TOWARDS A CYBER RESILIENT BANKING SYSTEM: EFFECTIVENESS OF CYBER FRAUD RISK MANAGEMENT STRATEGIES ADOPTED BY COMMERCIAL BANKS IN ZIMBABWE

Bronson Mutanda
Manicaland State University of Applied Sciences, Mutare, Zimbabwe
valemutanda@gmail.com
Maireva Chrispen
Manicaland State University of Applied Sciences, Mutare, Zimbabwe
chrispen.maireva@msuas.ac.zw

Abstract
The advent of digital financial technology left the business community and its clients celebrating convenient ways of online shopping, paying bills and money transfers. However, digital banking technology came with its share of challenges, due to highly digitalised economies in the context of the Fourth Industrial Revolution, cyber fraudsters are increasingly targeting and leveraging on financial market infrastructures. Cyber security of banking institutions and the financial systems across the globe remains a major concern of Central Banks, investors, internal auditors and financial risk managers. The purpose of this research paper was to examine the efficacy of cyber fraud prevention measures used by commercial banks in Zimbabwe. The study also looked into the difficulties encountered in managing cyber-fraud. Results indicate that cyber fraud risk management strategies adopted by Commercial banks are partly effective which indicates existence of opportunities for cyber fraudsters to attacks and get away with it at the expense of clients, banks and the financial system as a whole. Results also indicate that Commercial banks are facing quite a number of challenges which include the following: lack of sophisticated systems, cyber attackers are always ahead, some of the clients do not take awareness messages send to them seriously, some clients share passwords and credit cards and lack of enough education and knowhow of employees. The study therefore concludes that, cyber fraud risk management strategies adopted by Commercial banks are partly effective. Monetary and fiscal authorities need to continue monitoring Commercial banks with regard to implementation of cyber security risk based supervision framework.

Keywords
Cyber fraud; commercial banks; management strategies; resilience; risk

JEL Classification
G2

1. Introduction
Cyber fraud has emerged as a major issue in developing countries' financial systems and poses a danger to the global movement toward more inclusive financial sectors (Usman and Shah 2013; Baur-Yazbeck et al 2019). Zimbabwe, a member of the global village, has over time adapted and moderately converted to a largely digital economy, primarily in the financial and retail sectors (Reserve Bank of Zimbabwe 2021). This is unquestionably backed by the Reserve Bank's policy on employing digital financial services, and its success is attributable to teamwork, commitment, prudent risk management, and market innovation that continue to fuel the transformation in the digital financial system (Reserve Bank of Zimbabwe 2021).
Zimbabwe's 2020 National Risk Assessment (NRA) report, among other risks, notes the risk of cyber fraud, particularly through digital financial channels, contributes about US$900 million annually in illicit proceeds of crime. Zakrzewski et al (2019) find that

financial services companies are 300 times more likely to be targeted than others. This shows that successful criminal cyber fraud against financial sector firms can be particularly beneficial for cyber fraudsters. Accounts, customer information, related transactions, and backup systems are digitized, and by doing so, cyber fraudsters take advantage (Brenner, 2017). Cyber fraudsters using sophisticated systems employ more aggressive pressure tactics and target more vulnerable targets, affecting utilities, financial services firms, retail stores, health care systems and data-rich companies (Department of General Australian Government Attorney General's Office, 2013; Broadhurst, 2006; Clough, 2015; Webster & Drew, 2017; The Global Risks Report 2022). According to Shinder (2002), e-commerce, Internet banking and related technologies have network connections and as banks expand the range of online services for customers, the risk of Internet Computer Fraud (ICF) increases. High-profile financially motivated frauds have been observed around the world with the growing patronage of digital banking services and their expected dominance in the near future (Dzomira 2014; Baur-Yazbeck 2020).

Commercial banks in Zimbabwe are adjusting to technological advancements around the world, but cyber fraudsters are also on the lookout (Reserve Bank of Zimbabwe 2021, Mugari, Gono, Maunga and Chiyambira 2016). Thus, the financial services ecosystem's requirement for cyber resilience and endpoint security cannot be overstated (Reserve Bank of Zimbabwe 2021; Carstens 2019; Coeure 2019). Due to Zimbabwe's current liquidity crisis, more people are utilizing services like payment cards and the Real Time Gross Settlement System (RTGS) (Mugari, 2016). Due to these new payment methods, financial institutions are now more vulnerable to dangers like e-card fraud and fraudulent RTGS transfers (Mugari, 2016).

Significantly, authorities and other stakeholders are becoming increasingly concerned about the sophistication, cyber fraud frequency and cyber fraud as they pose a threat to undo the progress made thus far (Reserve Bank of Zimbabwe 2021). Following these developments, the Reserve Bank of Zimbabwe encouraged the adoption of cyber risk management methods in the banking industry. To lessen the danger of cyber fraud and all types of cyber-attacks, the Reserve Bank of Zimbabwe has suggested a variety of procedures under risk-based cyber risk management (Reserve Bank of Zimbabwe 2021). This study sought to determine the efficacy of commercial banks' strategies for reducing their exposure to cyber fraud risk as well as the difficulties they encounter in doing so.

