap testing, summing of numeric values and validating entry dates.

Cyber criminals know bank fraud systems rarely monitor customer behaviour across multiple accounts, channels and systems and this weakness opens the door for cross-channel fraud, in which a fraudster gains access to customer information in one channel and uses that to commit fraud through another (Joyner, 2011).

Financial institutions are faced with a number of ways to prevent and detect cyber fraud crime complementing digital forensics tools. Advances in technology increasingly allow organisations to implement automated controls to help prevent and detect fraud and to move from static or periodic fraud monitoring techniques such as detective controls, to continuous, real time fraud monitoring techniques (IIA, 2009). However, given that conventional methods of authentication via usernames and passwords are no longer sufficient (Vandommele, 2010), biometric technology has been identified as one of the potential technologies to improving security and prevent e-fraud (Usman & Shah, 2013). More so, to achieve better situational awareness, banks are improving customer visibility across lines of business and enhancing coordination between channels and educating the customer on how to help prevent online banking fraud defences (41^{ST} Parameters, 2013; ACI, 2013).

Rowlingson (2004) cited that, Yasinsac & Manzano (2002) noted that enterprise policies can enhance computer and network forensics and proposed; retention of information, planning the response, training, accelerating the investigation, preventing anonymous activities and protecting the evidence. An online fraud detection model is an online operational risk management system specifically designed to optimize online fraud investigation resources by queuing high-risk online banking activities in real-time for investigation (Pandey, 2010). The ultimate goal of intrusion detection is to identify, preferably in real-time, unauthorized use, misuse and abuse of computer systems by both systems insiders and external perpetrators (Balon et al, no date). Some intrusion detection systems (IDS) have the ability to store all sessions for a short period of time so that if something suspicious is detected, the previous activity in the same session can be preserved (intrusion prevention capabilities) (Kent et al, 2006). According to Joyner (2011), in a case study 2007, FBPB implemented a complete, end-to-end IT platform for detecting, preventing and investigation both opportunistic and organised first-party fraud. Rather than take a reactive approach to fraud detection by relying solely on tips and whistle-blower programs, banks should include an evaluation by internal auditing of the operating effectiveness of internal controls, along with an analysis of transaction-level of data for specific fraud indicators (IIA, 2009).

3. Methodology

The research on which this paper reports pertains to digital forensic tools and technologies as electronic fraud (cyber fraud) risk mitigation tool in the banking industry using Zimbabwe as a unit of analysis. The study was based on descriptive research. The purpose of descriptive study is to describe the characteristics of phenomena, relations between variables or relationships between phenomena and can be the purpose of qualitative and quantitative studies (Plooy-Cilliers et al, 2014). The descriptive study is popular in research because of its versatility across management disciplines (Cooper & Schindler, 2011). Descriptive research is intended to merely describe a phenomenon and the researcher does not manipulate any variables, and makes no effort to determine the relationship between variables (Brink et al., 2012). In this study the use and application of digital forensic tools to combat the risk of e-fraud in the banking industry, 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 used. Purposive and convenience sampling techniques were used. Purposive or judgmental sampling is based on the judgment of the researcher regarding participants that are typical or representative of the study phenomenon or who are especially knowledgeable about the question at hand (Brink et al, 2013). Convenience or accidental or availability sampling refers to situations when population elements/participants are selected based on the fact that they are easily and conveniently or readily available for the study (Kobus et al, 2013; Brink, 2013). 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 cyber fraud risk and digital forensics.

5. Tools for analysis

In this study a qualitative analysis was done using content analysis of data. According to Kobus et al, (2013), content analysis is a systematic approach to qualitative data analysis that identifies and summarizes message content (Neuendorf, 2002). 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 frequencies, 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).

