“Cyber-banking fraud risk mitigation conceptual model”

AUTHORS	Shewangu Dzomira

ARTICLE INFO	Shewangu Dzomira (2015). Cyber-banking fraud risk mitigation conceptual model. *Banks and Bank Systems*, *10*(2), 7-14
RELEASED ON	Friday, 31 July 2015
JOURNAL	"Banks and Bank Systems"
FOUNDER	LLC “Consulting Publishing Company “Business Perspectives”

NUMBER OF REFERENCES
0

NUMBER OF FIGURES
0

NUMBER OF TABLES
0

Shewangu Dzomira (South Africa)

Cyber-banking fraud risk mitigation – conceptual model

Abstract

The paper discourses the conceptualization of the cyber-banking fraud in an effort to mitigate the risk. Key role players and elements in electronic and online fraud (cyber fraud) risk management are examined, concerns addressed and the answer is suggested. The key participants and elements include e-fraud victims; fraudster (s), guardian (bank), environmental factors and fraud types. This paper is based on conceptual study and applies ontological tradition which emphasizes concepts that identify the basic features of the cyber fraud risk management phenomena and aims to explore how the banking community experiences the reality. The paper concluded by assimilating all the pertinent elements in cyber fraud risk management into a proposed model to aid financial institutions in mitigating cyber fraud risk and the model development creates a different way of looking at cyber fraud risk management phenomenon since it shows a logical extension of current knowledge.

Keywords: cyber-banking, e-fraud, mobile banking, cyber-fraudster, model.
JEL Classification: M15.

Introduction

Cyber-banking has proved indestructible to attacks, but the elementary dynamic of the online world has always been that it is unproblematic to beat than to shield. There are reasons to believe that resilience is gradually being undermined, allowing this dynamic of vulnerability to become more impactful in the wake of the "digitization of things" growth (World Economic Forum, 2014). For financial institutions, the free flow of digital information means that the backdoor is potentially always open to loss for instance, Russian cracker Vladimir Levin, siphoned $10 million from Citibank and transferred the money to bank accounts around the world (Aseef et al., 2005). In spite of the size of the banking institution or its operating alleyway, its provision of online banking services to customers poses the threat of e-fraud via the same channel. Clearly, internet fraud is a significant challenge for the financial services sector but however, financial institutions are increasingly offering online banking services to their customers (BITS, 2003). Banks, therefore need continuous improvement mindset that tests and retests the bank's e-fraud defences (ACI, 2013), since cyber-fraudsters always make use of the fissure hastily, quietly and be long gone before the bank or its customers unearth the predicament.

In the anonymous world of the internet, online transaction fraud has also been a greatest challenge for web merchants. This non-face-to-face environment of e-commerce makes verification of the true identity of a person extremely difficult (Harry, 2002). The complexity of the cyber-fraud phenomena is fuelled more as the world moves closer into becoming a global cashless society (Prabowo, 2011), and this has brought about even more urbane electronic fraud forms. The growth of more efficient banking systems which are at the same time vulnerable to fraudsters have been on the rise recently. Many banks have been looking to the mobile banking means as an area for augmented transformation and customer interaction. Unfortunately, cyber-criminals see an opportunity in mobile channel and they invent new ways to twist customer convenience to their own criminal advantage (41ST Parameter, 2013) and the security measures that are in place for online banking tend to be insufficient to cover new mobile channels.

According to Barker et al. (2008), it is a known fact that credit card is a growing problem owing to multiple skimming, counterfeiting and phishing schemes which occur throughout each year costing companies and victims billions of dollars. More so, while offering numerous advantages and opening up new channels for transaction business, the internet has brought in increased probability of e-fraud in credit card transactions (Bhatla et al., 2003). Undoubtedly, global networking presents as many new opportunities for fraudsters as it does for business and as card business transactions increase, so too do fraud. According to Tendelkur (2013), a suspected cyber attack brought down system and computers at some of Korea's major banks and broadcasters and that affected the local equity market which declined by 1.0%.

Despite the effectiveness of risk management systems being deployed, there are always individuals or groups of individuals who are able to spot an opportunity and circumvent or override controls (PWC, 2011) exclusively when it involves cyber fraud security. In addition, according to Joyner (2011) lack of fraud systems that monitor customer behavior across multiple accounts, channels and systems opens the door for cross-channel fraud, in which a fraudster gains access to customer information in one channel and uses it to perpetrate fraud via another channel.

Against this background the paper seeks to:

- Critically review the forms of cyber banking fraud risks exposed in the financial sector.