2. Literature Review

2.1. Types of Cyber Fraud

2.1.1. Phishing

Roger (2008) defines phishing as attacks on the accounts of individuals or organizations in order to obtain private information to be used for fraudulent purposes. Europol (2014) described it as fraud against businesses and financial institutions by stealing customer identification data. Phishing is also called identity fraud (United Nations Office on Drugs and Crime, 2010). Sarannia & Padma (2014) defined identity theft as the theft of private and confidential information for fraudulent use without acknowledgment of the owner. They went further and identified three types of phishing, namely spear, cloning and whaling (Saranni and Padma, 2014; Dubey and Manna, 2014, Chandhary, 2014). In line with the above, KPMG (2012) highlighted that phishing is the most common type of identity theft. Boateng and Amanor (2014) identified vishing and smishing as types of phishing.

2.1.2. Hacking

Padgett (2007) cited in Hedayati (2012) defined hacking as the illegal access to systems or databases to obtain personal or organizational private and confidential information. The availability of personal information online has made it easier for criminals to steal from businesses and individuals (Magutu et al, 2011). Bawane and Stelke (2014) listed hacking techniques such as denial of service, spoofing, sniffing, viruses and worms, key-loggers, social engineering, and fake messages.

2.1.3. Card fraud

Identity theft and credit/debit card fraud are two types of cyber fraud that are frequently used interchangeably. This entails pretending to be someone else and stealing their identity, their name, Social Security number (SIN), credit card number, or other identifying details, in order to engage in criminal activity. It involves the unauthorized collection of credit and debit card magnetic stripes and PINs (Dubey et al 2015). Card fraud can happen at any bank ATM or via a compromised EFTPOS device (Dubey et al 2015). The card information and PIN will be encoded into a phony card by online scammers, who then use the card to make fraudulent withdrawals and purchases.

2.1.4. Advance fee scams

These cyber scams are usually done through a letter, email or phone call offering a large sum of money if you can help someone transfer millions of dollars or other currency out of their country. To initiate the transaction, you are asked to send your bank account details and an administration fee. These bank details are then used fraudulently by cyber fraudsters.

2.1.5. Salami attacks:

The key is to keep the alterations subtle enough that they are overlooked in some cases (Kante 2017). For instance, a bank employee could install a program on the bank's servers that automatically deducts a tiny sum of money from each customer's account (let's say US$0.5 every month) (Kante 2017). This illicit debit will likely go unnoticed by the account user, but the bank employee will be paid significantly more each month as a result (Kante 2017).

2.2. Cyber Fraud Risk Management

Cyber fraud risk identification, cyber fraud risk assessment, cyber fraud risk measurement, cyber fraud risk mitigation/risk management, and cyber fraud risk understanding are all essential components of managing cyber fraud risk, just like managing any other financial risk. The risk management approach for cyber fraud is depicted in Figure 1 below. By removing threats, managing effects and lowering vulnerabilities, effective cyber fraud risk management lowers the likelihood of severe negative effects on a company (Reserve Bank of Zimbabwe 2021). Risk management for cyber fraud must be continual and proactive, requiring control over both the technology itself and the people and systems that use and support it (Reserve Bank of Zimbabwe 2021). Due to the constantly shifting risk environment, the procedure must be dynamic (Reserve Bank of Zimbabwe, 2021).

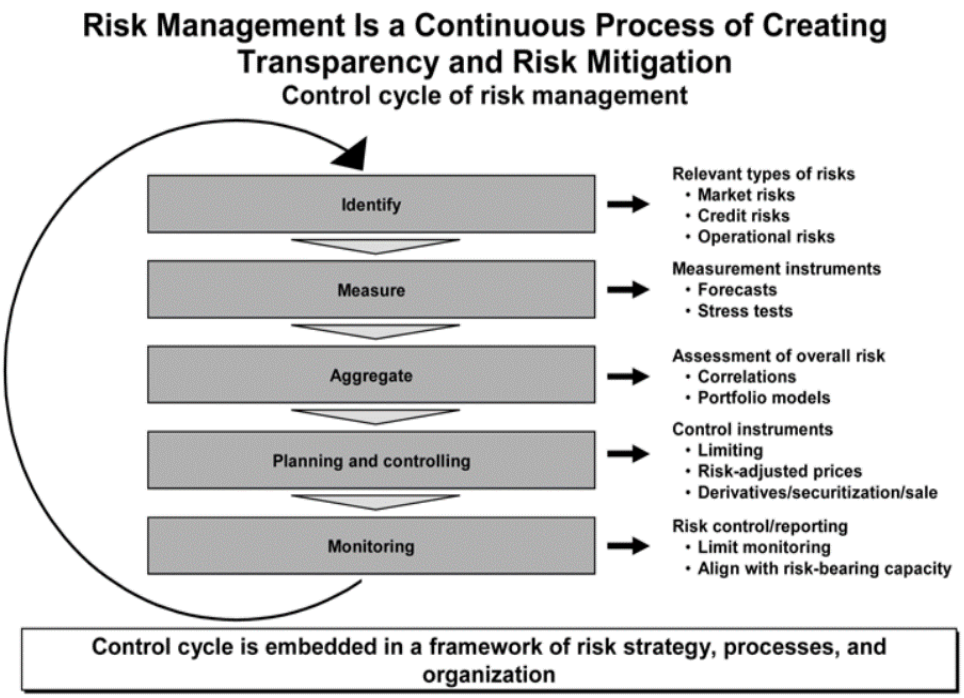

Fig 1. Financial Risk Management Process

Source: Oesterreichische National bank (OeNB) in cooperation with the Financial Market Authority (FMA) (December 2004)

2.2.1. Cyber Fraud Risk Identification

The proper assessment of cyber fraud risk centres on identifying and comprehending current hazards as well as potential new business venture threats (Reserve Bank of Zimbabwe 2006, Reserve Bank of Zimbabwe 2021). Cyber fraud risk assessment should be ongoing and take place at both the micro (transaction) and macro (whole portfolio) levels (Reserve Bank of Zimbabwe 2006, Reserve Bank of Zimbabwe 2021).