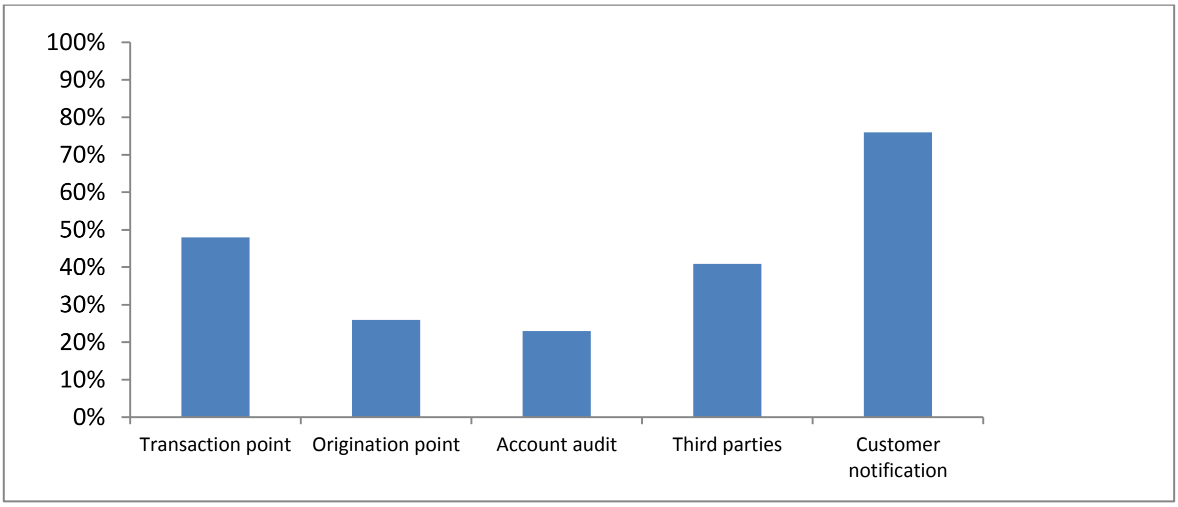
6. Findings

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

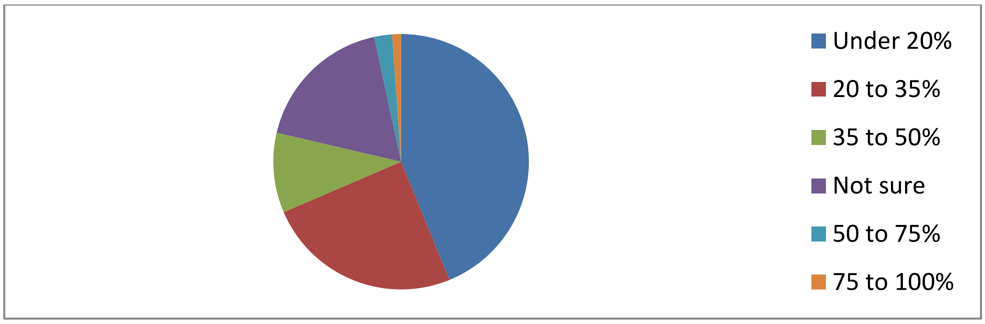
All the 28 respondents at least had passed Ordinary level and joined their respective institutions having acquired that qualification. A number of them (86%) had passed their Advanced Levels. Few of the respondents (43%) had bank related qualifications, such as Institute of Bankers Certificate or Diploma (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.

