The assessment of the impact of cyberfraud in the South African banking industry

Oluwatoyin Esther Akinbowale, Heinz Eckart Klingelhöfer and Mulatu Fekadu Zerihun

Faculty of Economics and Finance, Tshwane University of Technology, Pretoria, South Africa

Abstract

Purpose – The purpose of this study is to assess the impact of cyberfraud in the South African banks with the aim to provide recommendations to effectively mitigate it.

Design/methodology/approach – The study uses a qualitative approach involving the use of structured questionnaires. The questionnaires were made available to the staff of 17 licensed banks in South Africa who deal with management, operation, administration and banking services. Two hypotheses were formulated and non-parametric statistical analyses involving the use of Chi-square test, Fischer's Exact test and Spearman's correlation were carried out. The two hypotheses formulated were tested to draw a conclusion.

Findings – The results obtained indicate that the impact of cyberfraud in the South African banking industry is highly significant and has affected the reputation of some of the banks. This calls for the need to review the diverse ways of curbing cyberfraud to lessen their impact and that of associated fraud risks on the banking operation.

Practical implications – This study provides an analysis on the relationship cyberfraud occurrences and the reputation of South African banks. The implementation of the recommendations may reinforce the existing security measures in the fight against cyberfraud.

Originality/value – The novelty of this study lies in the fact that the assessment of the impact of cyberfraud on the banking industry in South Africa has not been sufficiently highlighted by the existing literature.

Keywords Banking operation, Cyberfraud, Fraud risk, Reputation

Paper type Research paper

1. Introduction

Fraud is a critical problem of global concern (Gbegi and Adebisi, 2014, p. 234). It involves the use of occupation for personal benefit via a deliberate misuse or misappropriation of an organisation's resources [Association of Certified Fraud Examiners (ACFE), 2012, 2019].

The South Africa banking industry is managed and controlled by the South Africa Reserve Bank (SARB) as the regulatory authority over the banking industry and financial institutions, aiming to achieve a robust and efficient banking system in the interest of the

Journal of Financial Crime
Vol. 31 No. 2, 2024
pp. 287-301
Emerald Publishing Limited
1359-0790
DOI 10.1108/JFC-10-2022-0260

customers and the economy in accordance with the Banks Act (No. 94 of 1990), or the Mutual Banks Act (No. 124 of 1993) (SARB, 2020). Information Technology (IT) is critical in achieving this aim and for performing the day-to-day operations for most organisations (Ali *et al.*, 2017, p. 70). However, it can be said that IT has an adverse impact on the banking industry, too, where crimes such as phishing, hacking and forgery are committed (Ramadani *et al.*, 2018, p. 341).

Cybercrime involving the use of malicious software, computer hacking and denial-of-service attacks, phishing, data theft, spamming, card theft, online fraud, vishing, spying, etc. are becoming more common (Tiwari *et al.*, 2016, pp. 47–50; Cassim, 2016, p. 131; Ali *et al.*, 2017, pp. 72–73).

In South Africa, there are efforts carried out by the government in mitigating cybercrime such as the establishment of the South African Banking Risk Information Centre (SABRIC). The SABRIC is saddled with the responsibility of providing the banking institutions with the necessary information related to crime and risk management and to promote inter-bank synergy aimed at reducing the risk of bank and organised related crimes (Cassim, 2016, p. 131). In addition, the effort of the police is also perceived as a positive move in the quest to sustain the fight against cybercrime (Cassim, 2016, p. 131). It collaborates with the banking institution and the IT industry through the SABRIC to combat cybercrime and bring perpetrators to book (Cassim, 2016, p. 131). The Computer Security Incident Response Team (CSIRT) has also been established in South Africa to response swiftly to incidences of cybercrime.

However, despite these efforts put in place by the South African banking sector in mitigating cyberfraud, the impact of cyberfraud on the banks is still detrimental.

The report from the PwC Biennial Global Economic Crime Survey published in February 2018, revealed that South African businesses continued to recount the highest instances of economic crime in the world over the past decade (2008–2017) (PwC, 2018, p. 6). Nevertheless, in 2020, the following report from the same source indicated that the rate of economic crime in South Africa dropped from 77% to 66% (PwC Report, 2020, p. 8). However, the percentage remains still higher than the global average rate of economic crime given as 47% in the same year (PwC Report, 2020, p. 8).

The purpose of this study is to assess the impact of cyberfraud on the South African banks with the aim to provide recommendations to effectively mitigate the impact of cyberfraud. The study objectives involve the statistical analysis of data obtained via a structured questionnaire, testing of hypotheses and drawing of conclusions from the results obtained. The motivation for this study is to expand research on the nature of cyberfraud affecting the South African banks with a view to propose sustainable approaches aimed at curbing the rising occurrence of cyberfraud in South Africa. The identified problem of an increasing cyberfraud rate in the South African banking sector has made customers lose confidence in the services provided by the sector.

To address this aim, two research questions were formulated as follows:

RQ1. What is the nature of cyberfraud perpetrated in the South African banking industry?

RQ2. What is the effect of the cyberfraud perpetration on the South African banking industry?

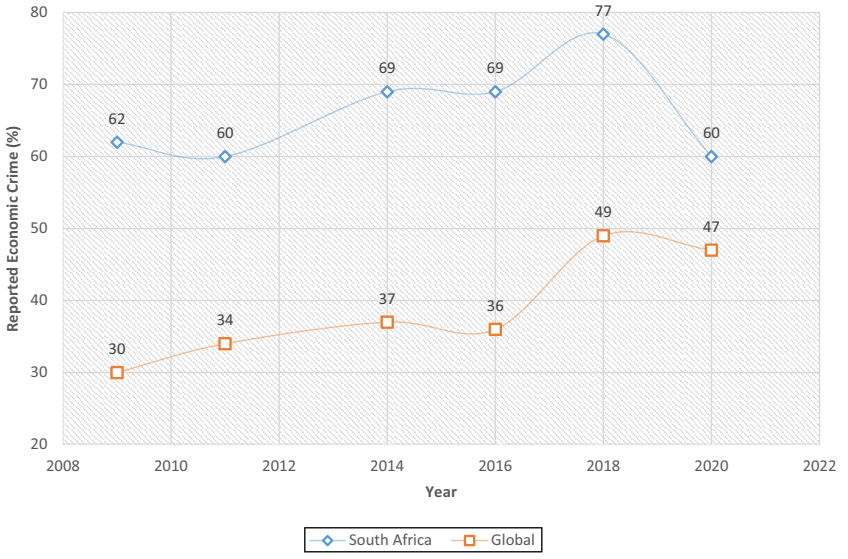
The novelty of this study lies in the fact that the assessment of the impact of cyberfraud on the banking industry in South Africa has not been sufficiently highlighted by the existing literature.