Shewangu Dzomira, Ph.D., Department of Finance, Risk Management and Banking, College of Economics & Management Sciences, University of South Africa, South Africa.

- To propose a cyber-banking fraud risk management model.

1. Conceptual and empirical literature review

Financial services institutions which are usually targets of cyber-fraudsters suffer from multifarious malware attacks in form of online phishing, keystroke-loggings malwares, and identity theft. According to Raghavan & Parthiban (2014), there are a number of e-fraud types witnessed in the banking sector like ATM fraud, cyber money laundering and credit card fraud and in general all the fraud types are executed with the ultimate goal of gaining access to user's bank account. This concurs with Dzomira (2014), that electronic fraud is classified into two categories namely direct fraud (e.g. money laundering, salami technique, employee embezzlement) and indirect fraud (e.g. malware, phishing, identity theft, etc.). Moreover, network-based threats, such as hacks, site defacement attacks, denial of service attacks, viruses and worms attack the core networks and infrastructure but do not directly try to carry out transactions and are not application specific (BITS, 2003).

Most banking institutions face the risk of their servers being attacked with cyber-fraudsters. According to Harry (2002), hackers and crackers directly attack servers to commit cybercrimes such as stealing passwords, credit card information and other confidential or secret information; to intercept transactions and communications, and to cause damage such as mutilation of websites or to corrupt or insert viruses into database of the target server. Hacking also involves the threat of unauthorized computer access to customer accounts over the internet by non-bank employees (hacker or interloper) (Potter, 2000). Hacking is all about gaining unauthorized access to and publicly exposing in plain view on the internet large amounts of confidential data with the aim of causing monetary and reputational damages to the targeted entity (EMC, 2013).

Financial services institutions should always stay alert on the e-fraud since with every new banking service, a new set of fraud risks emerge. Fraudsters perform illicit activity known as account takeover (ATO) after having illegally obtained valid customer's personal credentials (ACI, 2013). In account takeover the fraudster assumes complete control of a legitimate account by either providing the customer's account number or the card number (Bhatla et al., 2003). According to EMC (2013), "man-in-the-middle" and "man-in-the-browser" (MITB) Trojan attacks continue to be used as a weapon of choice for cybercriminals to perpetrate account takeover. For instance Aite Group estimated that account takeover was responsible for US$455 million in global losses to financial institutions in 2012 and expected that figure to increase to US$794 million by 2016 (EMC, 2013).

More so, according to KPMG (2012) malware is a software that takes control of any individual's computer to spread a bug to other people's devices or social networking profiles or as given by (Bailard et al., 2013), they described it as a common name given for all types of unwanted software such as viruses, worms, Trojan that can harm one's files and programs. Such software can be used to create a "botnet" that is a network of computers controlled remotely by hackers known as "herders" to spread spam or viruses and also that the criminals have a number of tools at their disposal to infect a customer's computer with malicious software or malware. In some instances a fraudster sends an email that convinces the recipient to click on a link, which in turn download the malware directly to the user's machine and the perpetrator waits for the customer to access the bank and steal their session directly in real time unbeknown to the customer (ACI, 2013). Therefore malware is designed to prevent detection both by human user and antivirus scans (41ST Parameter, 2013).

Another type of indirect fraud which poses threat to customers and banks is phishing. Phishing can simply imitate the actual daily deal email, replacing the legitimate links with nefarious ones which includes key loggers that capture the credentials for banking or other sensitive sites (41ST Parameter, 2013; KPMG, 2012; Gercke, 2011). The fraudsters (fishermen) send out a large amount of emails (the "bait") directing the victims to their phony websites (Barker et al., 2008; Usman et al., 2013; Bailard et al., 2013), and the emails are intended to hoodwink the customers as they would appear genuine. In this era of mobile channels of transacting business fraudsters also resort to mobile pharming/smishing/vishing (phishing by phone). Smishing involves sending of unsolicited test messages that prompt users to provide credentials (banking, e-commerce merchant sites which contains valuable loyalty points or stored payment card information that can be used for fraudulent purposes) (41ST Parameter, 2013). With the detonation in smart-phone usage, fraudsters have found a way to collect data they require to perpetrate fraud. Similar to email phishing scheme, mobile pharming/smishing sends a text message sometimes even described as a "fraud alert" that asks the recipient to provide personal banking access information (ACI, 2013).