Figure 1. Fraud incident detection



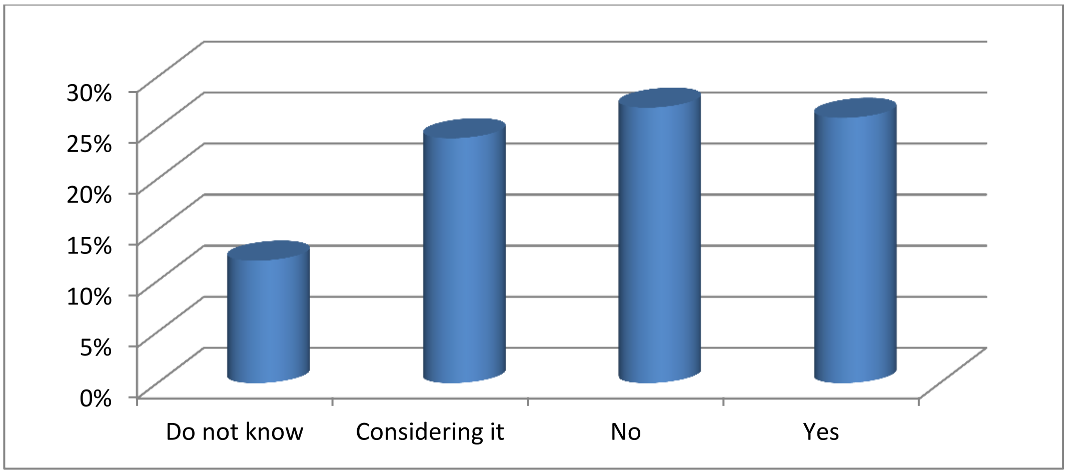
A total of 76% of the respondents learn about the fraud incidents from the customers, 48% of the total respondents indicated that they detect fraud cases at the point of transaction, 41% of the respondents showed that they get to know of the fraud incidents from third party notification. About 26% of the respondents revealed that at the point of origin that's when they learn about fraud incidents using detecting techniques tools and the 23% of the respondents indicated that during account audit or reconciliations that is when they know discover the fraud incident.

Figure 2. Cross-channel fraud



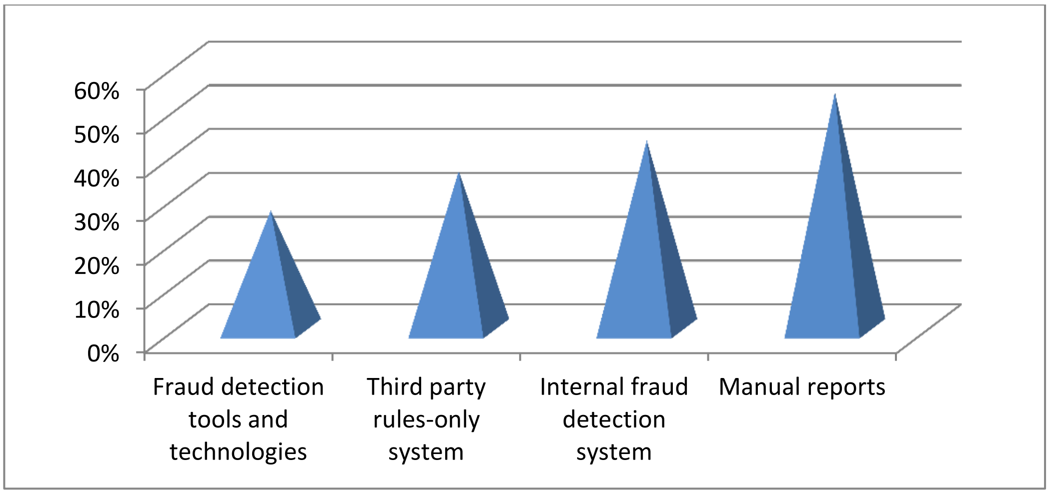
A total of 61% indicated that up to 35% of their fraud incidents are cross-channel while 16% were not sure about cross-channel fraud and 12 % revealed that from 35% up to 100% of their fraud cases is cross-channel.

Figure 3. Team assigned to execute plan and controls to detect cross-channel fraud



27% of the respondents said "no" they do not have a defined plan, a team assigned to execute this plan and controls to detect cross-channel fraud. 26% said "yes" they do have the plan, team and controls whilst 24% indicated that they were working on it and 12% of the respondents indicated that they "do not know".