Section 2 presents the literature review followed by the methodology used in this study in Section 3, while the succeeding sections present the results and their discussion in Section 4,

the conclusion drawn in Section 5 from the findings in relation to the study objectives as well as the recommendations and policy framework.

2. Literature review

Figure 1 presents the reported rate of economic crime in South Africa in comparison with the global average rate of economic crime in 2020 (PwC's Global Economic Crime Survey, 2020, p. 8). In the figure, South Africa was ranked in the third position in the ten top ranking of countries with the highest rate of reported economic crime in the world as compared to the first position in 2018 (PwC's Global Economic Crime Survey, 2020, p. 8; PwC's, 2018, p. 9). This implies a 17% decrease in the rate of economic crime between 2018 and 2020 reported globally. However, comparing these statistics with the global average rate of economic crime, it shows that the reported rate of economic crime in South Africa still exceeds the average global rate with by 13%. More worrisome is the fact that there is an increase in the rate of crime involving senior management from 20% in 2018 to 34% in 2020 as shown in Figure 2 (PwC's global Economic Crime Survey, 2020, p. 8). This implies that the percent rate of reported economic crime in South Africa decreased slightly between 2018 and 2020 when compared with other countries. The prevalent economic crime in South Africa has been identified as customer's fraud, bribery and corruption, financial statement fraud and cybercrime (PwC's Global Economic Crime Survey, 2020, p. 10). The PwC's Global Economic Crime Survey (2020, p. 12) categorised fraud perpetrators into three categories: external perpetrators, internal perpetrator as well as collusion between external and internal perpetrators. The internal perpetrators account for the highest percentage of the perpetrators accounting for (41%), followed by the external perpetrators (36%), while collusion between the internal and external perpetrators account for (21%) of the reported economic crime rate in South Africa (PwC's Global Economic Crime Survey, 2020, p. 12).



Source: PwC's Global Economic Crime Survey (2020, p. 8)

Figure 1.
Reported economic crime in South Africa and global average rate in 2020

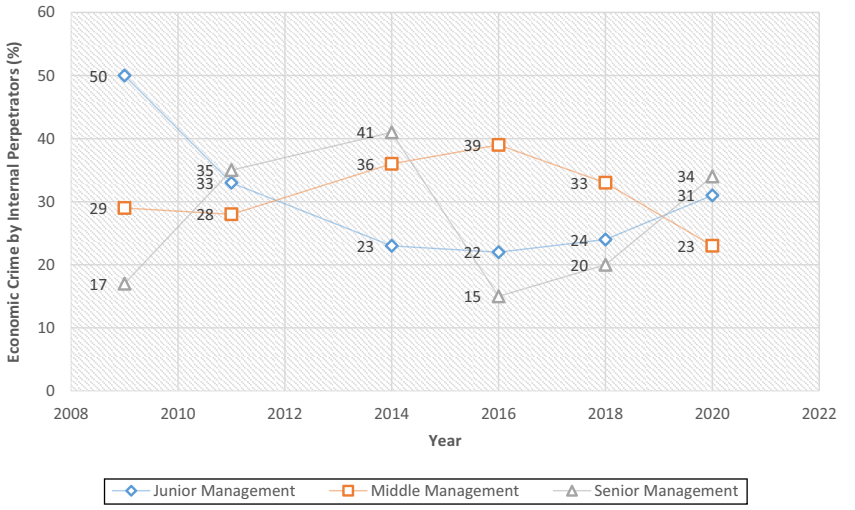


Figure 2.
Economic crime by internal perpetrators in South Africa

Source: PwC's global economic crime survey (2020, p. 13)

The internal perpetrators were further classified into three management levels, namely, senior, middle and junior management levels, and the statistics of the economic crime attributed to these three management levels are presented in Figure 2.

In a bid to sustain this fight, the Promotion of Access to Information Act 2 of 2000 (PAIA) as well as the Electronic Communication and Transaction Act 25 of 2002 (ECT) were enacted with the aim to facilitate and regulate communications and transactions to protect the interest of financial institutions and the general public. Unfortunately, the criminal section of the ECT act has been criticised as relatively not being stringent enough (Cassim, 2016, p. 128). The non-stringent nature of the ECT act might not send enough warning signals to the perpetrators.

The South African Banking Risk Information Centre (SABRIC, 2019) reported that, in 2017, a total of 13 438 cybercrime cases involving mobile and banking apps as well as online reportedly banking costed the banking industry a gross sum of more than R250,000,000. Furthermore, the rate of cybercrime and economic crime is reportedly increasing in the South African financial institutions (Cassim, 2016, p. 130; PwC's, 2016, p. 10; Van Niekerk, 2017, p. 126).

The literature confirmed that cybercrime is still a threat to the South African banking sector, despite the efforts of the sector to mitigate its occurrences (Mbelli and Dwolatzky, 2016, p. 1; Van Niekerk, 2017, p. 126; PwC, 2020, p. 8; Akinbowale *et al.*, 2022, p. 996). The literature also indicated that the rate of cybercrime is increasing globally with dire consequences on the customer's satisfaction, reputation and economic growth of financial institutions. Other losses include the indirect loss via loss of trust in the digital infrastructure, direct loss through fraud perpetration, as well as customer and stakeholder losses (Kraemer-Mbula *et al.*, 2013, p. 544; Lagazio *et al.*, 2014, p. 60).