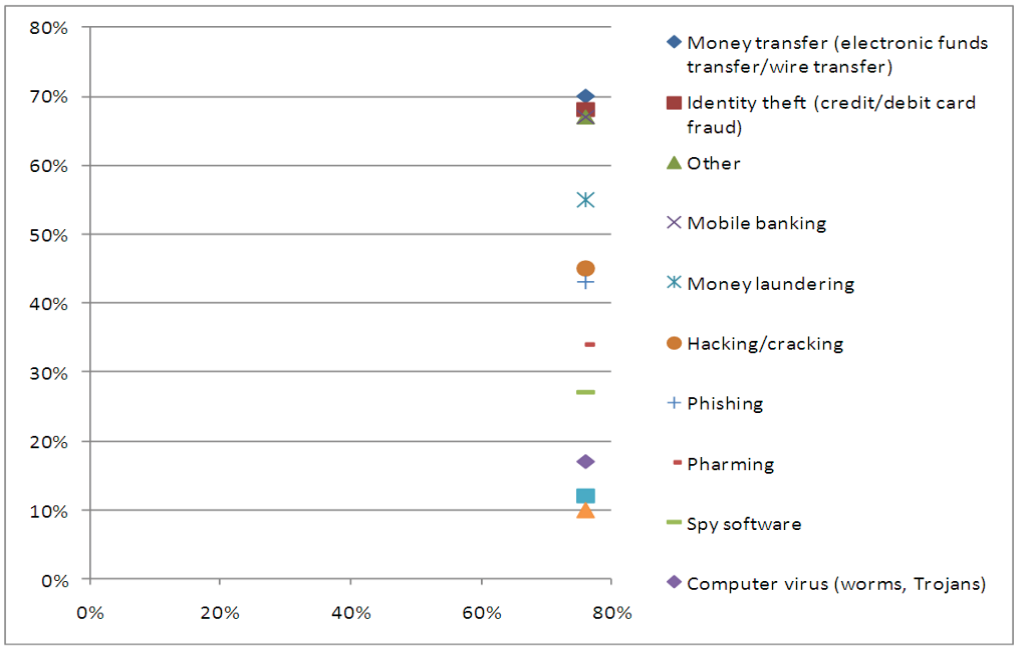
Electronic banking system users still face the security risks with unauthorized access into their banking accounts via identity theft. Identity theft is one of the fastest growing crimes in which a criminal obtains key pieces of personal information or person's identity in order to use for personal gain or in some way that involves fraud or deception (Saleh, 2013; Gercke,

2011; Harry, 2002). A similar fraud type involves the use of individual's credit card or corresponding data for payment of goods and services while the owner of the card and the issuer of the card are unaware (Simic, 2005). In other instances both the customer and the online merchant are potential victims of credit card fraud schemes (Harry, 2002), as customers may be persuaded to part with their credit card particulars to fraudulent merchants who then record transactions that are no fulfilled with the credit card companies. For instance, in 2012 an attack (Operation High Roller) siphoned around US$78 to U$2.5 billion from bank accounts in Europe, the USA and Latin America, and the attack located a victim's highest value account and transfer the money to a prepared debit card (which can be cashed in anonymously) (Tendelkur, 2013).

Moreover, new technologies and cyber space offer money launderers' new opportunities to perpetrate fraud and the intention of money laundering are to convert illicit cash to a less suspicious form, so that the true source or ownership is concealed (Thye Tan, 2002). In money laundering funds are electronically transferred among multifarious accounts disguising the origin of the funds via a series of complex transactions. According to NFC (2000), money laundering is the conduct of the customer of financial institution who deposits the proceeds of criminal activity with the bank and uses the bank to layer or launder the proceeds and to make easy the transportation of proceeds into or out of the country. Of late almost every bank institution operates online services and electronic wire transfer, and they are particularly susceptible to such conduct.

Electronic fraud can be also initiated from within a financial institution via collusion of bank's insiders and cyber criminals. According to ACI (2013), involvement of bank insiders (collusion), mostly bank employees with access to customer data can be coerced, bribed, blackmailed or duped by cyber fraudsters to disclose such information. In addition to collusion some bank employees often perpetrate what is called salami fraud. As Kabay (2008) posits, in the salami technique criminals steal money a bit at a time. An account of a customer is debited with a smallest or insignificant amount that normally a customer takes as immaterial but the fraudster does it to a huge number of customer accounts within the bank. At the end the fraudster builds up a significant amount of money from "tiny scraps" like salami.