Figure 4. Fraud detection tools employed



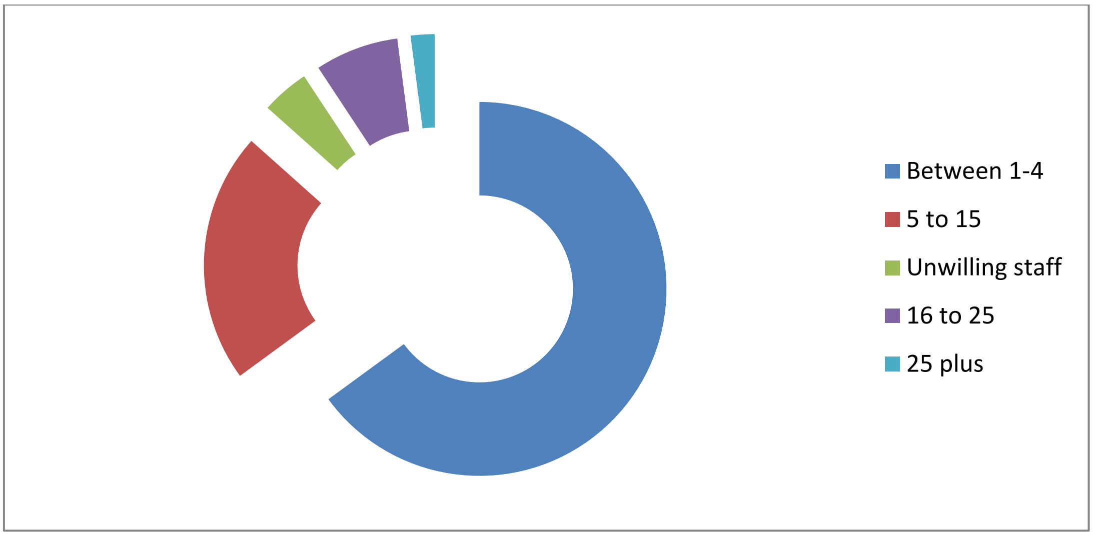
Of the total respondents 54% rely on manual reports to detect frauds. 43% of the respondents indicated that they rely on internal fraud detection system whilst 36% showed that they rely on third party rules-only system and 27% indicated that they rely on independent fraud detection tools and technologies for each channel.

Table 4. Alignment of fraud detection tools to detect cross-channel patterns

Description	Response (%)
No	38%
Yes	16%
Working on considering it	8%
To some extent	21%

About 38% of the total respondents indicated that their organisation's fraud detection tools are not aligned to detect cross-channel patterns, 16% of the respondents showed that there is alignment whilst 8% indicated that they are still working on it and 21% said to some extent they are aligned.

Figure 5. Number of people assigned for fraud prevention



63% of the total respondents indicated that between 4 to 5 people are assigned for fraud prevention. 21% showed that 5 to 15 people are assigned for prevention of fraud whilst 4% revealed that there are unwilling staff. 7% indicated that 16 to 25 people are assigned in fraud prevention and 2% of the respondents indicated that 25 plus are assigned for prevention of fraud.

Table 5. Most effective ways of fraud prevention and detection

Way	Response (%)
Fraud detection tools and technologies	80%
Real-time decision tools	43%
Monitoring of accounts manually	22%
Customer awareness on techniques used by fraudsters such as phishing, pharming etc	77%
Training of employees on identification and response to fraudulent activities.	76%

Of the total respondents 80% indicated that fraud detection tools and technologies is the most effective way of combating fraud. 43% of the respondents showed that real-time decision tools are effective in preventing fraud. 22% showed that monitoring of accounts is effective whilst 77% indicated that customer awareness is most effective of preventing fraud and 76% of the respondents revealed that training of employee putting emphasis on identification and response to fraudulent activities is the most effective way of preventing fraud in organisations.

Whilst, according to Deloitte (2013) survey in Tanzania most of the organisations use the following financial crimes detection mechanisms (50%); risk based internal audits (100%), ongoing risk based transaction monitoring (50%), technology solutions and whistleblowing/hotline (50%).

Table 6. Usage of other digital technologies on fraud prevention and detection

Way	Response (%)
Prevention technologies intrusion	87%
Fraud case management system	76%
End-to-end encryption	68%
Neural net fraud detection technologies	70%
Strong authentication, out-of-band authentication and knowledge-based authentication	65%

A total of 87% of the respondents indicated that they are planning to use prevention technologies intrusion. About 76% of the total respondents showed that fraud case management system be planned for use, 68% of the respondents revealed that they intend to use end-to-end encryption in future, whilst 70%

indicated that they plan to apply neural net fraud detection technologies and 65% of the respondents plan to use strong authentication, out-of-band authentication and knowledge-based authentication as on-going fraud prevention and detection program in future.