2.2.2. Cyber Fraud Risk Assessment

To thoroughly assess the efficacy of cyber fraud risk management measures, it may be helpful to walk through the relevant procedure or activity and assess how well the controls are currently performing. The organization must evaluate itself while assessing the risk of cybercrime (Reserve Bank of Zimbabwe 2006, Reserve Bank of Zimbabwe 2021). Self-evaluation can take the form of a qualitative risk assessment utilizing internal data and expert judgment, and, to a lesser extent, quantitative models (European Insurance and Occupational Pensions Authority 2019).

2.2.3. Cyber Fraud Risk Measurement

The capacity to measure cyber fraud threats is necessary for effective risk management. A banking organization must accurately and promptly measure its risks in relation to the possibility of negative consequences on its earnings, capital, and corporate goals (Reserve Bank of Zimbabwe 2006, Reserve Bank of Zimbabwe 2021). The institution's and the level of risk's complexity should be reflected in the complexity of the risk measuring tools (Reserve Bank of Zimbabwe 2006, Reserve Bank of Zimbabwe 2021).

2.2.4. Cyber Fraud Risk Treatment

The risk management procedure for cyber fraud starts when the risk assessment is finished. Using policies, standards, and processes that outline roles and authorities, a banking organization must set and convey control limitations (Reserve Bank of Zimbabwe 2006, Reserve Bank of Zimbabwe 2021). Whether residual risk is at an acceptable level or whether treatment is necessary depends on an organization's risk assessment and risk appetite (Reserve Bank of Zimbabwe 2006, Reserve Bank of Zimbabwe 2021). Treatment options for the risk may include enhancing current controls, putting in place new controls, or stopping the activity, program, or service altogether.

2.3. The Fraud Triangle Theory

In 1953, Cressey decided to pursue a doctorate in criminology and focused his thesis on organizational funds embezzlement. Cressey interviewed 200 people to understand more about embezzlement, which sparked the creation of this concept.
"Trusted people become trust breakers when they believe they have a financial issue that cannot be resolved openly, realize that this issue can be secretly resolved by breaching a position of financial trust, and can apply to their behavior in this situation a verbalization that allows them to adjust their representations of themselves as trustees with their representations of themselves as users of trust funds or property," was the formulation of the theory (Cressey, 1973). The hypothesis he created throughout his study was more widely known as the fraud triangle. One leg of the triangle represents motivation, the second leg represents opportunity, and the last leg represents rationalization (Mohottige, Sujeewa, Shukri, Yajid, Khatibi, Azam and Dharmaratne 2018).

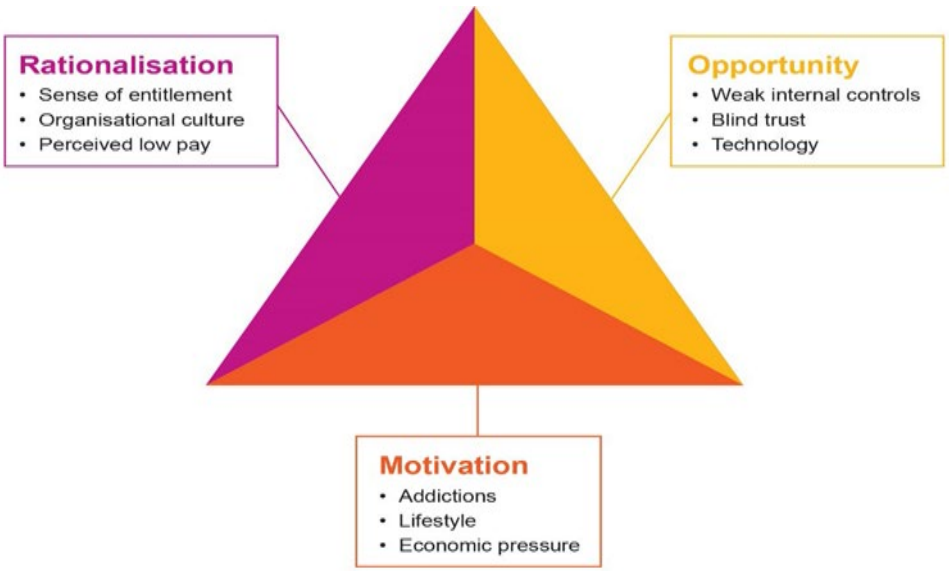

Fig 2. Fraud Triangle Model

Source: OAG adapted from Other People's Money (2009)

The most commonly used model to understand the causes of fraud is through the application of the fraud triangle. The fraud triangle explains that fraud is driven by three forces: motivation, rationalization, and opportunity.