All in all, most financial institutions face challenges of inadequate resources especially technological and (GTAG, 2009) tight budgets, limited staffing and extended workloads, lack of legislation, and education and awareness. Against this background there is a need for proactive role in assisting bank institutions in managing and mitigating fraud risks.



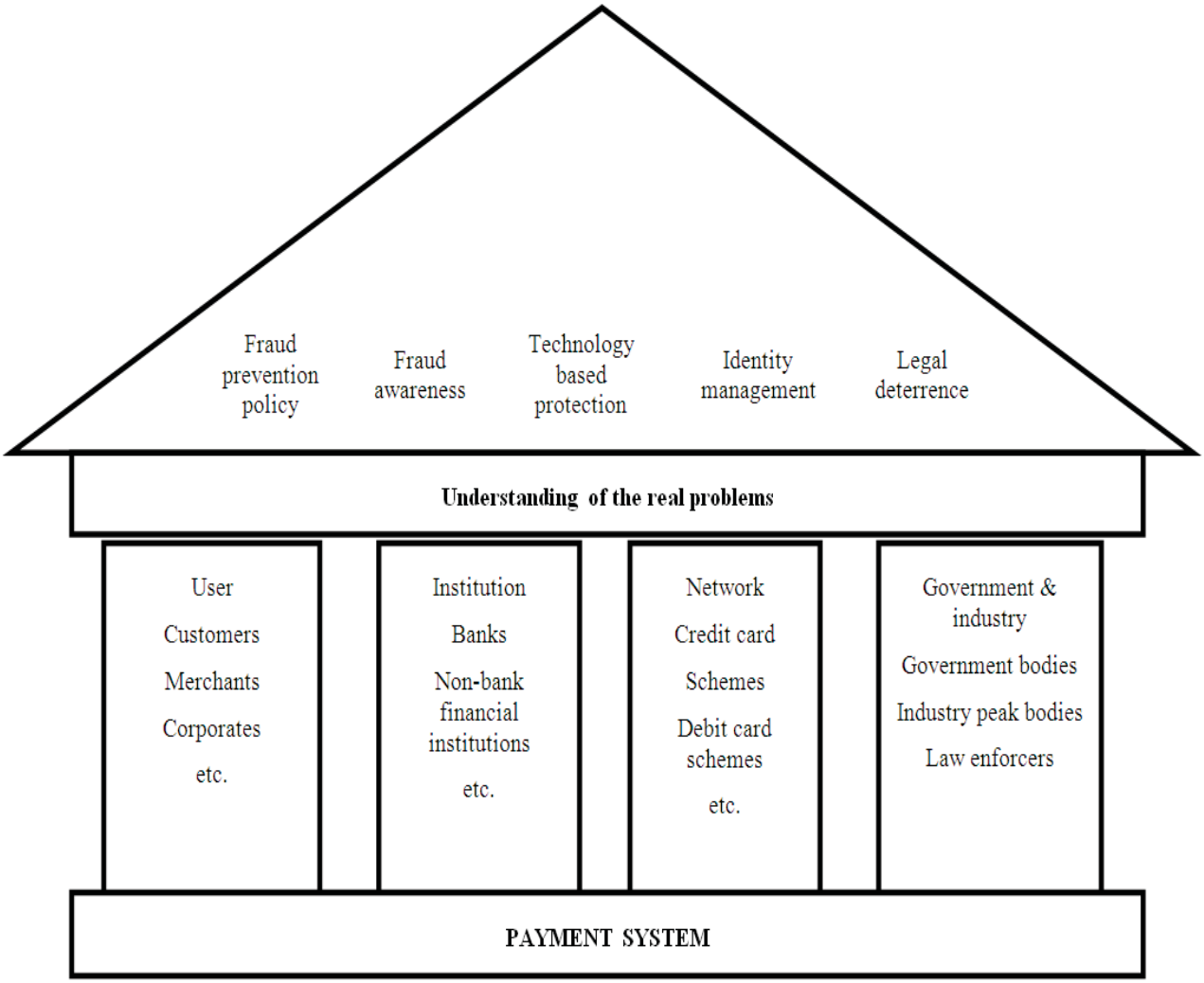
Source: Dzomira (2014) primary survey.