However, Deloitte (2013) survey found that in Tanzania regular trainings on financial crimes' trends and risks, ongoing monitoring of employees' activities in high risk departments, technology solutions and robust financial crimes control mechanisms forms the major prevention mechanisms.

Conclusions

From the above one can conclude that most electronic fraud incidents were learnt from customers' complaints followed by detection on point of transaction and third party notification respectively. Also fraud incidents detection was noted at origination point and through internal audits. Cross channel fraud can be concluded to be unfamiliar to most of the banks while other banks are experiencing it. Other banks do not have a defined plan and teams assigned for detection of cross channel fraud and others are working towards its implementation.

More so, it can be concluded that majority of the fraud cases are still detected through the formal and informal mechanisms. Internal audit reviews are used to detect fraud whilst other cases are detected accidentally and by anonymous complaints from third parties. This indicates that apart from anti-fraud strategies adopted by the banks, a significant number of frauds are detected by ways outside the organisation's electronic fraud control framework. However, the respondents felt that fraud detection tools and technologies would be most effective way of combating fraud risk and real time decision tools. Most banks are prepared to use intrusion technologies, fraud case management system, end-to-end encryption and application of neural net fraud detection.

However, banking institutions should reshape their anti-fraud strategies to be effective by considering fraud detection efforts using advanced analytics and related tools, software and application to get more efficient oversight. These would also help enhance fraud deterrence and also show regulators an enterprise-wide commitment.

Banks should create risk based layered fraud defences to remain competitive with threats of cyber fraud crimes rather than relying on one approach. Financial institutions must continually test, retest and revise their strategies in relation to changes in the threat landscape through an embraced security portfolio of related tools, tactics and strategies.

Financial institutions should also have programs for fraud prevention and detection incorporating a spectrum of transactional data analysis ranging from ad hoc, to repetitive, to continuous. Application of such programs would reduce likelihood of greater losses since fraud can be detected earlier.

References:

1. ACI, (2013), Fighting online fraud: An Industry perspective. Vol. 3, www.aciworldwide.com
2. ACL, (2013), Detecting and Preventing Fraud with Data Analytics. www.acl.com
3. ACL, (2014), Fraud Detection Using Data Analytics in the Banking Industry. www.acl.com
4. Agarwal, A., Gupta, S., Gupta, S., Gupta, S.C., (2011), Systematic Digital Forensic Investigation Model. International Journal of Computer Science and Security, Vol.5 Issue 1, pp.118-131
5. Alharbi, S., Weber-Jahnke, J., Traore, I., (2011), The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review. International Journal of Security and its Applications, Vol. 5 No.4, pp.59-72
6. Arnes, A., Haas, P., Vigna, G., Kemmerer, A., (no date), Digital Forensic Reconstruction and the Virtual Security Testbed ViSe.
7. Authorize.Net, (2006), Fraud Detection Suite. www.authorize.net
8. Bailard, F., Busony, B., Lilienthal, G., (2013), Organized Cyber Crime and Bank Account Takeovers. Federal Reserve Bank of San Francisco, Division of Banking Supervision and Regulation.
9. Balon, N., Stovall, R., Scaria, T., (no date), Compute Intrusion Forensics Research Paper.
10. Baryamureeba, V., Tushabe, F., (2004), The Enhanced Digital Investigation Process Model. www.makerere.ac.ug/ics
11. Bhasin, M.L., (2013), Corporate Governance and Forensic Accountant's Role; Global Regulatory Action Scenario. International Journal of Accounting Research, Vol.1 No.1, pp. 1-19
12. Brink H., Walt, C., Rensburg, G., (2012), Fundamentals of Research Methodology for Healthcare Professionals, Juta & Company, South Africa.
13. Carrier, B.D., Spafford, E.H., (2004), An Event Based Digital Forensics Investigation Framework.
14. Carrier, B., (2003), Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers. International Journal of Digital Evidence, Vol.1 Issue 4, pp.1-11
15. CERT Australia, & CIS, (2012), Cyber Crime and Security Survey Report 2012. Australia Government.
16. Cooper, D.R. and Schindler P.S. (2011), Business Research Methods, McGraw-Hill/Irwin Series
17. Crowther, D. and Lancaster, G., (2009), Research Methods: A concise introduction to research in management and business consultancy, Elsevier Butterworth-Heinemann.
18. Crane, B., (2013), Digital Forensics: A Decade of Changes. http://www.policemag.com/blog/technology/story/2013/11/digital-forensics-a-decade-of-changes.aspx
19. Deloitte, (2013), Deloitte Forensic. Protecting your business in the Banking sector. www.deloitte.com
20. Deloitte, (2013), Financial Crimes Survey Report 2013. Where is the exposure? www.deloitte.com
21. EMC, (2013), The Current State of Cybercrime 2013. An Inside Look at the Changing Threat Landscape. www.rsa.com