In South Africa, information security challenges due to cyberattacks continues to pose a serious economic threat to financial institutions and the country as a whole (Mbelli and Dwolatzky, 2016, p. 1; PwC Report, 2020, p. 8). This has made many financial institutions to consider risk management as an important entity in their business model.

Van Niekerk (2017, p. 126) identified the leading perpetrators of cyberattacks as hackers and criminals in South Africa while the two major cyberattack impacts are data exposure and financial theft.

The outcome of the review for this chapter indicates that the growing number of internet users coupled with the emerging technologies have increasingly exposed the information of many organisations to a variety of risks. Such attacks could be in the form of unauthorised access to the network or system with the intention to defraud or manipulate business operations (Tiwari *et al.*, 2016, p. 46). Furthermore, it can be in the form of a data breach where sensitive data are stolen.

The increasing risk of cyberfraud and the potential impacts on the financial institutions is a major concern for the stakeholders. The studies also indicated that the increasing fraud risks have impacted negatively on the operation, reputation and economic development of financial institutions. It is based on this reviews that two alternative hypotheses are formulated as follows:

H1. The impact of cyberfraud on the South African banking industry is significant.

H2. The occurrence of cyberfraud affects the South African banking industry.

3. Methodology

In this paper, the qualitative approach was used involving the gathering of different opinions and perspectives as well as the categorisation of the characteristics of the population about cyberfraud from the South African licensed banks. According to Mohajan (2018, p. 21), the qualitative approach boasts of the following merits: it can be used for the improvement of both the design and interpretation of traditional surveys; it can explore the research problem from the perspective of the actors involved, rather than explaining it from the outside; it can assist in the understanding of complex phenomena which are difficult to capture via quantitative research. In addition to these merits, the qualitative approach is reliable and objective, it simplifies a complex problem to a limited number of variables, investigates the relationships between variables, while establishing the cause and effect in highly controlled circumstances. It is also suitable for theories and hypothesis testing; it assumes sample which is representative of the population with reduction in the subjectivity of researcher although it is less detailed but simpler than the quantitative data (Ospina, 2004, p. 1279; Mohajan, 2018, p. 21). Due to the sensitive nature of cyberfraud and confidentiality which characterise the process of fraud investigation and uncovering, the researchers opted for the qualitative approach in view of the merits.

However, the qualitative approach involving the use of structured questionnaire was used for this study due to the fact is suitable for data collection, hypothesis testing and provision of results that would reflect the situation under investigation with statistical precision.

This study uses a purposive sampling because it permits the selection of specific groups in the sample who possess the necessary experience to understand cyberfraud, and it makes it possible to obtain the valuable perceptions of the target group. The population of this study consists of all the 17 licensed commercial banks listed in South Africa (Bankscope, 2018). All these banks were considered in this study for an effective response rate because the response rate in any research is expected to fall between 70% and 80% which translates into an adequate representation (Fincham, 2008, p. 2).

All the 17 licensed banks were considered so that the outcome of the findings in this study can be a true representation of the prevailing situation in the South African banks.

Using a structured questionnaire, a total number of 42 responses were obtained from all the 17 licensed banks in South Africa.

The research design used in this study is shown in Figure 3.

The study uses qualitative analysis with the use of structured questionnaire. The questionnaires were administered to the staff of the 17 licensed banks in South Africa who deals with management, operation, administration and banking services.

The variables used for the testing of *H1* include the responses obtained for the forms of cyberfraud.

The variables used for the testing of *H2* include reputation loss, revenue loss, productivity loss and shareholder's loss. This is because cyberfraud perpetration has been linked to the organisation's revenue losses, reputation, customer's loyalty and shareholder's confidence (Joyner, 2011; Dzomira, 2015, p. 13).

These hypotheses were tested in the SPSS environment (version 26) to draw a conclusion, using non-parametric statistical analyses:

- the Chi-square test and Fischer's Exact test for hypothesis testing; and
- Spearman's correlation for investigating the nature of the relationship between variables were carried out.

The rationale for using the Chi-square test lies in the fact that it is a non-parametric tool designed to analyse group differences when the variable is measured at a nominal (categorical) level (Mchugh, 2013, p. 143), and that it also allows for testing hypotheses as well as the relationship of two variables in a qualitative (categorical) data set (Abebe, 2019, p. 37; Rana and Singhal, 2015, p. 69). To determine the association between two categorical variables (whether they are independent or dependent with respect to each other), the Fisher's exact test was used. Unlike the Chi-Square test, it runs an exact analysis for a relatively small sized sample (Kim, 2017, p. 152). The Chi-square statistics were computed as well the p-values for the Chi-square and Fischer's exact tests. Where the *p*-value is less than 0.05, there is no enough evidence to accept the null hypothesis at 5% level of significance; hence, the alternative hypothesis is assumed to be true with the level of evidence presented in this study.

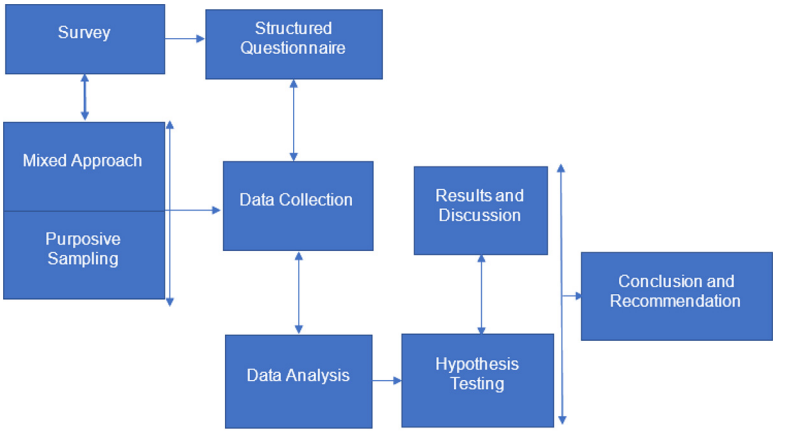


Figure 3.
Research design

Source: Authors' design

Finally, Spearman's correlation analysis was chosen as a non-parametric analysis to measure the degree of association between two variables of ranked scores (Choi *et al.*, 2010, p. 459). This is due to the fact that the effect of one variable may produce a direct or inverse effect on another variable once a common relationship exists between them. In this study, it was used for the determination of the degree of interdependence between the variables of cyberfraud and the effect of cyberfraud on organisation. According to Choi *et al.* (2010, p. 460), the Spearman's correlation coefficient (ρ) ranges from -1 to $+1$ with $+1$ denoting a perfect (correlation) between the variables and -1 implying a perfect negative correlation, while 0 means that there is no correlation between the variables.