2.3.1. Motivation

In simple terms, motivation is usually based on greed or need. Many people face the opportunity to commit fraud, and only a minority of the greedy and needy do (Mohottige et al 2018). Personality and temperament, including how fearful people are of the consequences of risk, play a role (Abdullahi, Mansor and Nuhu 2015). Some people with good objective principles may fall into bad company and develop a taste for the fast life, which tempts them to commit fraud (Abdullahi, Mansor and Nuhu 2015).

2.3.2. Opportunity

In terms of opportunities, fraud is most prevalent in companies with weak internal control systems, poor security of company assets, little fear of exposure and likelihood of detection, or unclear policies regarding acceptable behavior (Mohottige et al 2018). Research has shown that some employees are completely honest, some are completely dishonest, but many are driven by opportunity (Dharmaratne et al 2018).

2.3.3. Rationalisation

The third and final factor in the fraud triangle is rationalization. Cressey noted that rationalization is not an ex post facto means of justifying a theft that has already occurred. It should be noted that rationalization is a necessary component of a crime prior to its commission; in fact, it is part of the motivation for the crime (Dharmaratne et al 2018; Mohottige et al 2018). Since the treasure thief does not consider himself a criminal, he must justify his wrongdoings before committing them. Rationalization is necessary so that the offender can make sense of his wrongful behavior and maintain his self-image as a trustworthy person (Mohottige et al 2018).

2.4. Empirical Review of Literature

Aldasoro et al(2020b)'s study uses Advisen's unique dataset of more than 100,000 cyber incidents to explore the drivers of cyber costs across sectors. The cost of cyber incidents is generally greater for larger firms, but this effect is smaller for the financial sector (the first two columns in the fourth panel show the relationship between cyber cost and firm size) (Aldasoro et al. 2020b). Cyber incidents can be interconnected, that is, one incident can affect several organizations at the same time (Aldasoro et 2020b). The higher this connection, the higher the cost, especially for financial firms (third and fourth columns in the fourth panel (Aldasoro et al. 2020b). According to some estimates by Bouveret (2018), based on data collected from media and newspaper articles in the period 2009 -17 years in Singapore, the cost of risk for the entire banking sector, including the contagion effect, could be 14-19% of the banks' total net profit.

In a study conducted by Raghavan & Parthiban (2014) to examine how cyber fraud affects an organization's finances, they discovered that there are many different types of electronic fraud in the banking industry, including ATM fraud, cyber money laundering, credit card fraud and that the main objective of all scams is to gain access to a user's bank account. According to Dzomira (2014), there are two types of e-fraud: direct fraud (such as money laundering, salami technology, and employee embezzlement) and indirect fraud (eg malware, phishing, identity theft, etc.). In a study on the development of credit card fraud defenses in the USA, UK, Australia, and Indonesia, Prabowo (2011) discovered that a frequent method to credit card fraud prevention reduces the opportunities for offenders to commit their crimes, which are often resource-intensive and thus therefore, a smart strategy must be properly formulated and executed. Previous studies have failed to investigate the effectiveness of cyber fraud risk management strategies, something this study sets out to address.

3. Methodology

3.1. Sample

A random sample of 50 Officers and Managers from the IT department, Operations department, Risk management department and Senior Managers were chosen for responding to questionnaires while 5 officers from across the departments were considered for interviews.

3.2. Instruments

The tools for collecting data from the respondents were questionnaires and interviews. The questionnaire was developed on the basis of data from bank managers and tested before being used for the survey. The questionnaire was divided into two subsections to make it easier for participants to answer. The first section focused on the demographic information of the respondents, including; age, gender, years of experience in banking and the position they held in their organizations. The second section aimed to obtain information on the effectiveness of cyber fraud risk management strategies in a banking organization as well as the challenges faced. To verify the reliability of the questionnaires, a pilot study was conducted.

3.3. Data Collection and Analysis

This study used a combination of qualitative and quantitative research design. Data collection was done through a survey during which the researcher distributed questionnaires to the bank reception for further submission to the relevant departments. The researcher also selected 5 employees from IT department, risk management department, operations department and audit department of 5 commercial banks for interview. Data analysis was performed using SPSS version 23, descriptive and inferential statistics were used.

4. Results

From table 4.1 below, 33 respondents were males while 15 were females. Although 50 questionnaires were given out, only 48 bank employees responded which implies a 96% response rate.

Table 4.1. Cross Tabulation of Gender and Experience

		Experience					Total
		0-5 years	6-10 years	11-15 years	16-20 years	More than 20 years	
Gender	Male	6	7	9	6	5	33
	Female	1	7	4	3	0	15
Total		7	14	13	9	5	48

Table 4.1 above shows that 6 male respondents had 0-5 years of work experience, 7 men had 6-10 years of work experience, 9 men had 11-15 years of work experience, 6 men had 16 to 20 years of work experience and 5 men with more than 20 years of experience. In addition, Table 4.1 shows that one female respondent had experience of 0-5 years, 7 - 6-10 years, 4 women - 11-15 years, and 3 - 16-20 years. years. More men (33) were interviewed than women (15).