Fig. 1. Cyber fraud incurrence in Zimbabwe banking sector

The study found out that the occurrence of cyber 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 the study (Dzomira, 2014). The occurrence of each fraud type perpetrated in the banking showed that, accounting fraud is at the top with highest frequency indicating that the traditional ways of committing fraud are still being used but of

late electronically (internal computer fraud), followed by money transfer, identity theft, mobile banking and money laundering forming the top six categories. Other types shown include asset misappropriation, financial statement fraud, bribery and corruption which can be perpetrated online or offline platforms. Also being perpetrated are hacking/cracking, phishing, pharming, spy software, computer virus, scams and lastly wiretapping. Similar to the findings mentioned above is empirical evidence from India Risk Survey (Singh et al., 2013), Economist Intelligence Unit Global Fraud Survey (Kroll, 2011/12) and Singleton (2013).

Prabowo (2011) carried out a study on the USA, the UK, Australia and Indonesia and established that a common approach in preventing credit card fraud reduces offenders' opportunities to commit their offences, which often require significant amount of resources and thus sound strategy needs to be properly formulated and executed. Referring primarily to the practices in the USA, the UK, Australia and Indonesia, resources are mainly allocated to six key areas of fraud prevention: understanding of the real problems, fraud prevention policy, fraud awareness, technology-based protection, identity management and legal deterrence as is depicted in the model.



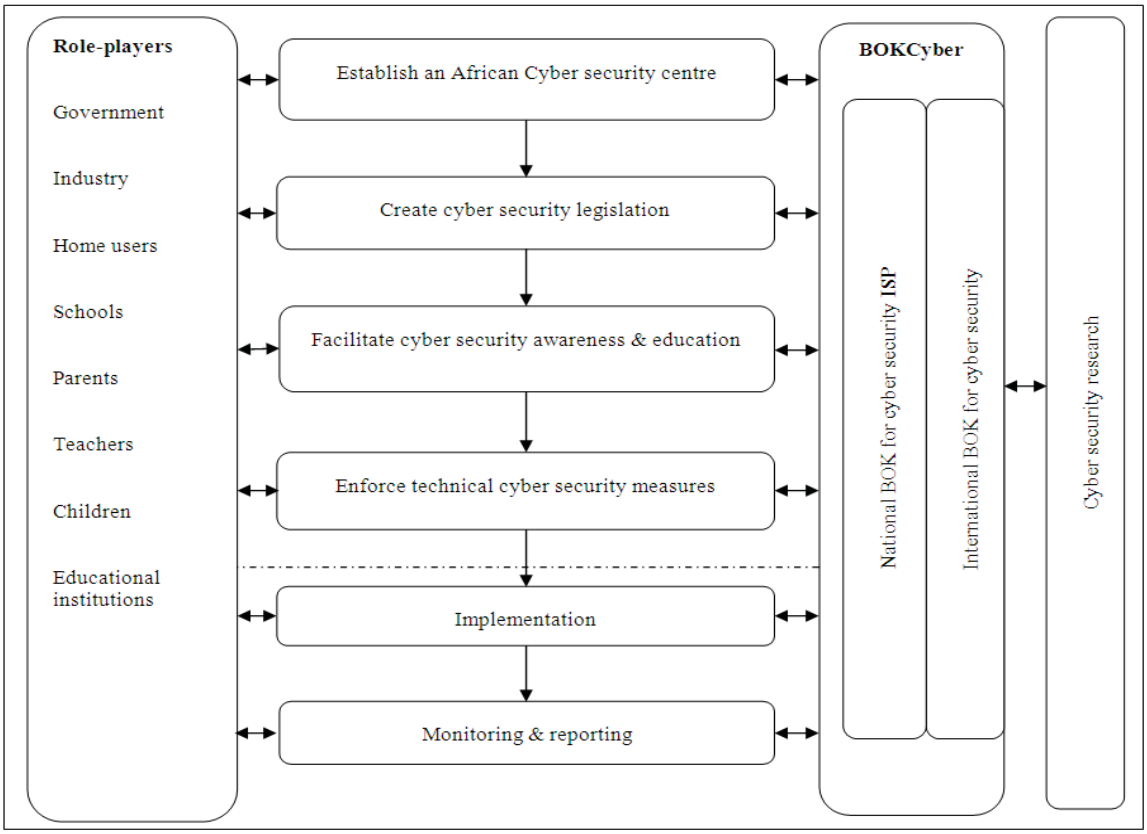
Source: Prabowo (2011).

Fig. 2. The four-pillared house of payments fraud prevention practice

As shown by Figure 2, the structure of the prevention practices is supported by four "pillars", which represent the four groups of key participants in the payments system (users, institutions, networks and government and industry) who work together to promote the safety of the payments industry. However, Probowa (2011) only attended to one form of fraud which can be perpetrated online or offline, it was going to be more effective if it had looked at other fraud types so that it would not be a model targeted on a specific type of fraud since fraudsters use an array of ways to commit the crime.