The choice of the non-parametric techniques (Chi-square statistical analyses, Fischer's exact test and Spearman's correlation non-parametric technique) for hypothesis testing and for establishing the association between the identified variables relating to cyberfraud stems from the fact that the data set used in this study is not normally distributed.

4. Results and discussions

The two formulated hypotheses underlying this study are tested as follows:

H3. The impact of cyberfraud on the South African banking industry is significant.

The variables used for the testing of this hypothesis include the responses obtained for the forms of cyberfraud. The respondents to the survey questions identified eight common forms of cyberfraud that are prevalent in South Africa. These include phishing, spying, malware, data theft, spam e-mail, online theft, hacking and skimming. This findings agree substantially with some existing literature which indicated that some financial institutions still suffer cyberattack in the forms identified via the survey (Tiwari *et al.*, 2016, pp. 47–50; Cassim, 2016, p. 131; Ali *et al.*, 2017, pp. 72–73; Ramadani *et al.*, 2018, p. 341).

Table 1 presents the Chi-square and the Fischer's Exact tests for the forms of cyberfraud identified from the survey. In *H1*, the alternative hypothesis tested was therefore accepted. This is justified by the fact that the *p*-values of each of the variables is less than 0.05 for both the Chi-square and the Fischer's Exact tests. This implies that the impact of cyberfraud on the South African banking industry may be significant.

Modugu and Anyaduba (2013, p. 282) explain that an employee of the organisation can take advantage of easy access to the banks and customer information as well as weak internal controls to commit fraud. On the other hand, people outside an organisation can also

Forms of cyberfraud	Chi-square statistics	Degree of freedom (df)	Asymptotic Significance (Asymp. Sig.)	Fischer's exact significance	Point probability
Phishing	26.236	4	0.000	0.000	0.000
Spying	21.773	4	0.001	0.001	0.000
Malware	35.634	4	0.001	0.001	0.000
Data theft	15.667	4	0.012	0.012	0.003
Spam e-mail	22.235	4	0.000	0.000	0.000
Online theft	18.987	4	0.000	0.000	0.000
Hacking	25.678	4	0.000	0.000	0.000
Skimming	28.876	4	0.001	0.001	0.000

Source: Statistical analysis of the responses obtained from the field survey

Table 1. Chi-square and Fischer's exact tests for the forms of cyberfraud

exploit the weak security and anti-fraud measures of financial institutions to commit fraud. Some take advantage of customers' ignorance to commit fraud (Modugu and Anyaduba, 2013, pp. 282–283). According to Hinde (2003, p. 664):

> It was estimated that 80% of the cyber security breaches result directly or indirectly (i.e. through collaboration with external bodies) by the people within the organisation.

This can be traced to the fact that internal employees have direct access to information and have a better knowledge of the control architecture of the organisation. This knowledge can be leveraged to invent cover-up schemes that can promote the affinity for continuous crime perpetration.

In *H1*, the alternative hypothesis tested was therefore accepted. This is justified by the fact that the *p*-values of each of the variables is less than 0.05 for both the Chi-square and the Fischer's Exact tests. This implies that the impact of cyberfraud on the South African banking industry may be significant. These findings agree significantly with the report of the South African Banking Risk Information Centre (SABRIC, 2018) which reported that in 2017 there were 13,438 reported cases of cybercrime incidences which cost the banking industry over R250m in gross losses. SABRIC (2018) also indicated that the rate of cybercrime increased by 20% in 2018 causing an 8% increase in the gross losses. SABRIC (2019) also reported that there had been an exponential increase in cyberfraud related cases from January to August 2018, with an estimated increase by 64%. This has further resulted in a 7% increase in the gross losses when compared to the same period in 2017. Comparing the losses incurred between January to August 2017 with the same period in 2018, the losses incurred amounted to more than twice the original loss (gross losses of R39,322,237), with an increase of 44% (gross loss of R89,368,722) in online banking incidents (African Union Report on Cyber Security and Personal Data Protection, 2016). The losses were mostly attributed to the use of online and mobile banking platforms. In 2019, the number of incidences increased to 26,567 which reportedly cost the South African banking industry about R308m in gross losses while in 2020, 35,308 incidences were reported which reportedly cost the banking industry about R309m in gross losses (SABRIC, 2020).

The variables used for the testing of *H2* include reputation loss, revenue loss, productivity loss and shareholder's loss.

Some of the identified indicators for measuring the impact of cybercrime on the financial institutions include customer and employee satisfaction, product innovation, organisation's growth and productivity, market share, and position in the stock market, financial losses, loss of customers and business partners or opportunities, loss of reputation and decrease in the organisation's market value (Dzomira, 2014, p. 23; Goel and Shawky, 2009, p. 404; Kraemer-Mbula *et al.*, 2013, p. 544).