4.1. Frequently Reported Cyber Frauds

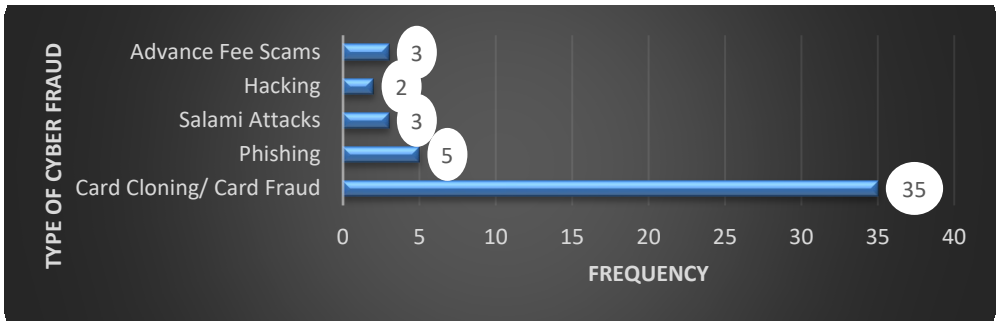

Fig. 3: Types of Cyber Fraud Risks Reported in Commercial Banks in Zimbabwe

From the bar graph above, 72.9% (35) of the respondents indicated that card cloning/ card fraud is the most frequently reported cyber fraud risk in Commercial banks of Zimbabwe, 10.4% (5) of the respondents cited phishing as the most frequently experienced cyber fraud, 6.3% (3) cited salami attack as the most frequently reported cyber fraud risk while 4.2% (2) and 6.3% (3) cited hacking and advance fee scams as most frequently reported cyber fraud risks respectively. From the interviews carried out, respondent 2 said:

"Despite several attempts by the bank to warn customers, card cloning cases are on the rise, and victims are being unknowingly plundered of their hard-earned money. Several victims of these online fraudsters misplaced their credit cards or gave up their card information in retail establishments. It is unfortunate to learn that some online scammers record video of transactions made by customers at POS terminals. Cybercriminals will later utilize these films to conduct unauthorized transactions.".

The above response unveils tricks and strategies being employed by cyber fraudsters to steal from Commercial bank clients. Having identified these strategies, Commercial banks need to continue encouraging their clients never to expose card numbers and secret codes even during the process of transacting in retail shops.

4.2. Cyber Fraud Prevention Strategies

All respondents indicated that Commercial banks have crafted cyber fraud prevention strategies which include inter-alia the following: Intrusion Detection and Prevention Systems, thorough vetting of new employees, keeping software and devices up to date, antivirus and antimalware protection software, use of different and unique passwords for all accounts, setting up of a whistle-blower hotline, training and education of employees on preventing and controlling risk, use of multi-factor authentication technology, alerting clients about cyber fraud through SMS, firewalls and role-based

access of bank systems. All respondents cited that these are some of the strategies put in place by Commercial banks to prevent cyber fraud within Commercial banks.

4.3. Management of Cyber Fraud Risk in the Organisation

Fig 4 below indicate perception of respondents concerning management of cyber fraud risks in the organisation. These responses come after a question was included in the questionnaire in-order to investigate perception of the workforce concerning cyber fraud risk management. The way risks are managed within an organisation determines whether an organisation will win or not. Cyber resilience requires all hands on the deck, it demands a holistic approach to risk management.

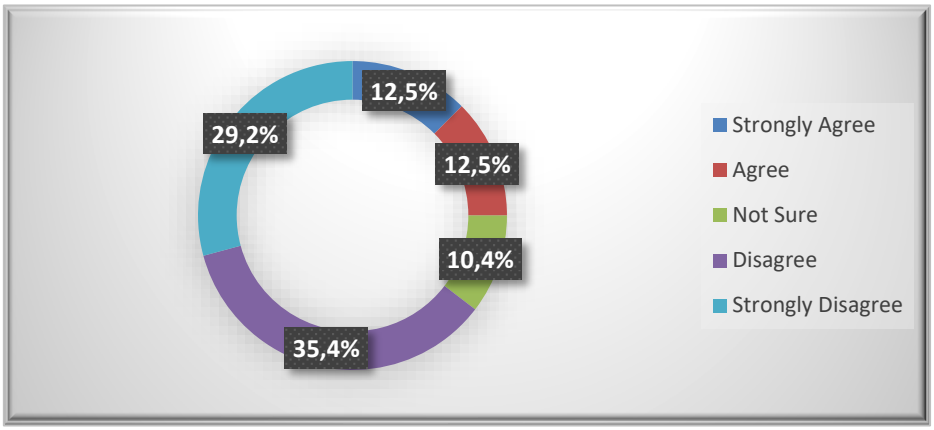

Fig. 4: Perception of Respondents Concerning Management of Cyber Fraud Risk

The Chart above represents perception of respondents concerning cyber fraud risk management in the bank. 35.4% of the respondents indicated that they disagree to the holistic approach of cyber fraud risk management, 29.2% of the respondents indicated that they strongly agree to the holistic approach of cyber risk management, 12.5% of the respondent strongly agree that cyber fraud risk management is the duty of everyone within the organisation, 10.4% are not sure and 12.4% agree that cyber risk management is the duty of everyone in the organisation. From the interviews carried out, respondent 5 said:

"The risk management division and the IT division are solely responsible for controlling cyber fraud threats, rather than assigning this obligation to every employee in the bank. They must implement procedures robust enough to safeguard customers and the bank as a whole.".