Moreover, Kritzinger and von Solms (2012) proposed a framework focused on cyber safety concerns in Africa and includes aspects such as policies, procedure, awareness, research and the provision of technical security measures. This paper concludes by combining all relevant solutions

into a proposed cyber security framework to assist Africa in decreasing its cybercrime rate especially among home users with no or limited cyber safety knowledge.



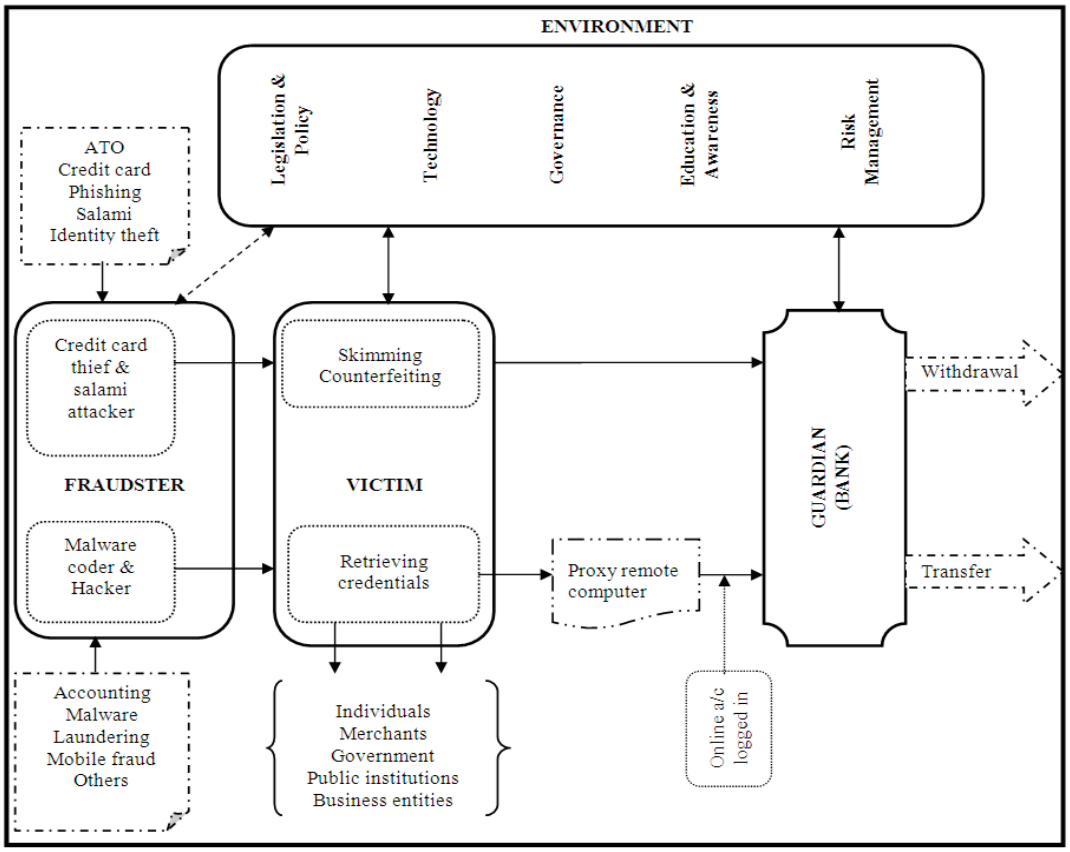
Source: Kritzinger and von Solms (2012).

Fig. 3. Proposed comprehensive framework for cyber safety

The cyber prevention model suggested by Kritzinger and von Solms (2012) comprises four dimensions vital for cyber protection. The dimensions in Figure 3 depict the various cyber tools needed for fighting cybercrime. There are four identified dimensions; role-players; body of knowledge (BOK) for cyber safety; cyber security research; and cyber actions. The first is the role-players which include all people with a role and responsibility to ensure the cyber safety of cyber users. The next dimension is the BOK and it is vital that there is BOK regarding cyber safety that is obtained from international (outside of Africa) sources. The third dimension is that of cyber research which put emphasis on effort from all sectors (academic, industry and government) in doing research to enhance the understanding. Lastly, the fourth dimension that is core to the proposed model is that of cyber action. This includes all actions to be taken by all role-layers involved to design, approve and implement cyber security to enhance the cyber culture. However, having put enough effort on safety strategies on cyber threats, it appears as if the model should have also included the nature and types of the threats so that the strategies can be matched with the practical implications.