Table 2 presents the Chi-square and Fischer's Exact tests for the effect of cyberfraud on the organisation. The alternative hypothesis tested was therefore accepted to be true as the

Table 2.
Chi-square and Fischer's exact tests for the effect of cyberfraud on organisation

Effect of cyberfraud on organisation	Chi-square statistics	df	Asymp. Sig.	Fischer's Exact Sig.	Point probability
Reputation loss	21.429	1	0.000	0.000	0.000
Revenue loss	18.667	1	0.000	0.000	0.000
Productivity loss	31.333	3	0.000	0.000	0.000
Shareholder's loss	30.952	3	0.000	0.000	0.000

Source: Statistical analysis of the responses obtained from the field Survey

p-values (0.000) of each of the variables is less than 0.05 for both the Chi-square and the Fischer's Exact tests. This means that the occurrence of cyberfraud may affect the South African banking industry in terms of reputation loss, revenue loss, productivity loss and shareholder loss. This finding agrees significantly with the findings of Dzomira (2015, p. 13) and Joyner (2011) that cyberfraud perpetration has an adverse effect on the organisation's revenue losses, reputation, customer's loyalty, and shareholder's confidence. In South Africa, BusinessTech (2017, p. 2) reported that in 2017, "ABSA and Standard Bank clients have lost between R1 million and R^2 million to Internet banking or SIM swap fraud, hence, they want the banks to be held liable for fraudulent activity". BusinessTech (2017, p. 2) also explains that fraud can result from the loss of trust by stakeholders, thus leading to loss of credibility and a lack of confidence in the organisation amongst the public. Cyberfraud has been identified as one of the major challenges in the banking industry [PwC (2016), p. 22, South African Banking Risk Information Centre (SABRIC) (2018)]. If not effectively mitigated, it can have grave consequences on a business, trigger financial damage and destroy the reputation of the banking institution or the company's reputation.

Wanemba (2010, p. 6) found that the financial institutions have consistently lost huge sums of money to cyberfraud or other forms of fraud. This has led to a negative impact on the organisation's profitability. Although the banking institutions decry that the impact is on increasing operational costs, loss of reputation and customer's dissatisfaction as well as revenue loss.

Table 3 depicts the impact of cyberfraud incidents on the banking industry with respect to individual responses. The dimension of the responses gathered from the respondents indicated that the banking industry suffers different losses because of the occurrence of cyberfraud incidents as shown in Figure 4.

In line with the findings of this study, cybercrime had been reported to exert a negative impact on organisation's profitability, customers' satisfaction, public trust, organisational goodwill and risk management, globally (Goel and Shawky, 2009, p. 404; Martin and Rice, 2011, p. 803; Saini *et al.*, 2012, p. 202; Kraemer-Mbula *et al.*, 2013, p. 544; Lagazio *et al.*, 2014, p. 60).

Existing literature has traced one of the major causes of cyberfraud and its increasing risk in South Africa to the recent innovations and technological development in this digital era (Dlamini and Mbambo, 2019, p. 1; Herselman and Warren, 2004, p. 263; Dzomira, 2017, p. 143; Coetzee, 2018, p. 3; Dagada, 2013, p. 148; Sutherland, 2017, p. 84).

UK Finance (2018, p. 6) reported that, over the years, cybercriminals have deployed many means of manipulating financial institutions via phishing emails, impersonation and

Effects	No. of response (*n*) Agree	No. of response (*n*) Strongly agree	No. of response (*n*) disagree	No. of response (*n*) Strongly disagree	No. of response (*n*) undecided	Total no. of respondents (*N*)
Reputation loss	6	36	0	0	0	42
Loss of revenue/ profit	7	35	0	0	0	42
Productivity loss	18	21	2	1	0	42
Depletion of shareholder's fund	20	19	1	0	2	42

Source: Responses obtained from the field survey

Table 3. Effects of cyberfraud incidents on organisation

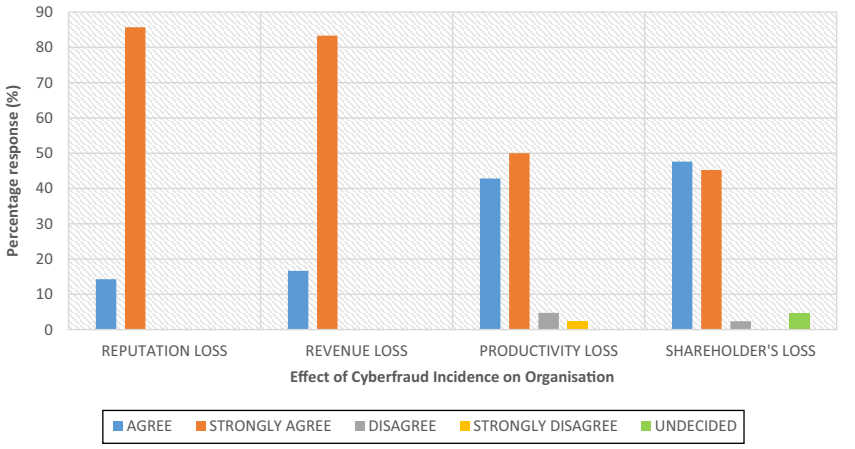


Figure 4.
The effect of cyberfraud on organisation

Source: Responses obtained from the field survey

account hacking, thereby paving way for unauthorised access to sensitive information and the compromise of the financial institutions. Similarly, Dzomira (2014, p. 16) explained that the banking industry in Zimbabwe has also suffered cyberfraud different forms such as unauthorised intrusion into the banks' or personal information or accounts, credit/debit card fraud, money laundering, employee embezzlement, pharming, phishing, malware, hacking, virus, spam and advance fee fraud.

To mitigate cyberfraud occurrences, Akinbowale *et al.* (2020a, p. 945) suggested the need for the use of a real time an alert system capable of creating awareness for both the financial institutions and their customers whenever there is unauthorised access into the customers' account or the database of the financial institution. This will enhance a rapid response to block such intrusion before any unauthorised transaction takes place. Two simplified conceptual models for cyberfraud mitigation have also been reported by Akinbowale *et al.* (2020b, p. 1253). The first model addressed the incorporation of forensic accounting into the organisation's structure while the second captured the detailed investigation and comprehensive data analysis processes of uncovering fraud. This will strengthen the organisation's control structure and aid the process of fraud investigation and mitigation. This is because the procedural steps for implementation of forensic accounting, namely, preliminary survey, detailed investigation, comprehensive data analysis, reporting and expert witness are captured in the model.