This perception by some respondents is a clear testimony that in some organisations, cyber fraud risk management is being left out to the IT and risk management department. There is need for such organisations to adopt a holistic approach whereby everyone in the bank is involved in the fight against cyber fraud risks.

Table 4.2 Responses Showing the Effectiveness of Cyber Fraud Prevention Strategies

	Frequency	Percent	Valid Percent	Cumulative Percent

Valid	Very Effective	6	12.5	12.5	12.5
	Partly Effective	40	83.3	83.3	95.8
	Neutral	2	4.2	4.2	100.0
	Ineffective	0	0	0	
	Very Ineffective	0	0	0	
	Total	48	100.0	100.0	

The effectiveness of commercial banks' cyber fraud prevention techniques was investigated using a 5-point Likert scale. According to Table 4.2, 12.5% of respondents said the adopted cyber fraud prevention techniques are effective, 83.3% said the strategies are only somewhat effective, and 4.2% said they had no opinion on the topic. Respondent 1 stated:

"*Because of the complexity of the systems utilized by fraudsters, it is very difficult to be certain of the efficiency of cyber fraud control techniques. They constantly innovate new ways to hack our systems and are one step ahead of us. What we can only conclude is that our strategies are only partially successful.".*

Information from respondents reveal that strategies adopted by Commercial banks in order to mitigate against cyber fraud incidences are not hundred percent effective. Cyber fraudsters always invent ways of attacking and getting away with it.

Table 4.3 Influence of Gender, Experience and Level of Education on Rating of Cyber Fraud Risk Management Strategies

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
	(Constant)	2.722	.222		12.283	.000
	Experience	-.052	.043	-.155	-1.193	.002
	Gender	-.327	.116	-.379	-2.826	.125
	Highest Level of Education	-.134	.070	-.253	-1.899	.004

A test was carried out in order to determine if education level, gender and level of education have an effect on the way employees rate cyber fraud risk management strategies. Findings in table 4.3 show that employees' opinions of cyber fraud management strategies are not significantly influenced by their gender. Gender beta was discovered to be ß = -0.379, t (48) = -2.826, and p=0.125> 0.05. In this regard, it is evident that gender has no bearing on how risk management solutions for cyber fraud are rated. Further analysis reveals that education ß=-0.134, t (48) = -1.899, p=0.0040.05, experience ß=-0.155, t (48) = -1.193, and experience ß=-0.134, respectively. This suggests that the workforce's perceptions of the efficacy of cyber fraud risk management techniques are highly influenced by their level of education and work experience. In order to check the significance of the model, ANOVA parameters were used and the information is shown in the table 4.4 below.

Table 4.4 ANOVA Table Showing the Significance of the Regression Model

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
	Regression	2.048	3	.683	5.346	.003[b]
	Residual	5.619	44	.128		
	Total	7.667	47			
a. Dependent Variable: How do you rate cyber fraud risk mitigation strategies in your organisation?						
b. Predictors: (Constant), Highest Level of Education, Experience, Gender						

F (3; 48) = 5.346, p=0.003–0.05, which shows that the regression model is significant. To put it another way, the regression model effectively explains how the workforce perceives the usefulness of cyber fraud risk management measures. Findings reveal that evaluation of the efficacy of cyber fraud risk management is influenced by the worker's level of education and experience. These findings show that one's degree of education and experience have a significant impact on how people perceive the value and capability of cyber fraud risk management measures.

Table 4.5 Responses Showing the Effectiveness of Cyber Fraud Detection Systems

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Effective	3	6.1	6.3	6.3
	Partly Effective	37	75.5	77.1	83.3
	Neutral	7	14.3	14.6	97.9
	Ineffective	1	2.0	2.1	100.0
	Total	48	98.0	100.0	
Total		49	100.0		

Answers to the questions of whether commercial banks have cyber fraud detection systems and how successful these systems are shown in Table 4.5. above. According to 6.1% of respondents cyber fraud detection systems are effective, 75.5% of respondents said they are partially effective, 14.3% of respondents said they were neutral, and 2% said they are ineffective. Based on the interviews, respondent 3 stated:

"Of course we have systems in place to deal with cyber fraud but systems meant to detect cyber frauds are limited. Investments are being made towards installation of more advanced computer systems meant to ring fence our servers. However, cyber fraudsters are not novice in as far as computer systems is concerned, they will always find ways of circumventing our detection systems".

It is clear from the above statement that commercial banks still struggle with cyber fraud despite having detection systems. Cybercriminals spend more money on highly

developed and advanced systems that can get beyond software that can detect them. Additionally, data show that commercial banks' detection systems are constrained and unable to catch every effort made by cybercriminals.