2. Methodology

This paper is based on conceptual study and applies ontological tradition (Pooley-Cilliers, 2014) which emphasizes concepts that identify the basic features of the cyber fraud risk management phenomena and aims to explore how the banking community experience the reality. The study unveils a conceptual framework developed through identifying and defining concepts and proposing relationships (Brink et al., 2012) among key participants (fraudsters, victims, guardian and the environment). Proposed model development creates a different way of looking at cyber fraud risk management phenomenon since it shows a logical extension of current knowledge.



Source: Author derived model.

Fig. 4. Proposed framework

Conclusion

Yet the following segment combined the major players and the elements in the electronic and mobile fraud risk management model.

The proposed model above elucidates on how the fraudster perpetrates the crime, the types of e-fraud which are perpetrated and the environment in which all this happens. As cyber fraud has developed from being committed by causal fraudsters to being committed by organized crime and fraud rings that use sophisticated methods to takeover control accounts and commit fraud; the model is therefore comprised of the perpetrator, the fraud types, the victim, the environment and the guardian. It is vital to note that these focus areas are not new-fangled and have been revealed in literature as aforementioned. Nevertheless, what is deficient for developing and emerging economies is that these focus areas are not pooled into one solitary execution action plan clear-cut to developing and emerging economies. Wholly the above-mentioned elements are detached concepts that are not currently allied. The model therefore suggests the bringing together of the participants such that the management of e-fraud is done involving all the relevant factors.

The above model (Figure 4) highlights the concepts crucial to a better approach in e-fraud risk management. The identified concepts include:

- Environment (legislation & policies, technology, education & awareness, governance, & risk management).
- Fraudster (s) (malware coders, hackers, identity thieves, credit card thieves).
- Victim(s) (individuals, merchants, government, business entities, public institutions).
- Guardian (bank).
- Fraud types (account takeover (ATO), credit card, phishing, mobile fraud, salami, malware, laundering, and identity theft).

The environment which affects everybody in the system comprises five focus areas including legislation and policies, technology, education & awareness, governance & risk management. E-business poses distinct encounters to law execution arms as there is often a component of extra-territorial dominion and for the common purpose of apprehending international cyber fraudsters (Harry, 2002), inordinate collaboration and announcement among international law administration agencies is desirable. For instance when money is transferred to a mule account through account takeover legislation differs across one boarder to the other. Unfortunately, many other countries do not have the laws or the

essential skilled law enforcers to deal with computer related or online related crimes and this tends to weaken the exertions to skirmish the mounting risk. Significant challenges for cyber legal jurisprudence has been created as mobile users are considerably increasing and the use of mobile services and generated content. In most developing economies there are no defined authorities fanatical to laws dealing with the use of electronic devices and mobile platforms.

Technology has been of late the centre of attraction to all players in the financial services sector. It is crucial for the participants in the banking sector to be vigilant on the fraudsters who always take advantage of the loopholes and deficiencies in the banking system. Technological advancement is fast-paced, as are the cyber criminals (PWC, 2011), and nonetheless, most entities appear to be out paced by the criminals.

In an endeavor to prevent electronic or cyber fraud, it is customer awareness and education that is most effective. Other stakeholders such as government, businesses, consumer groups, financial guardians in the financial services system must put and increase collaborated determination in the provision of customer education and awareness. Customer education on how to aid avert online banking fraud is just one constituent of a bank's fraud barricade. Moreover, the banking institutions are well cognizant of the adverse bearing of cyber fraud on institutions' reputation, customer loyalty, and shareholder confidence (Joyner, 2011) apart from fraud losses. Risk management affects all the role players since banks, merchants, government and industry, businesses and customers must manage the hazard of being preys to e-fraudsters.

From the proposed e-fraud risk management model, it is quite limpid that management of cyber fraud risk can be effective if the various components are considered in unison and not as standalone elements.

Limitations of the study

This study was primarily limited by nature of methodology which lacked quantitative approach due to scarcity and unavailability of data regarding the area of study (fraud) which is treated as very confidential by most financial institutions. The author resorted to secondary sources what has been done and reported in the field. However, this study could lead to ideas for future research involving surveys and interviewing of participants in the financial sector or banking sector.