Dzomira (2017, p. 143) suggested the need for the augmentation of cyberfraud alert systems and sensitisation of internet banking users about the nature of cyberfraud perpetrated by cyber attackers in South Africa. While there was access to information on fraud-related Internet banking on the websites of the South African banks, this study suggested improved sensitisation about the nature of cyberfraud perpetrated and how they were perpetrated. Dzomira (2017, p. 150) stated that the banking sector should relentlessly campaign against internet banking fraud in a manner that would benefit the clients and the diverse communities in South Africa.

Dlamini and Modise (2012, p. 1) explained that for the South African Banks to reduce cyberfraud incidences, the first line of defence was cybersecurity. In the absence of a

national cybersecurity policy in South Africa, cybersecurity awareness and initiatives were gaining momentum to create cybersecurity awareness (Dlamini and Modise, 2012, p. 1).

Using the cross tabulation function, the statistical analysis of the cross effect of pair of reputation loss and revenue loss was statistically significant at 95% confidence level, thus, indicating that a direct relationship may exist between two variables.

The magnitude of the Spearman's correlation coefficient (0.365) shows that the two variables are dependent. Fischer's Exact statistical value for the cross effect of reputation loss and revenue loss was 5.600 with a significance level ($0.048 < 0.05$) at one degree of freedom (Table 4). Table 4 shows the cross-tabulation for the pair of reputation loss and revenue loss, while Figure 5 indicates the number of counts for the relationship between reputation loss and revenue loss based on the outcome of survey. The variations between the number of counts and the expected number of counts in Table 5 shows that the variables are dependent. This further lends credence to the fact that a relationship may exist between two variables, namely, reputation loss and revenue loss.

These results imply that a loss of reputation due to cyberfraud occurrence can cause a decline in the revenue generated by the organisation due to a negative public image. Similarly, revenue loss due to cyberfraud occurrence could also impair the reputation of the organisation.

Paired factors	Fischer's exact test statistics	df	Exact Sig. (2 tailed)	Remarks	Spearman's correlation coefficient	Relationship
Reputation loss and revenue loss	5.600	1	0.048	1 cell (25.0%) have expected outcomes less than 5. The minimum expected count is 1	0.365	Positive but weak

Source: Statistical analysis of the responses obtained from the field survey

Table 4. The statistical analysis for the pair of the most significant factors (reputation and revenue loss)

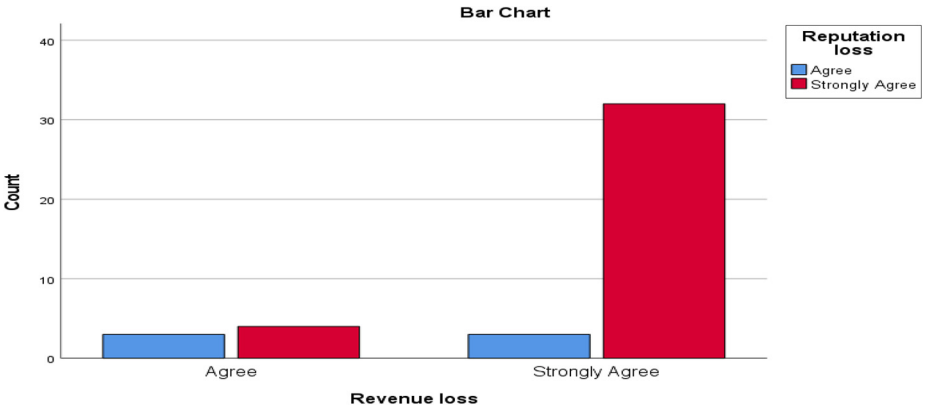


Figure 5. The number of counts for pair of reputation loss and revenue loss

Table 5.
The cross-tabulation for the pair of the most significant factors (reputation and revenue loss)

			Reputation loss		
			Agree	Strongly agree	Total
Revenue loss	Agree	Count	3a	4b	7
		% within revenue loss	42.9	57.1	100.0
		% within reputation loss	50.0	11.1	16.7
		% of total	7.1	9.5	16.7
	Strongly agree	Count	3a	32b	35
		% within opportunity	8.6	91.4	100
		% within greed	50.0	88.9	83.3
		% of total	7.1	76.2	83.3
Total		Count	6	36	42
		% within opportunity	14.4	85.7	100.0
		% within greed	100.0	100.0	100.0
		% of total	14.3	85.7	100.0

5. Conclusion and policy implications

The purpose of this study is to assess the impact of cyberfraud on the South African industry with the aim to provide recommendations to effectively mitigate the impact of cyberfraud. This was achieved using a qualitative approach involving the use of structured questionnaire. A total of 42 responses were obtained across selected participants in the 17 licensed banks in South Africa. The results obtained indicated that the impact of cyberfraud on the South African banking industry is significant and that the occurrence of cyberfraud affects the reputation of the South African banking industry in terms of reputation loss, revenue loss, productivity loss and shareholder loss. According to the results obtained, the prevalent forms of cyberfraud perpetrated in the South African banking industry include phishing, spying, malware, data theft, spam e-mail, online theft, hacking and skimming.

Hence, a holistic review of the internal control system of the banking structure is hereby recommended. Cyberfraud had been reported to have negative impact on an organisation's profitability, customers' satisfaction, public trust, organisation good will and risk management globally. This calls for the need to review the diverse ways of curbing cyberfraud to lessen its impact or associated fraud risks on the banking operation.

This study provides empirical findings that could assist the South African banking industry in the areas decision making or policy formulation geared towards of cyberfraud mitigation. This research notifies the South African banking industry about the nature of cyberfraud perpetrated. The understanding of the nature of cyberfraud perpetrated can assist the South African banking industry to formulate measures to mitigate them. The findings reported in this study is based on the views of the bank experts consulted as well as those of the organisations. Future works can consider the analysis of the level of effectiveness of the fraud control measures in the South African banking industry *vis-à-vis* the forms of cyberfraud identified.