Table 4.6 Challenges Faced by Commercial banks in Fighting Cyber Fraud

Challenges		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Lack of Sophisticated Systems	7	14.6	14.6	14.6
	Cyber Fraudsters are Always Ahead	21	43.8	43.8	58.3
	Some clients do not take SMS send to them seriously	7	14.6	14.6	72.9
	Clients are always sharing passwords and cards	6	12.5	12.5	85.4
	Some cyber fraudsters are former employees	3	6.3	6.3	91.7
	Lack of enough education and knowhow of employees	4	8.3	8.3	100.0
	Total	48	100.0	100.0	

Table 4.6 above represents challenges faced by Commercial banks in their quest to manage and mitigate cyber fraud risks. From the information on the table, 43.8% of the respondents indicated that the greatest challenge is the level of swiftness with which cyber fraudsters are advancing in technology. Other challenges include, lack of sophisticated systems and software to ring fence Commercial bank systems, 14.6% of the respondents cited that they lack sophisticated systems to deal with cyber fraudsters, on the same note, respondents cited that clients are not taking warning messages sent to them seriously and by so doing, they expose themselves to cyber fraudsters. The other challenge cited by 6.3% of respondents is that clients share passwords and by so doing give room to cyber-attacks. 8.3% of the respondents indicated that there is information deficiency on its manpower which can only be closed by training and development. 6.3% of the respondents cited that, cyber fraudsters are former employees who take advantage of their knowledge of bank systems to attack and get away with organisational money.

5. Discussion of Research Findings

The study carried out revealed almost three important themes which are: cyber fraud risk management strategies adopted by commercial banks are partly effective, the

greatest challenge faced by Commercial banks in their quest to manage cyber fraud is the pace at which cyber fraudsters are moving. The last observation from the study is that card cloning is the greatest form of cyber fraud experienced by Commercial banks in Zimbabwe.

5.1. Commonly Reported Cyber Fraud

Although commercial banks are subject to other types of cyber fraud, statistics indicate that card cloning/card fraud is the most frequently reported. Commercial banks must create measures to improve the security of credit/debit cards in light of this knowledge. Without investment in credit/debit card securitization, cyber resilience will only ever be a pipe dream. If businesses want to safeguard their customers from online fraud, they must make significant investments in credit card security. Also, banks must constantly inform their customers on the tactics employed by cyber fraudsters. Commercial banks should use walk-in customers as an opportunity to inform them about cyberattacks and how to defend against them. Some customers unknowingly reveal their card details and secret codes to cyber fraudsters increasing chances of attacks.

5.2. Effectiveness of Cyber Fraud Risk Management Strategies

The study's findings show that cyber fraud risk management strategies adopted by commercial banks are effective in part because of how sophisticated fraudsters are. Given this information, commercial banks need to create a research and development department dedicated to obtaining the latest developments in the protection of banking systems. This opinion is in line with the recommendations of Duby and Manna (2014) who state that all banks should have a dedicated anti-fraud department, its role is to monitor, investigate, report and raise awareness. Research and development should invest in obtaining the latest information on how cybercriminals attack systems so that mitigation strategies can be developed. Commercial banks are also encouraged to invest in the latest technologies and systems in tandem with the development of the world and which are also ready to repel the attacks of cyber-attacks.

Findings also point to the need for banks to invest more in training and developing workforce so that everyone in the organization is aware of the need to combat cyber fraud. This is in line with Dubi and Manna (2014) who state that banks should inform and train employees about different types of fraud and how to detect them. Mwabu's (2013) research in Kenya revealed that another factor that affects e-fraud in the banking sector is the customer's level of e-fraud awareness. Research findings show that cyber fraud in the banking industry thrives on customer ignorance, so fraudsters steal using card cloning, phishing (fake emails and/or fake websites), identity theft, password or PIN disclosure, trojan horses (embedded computer virus). In line with this, Adeyemi (2010) observed that criminals obtain customer account credentials, that is login name and password, using various schemes. A "look over the shoulder" scheme occurs when a customer carries out financial transactions while under the supervision of a criminal (Mwabu 2013). A large number of cases have been reported where criminals obtained access data to customer accounts simply by observing customers at a public Internet access point (Mwabu 2013). Cyber fraud risk management cannot be left to the risk management department. If commercial banks are to be resilient to cyber challenges, a holistic approach is needed.

5.3. Challenges Faced in the Fight against Cyber Fraud Risks

The development and complexity of cybercriminals was named as the biggest difficulty in the fight against cybercriminals by a lot of respondents. To increase their effectiveness and reach, cybercriminals work together in organized or loosely connected cybercrime syndicates, using sophisticated software tools, social

engineering, and psychological approaches (Broadhurst, 2006; Ionescu et al., 2011). Commercial banks should increase their investments in modernizing and updating their systems in light of this. Systems that are not modernized and upgraded will develop flaws that cybercriminals can exploit. To protect depositors' money from online scammers, highly advanced technology must be purchased. If banks are to be cyber-resilient, they must invest in multi-factor authentication technologies, intrusion detection and prevention systems, antivirus, and antimalware security software. According to Dubey and Manna (2014), banks should work to increase customer and staff knowledge of fraud. The foundation of fraud management is having an understanding of how to avoid and detect scams. Banks must implement a variety of strategies to raise customer and employee knowledge (Dubey and Manna 2014). Also, it is crucial for commercial banks to think about educating their customers so that they won't be caught off guard.

To prevent customers from disclosing their card information and secret codes to others, commercial banks may want to consider handing out booklets to all walk-in customers. Dzomira (2015) also mentioned the necessity of awareness campaigns in order to build cyber resilience. The most effective strategy for preventing electronic or cyber fraud is customer awareness and education (Dzomira 2015). Various parties involved in the financial services sector, including the government, corporations, consumer advocacy groups, and financial guardians, must improve their commitment to working together to provide client education and awareness (Dzomira 2015). Education is needed to inform clients of these advances because card cloning has been identified as the most often reported cyber fraud risk. The bank systems must be set up to automatically log out any employees who leave the company, and role-based log in procedures must be implemented. To improve cyber resilience, the banking sector must make significant investments.