Implications of the study

Banks should ensure robust enterprise wide fraud risk management programs which correlate customers' conduct across all communication channels and products to detect "cracked" situations, social grids and cross channel fraud are in place. To scrap the broadest assortment of electronic fraud threats, financial institutions must augment their visibility and consciousness of criminal enterprise and advance their ability to associate events across channels and lines of business and locate patterns in the substantial amounts of operational data composed throughout the business (Big data analytics). To realize better operational awareness, banks should perk up customer visibility across online channels of business, enhancing coordination between channels, applying more meticulous technologies for recognizing and trailing hostile devices and using more urbane link analysis tools that look for connections between ostensibly incongruent actions.

The financial services institutions therefore should prioritize cyber and information security aspects on organization's risk register so as to stand competitive advantage in the current technologically advanced era. More so, financial services institutions should ensure state-of-the-art security and fraud detection and anti-fraud technologies to protect customers' monies.

Electronic and online fraud (cyber fraud) risk management model was suggested to aid financial institutions stakeholders in articulating and fight the hasty upsurge in electronic and online fraud risk. It will be more useful if the involved stakeholders can adopt the model.

References

1. ACI (2013). Fighting online fraud: An industry perspective. Vol. 3, available at: www.aciworldwide.com.
2. Authorize. Net (2006). Fraud Detection Suite. A Cyber source solution. Available at: www.authorize.net.
3. 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.
4. 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.
5. Bhatla, T.P., Prabhu, V. & Dua, A. (2003). *Understanding Credit Card Frauds*. Cards Business Review, #2003–01.
6. BITS (2003). *Fraud Prevention Strategies for Internet Banking*, A Publication of the BITS Fraud Reduction Steering Committee, available at: www.BITSINFO.ORG.
7. Brink H., Walt, C., Rensburg, G. (2012). *Fundamentals of Research Methodology for Healthcare Professionals*, Juta & Company, South Africa.
8. Dzomira, S. (2014). Electronic Fraud (Cyber Fraud) Risk in the Banking Industry, Zimbabwe, *Risk governance & control: financial markets & institutions*, Vol. 4, No. 4, pp. 17-27.

9. EMC (2013). *The Current State of Cybercrime 2013*. An Inside Look at the Changing Threat Landscape. Available at: www.rsa.com.
10. 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, available at: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.
11. KPMG (2012). *Government and Public Sector Cybercrimes*. A Financial Sector View.
12. Kabay, M.E. (2008). *A Brief History of Computer Crime*: An Introduction to students.
13. Joyner, E. (2011). *Enterprise wide Fraud Management. Banking, Financial Services and Insurance.* SAS Global Forum 2011. SAS Institute Inc. Cary, NC, USA.
14. National Fraud Centre (2000). *The Growing Global Threat of Economic & Cyber Crime*. The National Fraud Center, Inc. A member of the Lexis-Nexis Risk Solutions Group in conjunction with the Economic Crime Investigation Institute Utica College.
15. Plooy-Cilliers, F., Davis, C., Bezuidenhout, R. (2014). *Research Matters*, Juta & Company, South Africa.
16. 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.
17. Potter, M. (2000). *Internet Banking and Fraud: making business less risky*, Community Banker 9 No.7 JI 2000.
18. PWC (2011). *Cybercrime: protecting against the growing threat*. Global Economic Crime Survey, available at: www.pwc.com/crimesurvey.
19. Raghavana, A.R., Parthiban, L. (2014). The effect of cybercrime on a Bank's finances, *International Journal of Current Research & Academic Review*, Vol. 2, No. 2, pp. 173-178.
20. Simic, D. (2005). *Reducing Fraud In Electronic Payment Systems*. The 7th Balkan Conference on Operational Research BACOR 05 Constanta, May 2005, Romania.
21. Tan Harry S.K. (2002). E-fraud; current trends and International developments, *Journal of Financial Crime*, Vol. 9, No. 4, pp. 347-354.
22. Tendelkur, R. (2013). *Cyber-crime, securities markets and systematic risk*, Joint Staff Working Paper of the IOSCO Research Department and World Federation of Exchanges.
23. The Institute of Internal Auditors (2009). *Fraud Prevention & Detection in an Automated World*. Global Technology Audit Guide (GTAG) 3.
24. Tan, S.T. (2002). Money laundering and E-commerce, *Journal of Financial Crime*, 9 (3), Banking Information Source, pp. 277-285.
25. 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.
26. Zakaria, S. (2013). The Impact of Identity Theft on Perceived Security and Trusting E-Commerce, *Journal of Internet Banking and Commerce*, Vol. 18, No. 2, pp. 1-12.
27. 41ST Parameter (2013). *The Growing Threats of Cyber Crime*, available at: www.the41st.com.