References

Abebe, T.H. (2019), "The derivation and choice of appropriate test statistic (Z, *t*, F and Chi-Square test) in research methodology", *Mathematics Letters*, Vol. 5 No. 3, pp. 33-40.

African Union Report on Cyber Security and Personal Data Protection (2016), [Online], available at: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (accessed 18 November, 2022).

Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. (2020a), "Analysis of cyber-crime effects on the banking industry using balance score card: a survey of literature", *Journal of Financial Crime*, Vol. 27 No. 3, pp. 945-958.

Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. (2020b), "An innovative approach in combating economic crime using forensic accounting techniques", *Journal of Financial Crime*, Vol. 27 No. 4, pp. 1253-1271.

Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. (2022), "Analytical hierarchy process decision model and Pareto analysis for mitigating cybercrime in the financial sector", *Journal of Financial Crime*, Vol. 29 No. 3, pp. 884-1008.

Ali, L., Ali, F., Surendran, P. and Thomas, B. (2017), "The effects of cyber threats on customer's behaviour in e-banking services", *International Journal of e-Education, e-Business, e-Management and e-Learning*, Vol. 7 No. 1, pp. 70-78.

Association of Certified Fraud Examiners (ACFE) (2012), "Managing fraud risk: first, second, or third line of defense responsibility?", United States of America, pp. 1-19, [Online], available at: www.acfe.com/uploadedfiles/acfe_website/content/european/course_materials/2012/11c_risch-cpp.pdf (accessed 2 February 2020).

Association of Certified Fraud Examiners (ACFE) (2019), "Anti-fraud technology benchmarking report", pp. K1-28, [Online], available at: www.acfe.com/uploadedFiles/ACFE_Website/Content/resources/Benchmarking_Technology_Report.pdf (accessed 2 December 2020).

Bankscope (2018), "Bankscope Internet quick guide", [Online], available at: www.bankscope.bvdep.com (accessed 19 October 2018).

BusinessTech (2017), "Major SA banks taken to court over internet fraud", [Online], available at: https://businesstech.co.za/news/mobile/170629/major-sa-banks-taken-to-court-over-internet-fraud/ (accessed 1 August 2021).

Cassim, F. (2016), "Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South Africa and other regional role players. School of law, university of South Africa", Based on a paper presented at the First International Conference of the South Asian Society of Criminology and Victimology (SASCV) at Jaipur, India from 15–17 January 2011, pp. 126-138.

Choi, J., Peters, M. and Mueller, R.O. (2010), "Correlational analysis of ordinal data: from Pearson's r to Bayesian Polychoric correlation", *Asia Pacific Education Review*, Vol. 11 No. 4, pp. 459-466.

Coetzee, J. (2018), "Strategic implications of Fintech on South African retail banks", *South African Journal of Economic and Management Sciences*, Vol. 21 No. 1, pp. 1-11.

Dagada, R. (2013), "Digital banking security, risk and credibility concerns in South Africa", *The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013)*, *Kuala Lumpur, Malaysia*, 4-6 March 2013.

Dlamini, S. and Mbambo, C. (2019), "Understanding policing of cybercrime in South Africa: the phenomena, challenges and effective responses", *Cogent Social Sciences*, Vol. 5 No. 1, pp. 1-13.

Dlamini, Z. and Modise, M. (2012), " Cyber security awareness initiatives in South Africa: a synergy approach", *7th International Conference on Information Warfare and Security*, *Seattle, USA*, pp. 1-10.

Dzomira, S. (2014), "Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe", *Risk Governance and Control: Financial Markets and Institutions*, Vol. 4 No. 2, pp. 16-26.

Dzomira, S. (2015), "Cyber-banking fraud risk mitigation conceptual model", *Banks and Bank Systems*, Vol. 10 No. 2, pp. 7-14.

Dzomira, S. (2017), "Internet banking fraud alertness in the banking sector: South Africa", *Banks and Bank Systems*, Vol. 12 No. 1, pp. 143-151.

Fincham, J.E. (2008), "Response rates and responsiveness for surveys, standards and the journal", *American Journal of Pharmaceutical Education*, Vol. 72 No. 2, pp. 1-3.

Gbegi, D.O. and Adebisi, J.F. (2014), "Forensic accounting skills and techniques in fraud investigation in the Nigeria public industry", *Mediteranean Journal of Social Sciences*, Vol. 5 No. 3, pp. 243-252.

Goel, S. and Shawky, H.A. (2009), "Estimating the market impact of security breach announcements on the firm values", *Information and Management*, Vol. 46 No. 7, pp. 404-410.

Herselman, M. and Warren, M. (2004), "Cyber crime influencing businesses in South Africa", *InSITE 2004: Informing Science + IT Education Conference*, *Rockhampton, Australia*, Jun 26-28 2004, Issues in Informing Science and Information Technol, pp. 253-266.

Hinde, S. (2003), "Computer security: mapping the future", *Computers and Security*, Vol. 22 No. 8, pp. 664-669.

Joyner, E. (2011), "Enterprise-wide fraud management", *Banking, Financial Services and Insurance*, SAS Global Forum 2011, Cary, NC, SAS Institute.

Kim, H.Y. (2017), "Statistical notes for clinical researchers: Chi-squared test and fisher's exact test", *Open lecture on Statistics*, Vol. 42 No. 2, pp. 152-155, [Online], available at: https://doi.org/10.5395/rde.2017.42.2.152 (accessed 2 December 2020).

Kraemer-Mbula, E., Tang, P. and Rush, H. (2013), "The cybercrime ecosystem: online innovation in the shadows?", *Technological Forecasting and Social Change*, Vol. 80 No. 3, pp. 541-555.

Lagazio, M., Sherif, N. and Cushman, M. (2014), "A multi-level approach to understanding the impact of cybercrime on the financial industry", *Computers and Security*, Vol. 45, pp. 58-74.