Conclusion

Findings of the study reveal the following three things: cyber fraud risk management strategies by Commercial banks are not very effective but partly effective. The research also concludes that the greatest challenge faced by Commercial banks in their endeavour to fight against cyber fraud is the rate at which cyber fraudsters are innovating strategies and tactics to attack. Lastly, the study concludes that card cloning is the most frequently reported cyber fraud risk. Given these conclusions, the researcher encourages Commercial bank managers and the regulatory authorities to invest more in sophisticated and modern systems and technology so as to enhance cyber resilience. The researcher encourages bank managers to consider cyber fraud risk management as the responsibility of everyone in the organisation rather than leaving it to the IT and risk management department. Training and development of the workforce need to be prioritised, Commercial banks need to allow their workforce to go for forensic examination courses.

References

Abdullahi R.M.N and Nuhu S.M. (2015). Fraud Triangle Theory and fraud Diamond Theory: Understanding the Convergent and Divergent for Future Research. European Journal of Business and Management. Vol 7(8)

ACI (2013). Fighting online fraud: An industry perspective. Vol. 3 pp 34

Adeyemi, A. (2010). Winning customers' confidence: The new banking focus. The Guardian, May 26: 2

Aldasoro I.F.J., Gambacorta L., and D.W (2020). "Covid-19 and cyber risk in the financial sector", BIS Bulletin, forthcoming. pp24-35

Australian Government Attorney-General's Department. (2013). National plan to combat cybercrime

Brenner J. (2017). "Keeping America safe: toward more secure networks for critical sectors", MIT Centre for International Studies and MIT Internet Policy Research Initiative.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. Policing: An International Journal of Police Strategies and Management, 29(2), pp408- 433.

Carstens A. (2019). "A handful of cyber – five key issues for international cooperation", speech, 10 May.

Clough, J. (2015). Principles of cybercrime (2nd ed.). Cambridge: Cambridge University Press.

Coeure, B. (2019). "Cyber resilience as a global public good", speech, 10 May 2019.

Credit Card Fraud: Awareness and prevention, Journal of Financial Crime*,* 15 (4), pp 398-410.

Cressey, D.R. (1973). Other Peoples' Money: A study in the social psychology of embezzlement. Glencoe: Free Press

Domingues V. (2018). Finance and Cyber-security Risk Management. Research Dissertation

Dubey. D. R and Manna. A. (2014). E-banking Frauds and Fraud Risk Management. *Tactful Management Research Journal.* Vol 1(2)

Financial Services Information Sharing and Analysis Centre (FS-ISAC) (2020). "COVID-19 effects on cyber security survey".

IAIS (2018) Draft Application Paper on Supervision of Insurer Cyber security.

IMF WP/2018/143, Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment

Ionescu, L. Mirea, V. & Blajan, A. (2011). Fraud, corruption and cybercrime in a global digital network. Economics, Management and Financial Markets, 6(2), 373-380.

Kaffenberger L, Kopp E., and Wilson C. (2017). Cyber risk, market failures, and financial stability. 17-185. International Monetary Fund.

Kante S. (2017). Prevention of Cyber Crimes and Fraud Management.

Kashyap A.K, Wetherilt A. (2019). Some principles for regulating cyber risk. In AEA Papers and Proceedings, 109. pp482–87.

Mohottige G, Sujeewa M, Shukri M, Yajid A, Khatibi A, Azam S. M. F and Dharmaratne (2018). The New Fraud Triangle theory - Integrating ethical values of employees. International Journal of Business, Economics and Law, *16(5), pp304-355*

Mugari I., Gona S., Maunga M and Chiyambiro R. (2016). Cybercrime - The Emerging Threat to the Financial Services Sector in Zimbabwe. Mediterranean Journal of Social Sciences. Vol 7 No 3 S1

Mwabu D.K. (2013). Factors influencing electronic fraud in the banking industry in Kenya: A case of Kenya Commercial Bank Central Region. Masters Dissertation. University of Nairobi, Kenya

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

Oesterreichische National bank (OeNB) in cooperation with the Financial Market Authority (FMA) December, 2004 credit approval process and credit risk management

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.

Raghavana, A.R., Parthiban, L. (2014). The effect of cybercrime on a Bank's finances, International Journal of Current Research & Academic Review, 2(2), pp. 173-178.

Usman, A.K. and Shah M.H. (2013), Critical Success Factors for Preventing e-Banking Fraud, *Journal of Internet Banking and Commerce*, 18(2), pp25-39

Webster, J. & Drew, J.M. (2017). Policing advance fee fraud (AFF): Experiences of fraud detectives using a victim-focused approach. International Journal of Police Science and Management, 19(1), pp39-53.

Williams, D.A. (2007), Credit Card Fraud in Trinidad and Tobago, Journal of Financial Crime, 14(3), pp225-215.

Zakrzewski A., Tañg T., Appel G., Fages R., Hardie A., Hildebrandt N., Kahlich M., Meñde M., Muxí F. and Xavier A. (2019). "Global Wealth 2019: Reigniting Radical Growth", Boston Consulting Group, 20 June.