22. Global Digital Forensics, (2006), Case study – Banking Industry Executive Level Financial Fraud. http://www.evestigate.com
23. Garfinkel, S.L., (2010), Digital forensics research: The next 10 years. 7(2010) S64-S73
24. Joyner, E., (2011), Enterprise Fraud Management. SAS Global Forum 2011. Banking, Financial Services and Insurance. www.sas.com
25. Kasharwani, A., Radhakrishna, G., (2013), Drivers and Inhibitors of Internet Banking Adoption in India. Journal of Internet Banking and Commerce, Vol.18 No.3, pp.1-18
26. Kent, K., Chevailer, S., Grance, T., Dang, H., (2006), Guide to Integrating Forensic Techniques into Incident Response, Recommendations of the National Institute of Standards and Technology.
27. Kobus, M., et al, (2013), First Steps in Research, Van Schaik Publishers, South Africa.
28. KPMG Forensic, (2006), Guide to Preventing Workplace Fraud. Taking Action to Reduce Business Crime Exposure.
29. KPMG, (2012), Government and Public Sector Cybercrimes. A Financial Sector View.
30. Mercuri, R.T., (2005), Challenges in Forensic Computing. Communications of the ACM, Vol.48 No.12, pp.17-21
31. Mujuru, J., (2011), Forensic Conference tackles white collar crime in Africa. http://www.theafricareport.com/News-Analysis/forensic-conference-tackles-white-collar-crime-in-africa.html. Posted on Tuesday, 14 June 2011 18:11
32. Nyemba, P., (2011), Forensic Conference tackles white collar crime in Africa. http://www.theafricareport.com/News-Analysis/forensic-conference-tackles-white-collar-crime-in-africa.html Posted on Tuesday, 14 June 2011 18:11
33. Page, C. and Meyer D. (2000), Applied Research Design for Business and Management, McGraw-Hill Book Company Australia.
34. Pandey, M., (2010), A Model for managing online fraud risk using transaction validation. The Journal of Operational Risk, Vol. 5 No.1, pp.49-63
35. Plooy-Cilliers, F., Davis, C., Bezuidenhout, R., (2014), Research Matters, Juta & Company, South Africa.
36. PWC, (2008), Fraud A Guide to its prevention, detection and investigation. www.pwc.com/au
37. Raghavana, A.R., Parthiban, L., (2014), The effect of cybercrime on a Bank's finances. International Journal of Current Research & Academic Review, Volume 2 No.2, pp.173-178
38. Rowlingson, R., (2004), A Ten Step Process for Forensic Readiness. International Journal of Digital Evidence, Vol.2 Issue 3, pp.1-27
39. Selamat, R.S., Sahib, S., Hafeizah, N., Yosof, R., Abdollar, M.F., (2013), A Forensic Traceability Index in Digital Forensic Invesitigation. Journal of Information Security, Vol.4.19-32
40. The Institute of Internal Auditors, (2009), Fraud Prevention and Detection in an Automated World. www.theiia.org
41. Usman, A.K., Shah,M.H., (2013), Critical Success Factors for Preventing e-Banking Fraud. Journal of Internet Banking and Commerce, Vol.18 No.2, pp.1-15
42. 41ST Parameter. (2013), The Growing Threats of Cyber Crime, www.the41st.com.