Mchugh, M.L. (2013), "The Chi-square test of independence", *Biochemia Medica: Biochemia Medica*, Vol. 23 No. 2, pp. 143-149.

Martin, N. and Rice, J. (2011), "Cybercrime: understanding and addressing the concerns of stakeholders", *Computers and Security*, Vol. 30 No. 8, pp. 803-814.

Mbelli, T.M. and Dwolatzky, B. (2016), "Cyber security, a threat to cyber banking in South Africa: an approach to network and application security", *2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing*, pp. 1-6.

Modugu, K.P. and Anyaduba, J.O. (2013), "Forensic accounting and financial fraud in Nigeria: an empirical approach", *International Journal of Business and Social Science*, Vol. 4 No. 7, pp. 281-289.

Mohajan, H. (2018), "Qualitative research methodology in social sciences and related subjects", *Journal of Economic Development, Environment and People*, Vol. 7 No. 1, pp. 23-48.

Ospina, S. (2004), "Qualitative Research", in Goethals, G., Sorenson, G. and MacGregor, J. (Eds), *Encyclopedia of Leadership*, SAGE, London, pp. 1279-1284.

PwC (2016), "Banking in Africa matters – African banking survey", *Global Fintech Report*, pp. 1-100, [Online], available at: www.pwc.org (accessed October 2018).

PwC (2018), "Global economic crime survey: pulling fraud out of the shadows", pp. 1-30, [Online], available at: www.pwc.org (accessed 25 January 2021).

PwC's Global Economic Crime Survey (2020), "Global economic crime and fraud survey", (7th ed.), pp. 1-32, [Online], available at: www.corruptionwatch.org.za/wp-content/uploads/2020/06/global-economic-crime-survey-20201.pdf (accessed 17 January 2021).

Ramadani, S., Siahaan, A.P.U., Sutrisno, R.S., Amelia, W.R., Dalimunthe, H. and Munthe, R. (2018), "Impact of cybercrime on technological and financial developments", *International Journal for Innovative Research in Multidisciplinary Field*, Vol. 4 No. 10, pp. 341-344.

Rana, R. and Singhal, R. (2015), "Chi-square test and its application in hypothesis testing", *Journal of the Practice of Cardiovascular Sciences*, Vol. 1 No. 1, pp. 68-71.

Saini, H., Rao, Y. and Panda, T.C. (2012), "Cyber-crimes and their impacts: a review", *International Journal of Engineering Research and Applications*, Vol. 2 No. 2, pp. 202-209.

South African Banking Report (2019), [Online], available at: www.globenewswire.com/news-release/2019/02/20/1738270/0/en/South-Africa-Banking-Industry-Report-2018.html (accessed 1 June 2019).

South African Banking Risk Information Centre (SABRIC) (2018), "Digital banking crime statistics", [Online], available at: www.sabric.co.za/media-and-news/press-releases/digital-banking-crime-statistics/ (accessed 5 June 2021).

South African Banking Risk Information Centre (SABRIC) (2019), "Digital banking crime statistics", [Online], available at: www.sabric.co.za (accessed 2 February 2020).

South African Banking Risk Information Centre (SABRIC) (2020), "Annual crime statistics", [Online], available at: www.sabric.co.za/media/20oouwbg/sabric-annual-crime-stats-2020.pdf (accessed 20 June 2022).

South African Reserve Bank (SARB) (2020), "Management of the South African money and banking system", [Online], available at: www.resbank.co.za/AboutUs/Functions/Pages/Management-of-the-South-African-money-and-banking-system.aspx (accessed 2 February 2020).

Sutherland, E. (2017), "Governance of cybersecurity – the case of South Africa", *The African Journal of Information and Communication*, Vol. 20, pp. 83-112.

Tiwari, S., Bhalla, A. and Rawat, R. (2016), "Cybercrime and security", *International of Advanced Research on Computer Science and Software Engineering*, Vol. 6 No. 4, pp. 46-52.

UK Finance (2018), "Staying ahead of cybercrime", pp. 1-16, [Online], available at: www.ukfinance.org.uk (accessed 20 January 2022).

Van Niekerk, B. (2017), "An analysis of cyber-incidents in South Africa", *The African Journal of Information and Communication*, Vol. 20, pp. 113-132.

Wanemba, M.A. (2010), "Strategies applied by commercial banks in Kenya to combat fraud", A Management Research Project Submitted in Partial Fulfilment of the Requirements for The Award of the Degree of Master of Business Administration, Department of Business Administration, School of Business, University of Nairobi.

Further reading

Anti-Intimidation and Ethical Practices Forum (AEPF) (2020), "Unpacking fraud", pp. 1-9, [Online], available at: www.aepf.co.za/Unpacking_Fraud.pdf (accessed 16 November 2020).

Ezejiofor, R.A., Nwakoby, N.P. and Okoye, J.F.N. (2016), "Impact of forensic accounting on combating fraud in Nigerian banking industry", *International Journal of Academic Research in Management and Business*, Vol. 1 No. 1, pp. 1-19.

Isa, T. (2011), "Impacts and losses caused by the fraudulent and manipulated financial information on economic decisions", *Review of International Comparative Management*, Vol. 12 No. 5, pp. 929-939.

KMPG (2019), "The Multi-Faceted threat of fraud: are banks up to the challenge?", *Global Banking Fraud Survey*, [Online], available at: www.kpmg.com (accessed 5 May 2022).

Kroll (2011/12), "Global fraud report: economist intelligence unit survey results", [Online], available at: www.kroll.com (accessed 1 August 2020).

PwC (2014), "Global economic crime survey", pp. 1-60, [Online], available at: www.pwc.org (accessed January 2021).

WIlhelm, W.K. (2004), "The fraud management lifecycle theory: a holistic approach to fraud management", *Journal of Economic Crime Management*, Vol. 2 No. 2, pp. 1-38.

Corresponding author
Oluwatoyin Esther Akinbowale can be contacted at: oluwatee01@gmail.com