Enhancing Fraud Detection Through Integration of Forensic Accounting Techniques and Cyber-Security in Financial Institutions in Kenya

Jared Mobisa Mosoti
Department of Accounting and Finance
School of Business and Economics, Mount Kenya University
P.O Box 342-001000 Thika Kenya
Tel: +254-721584620, Email address jmosoti451@gmail.com, jmosoti@mku.c.ke
ORCID No. 0000-0002-7528-1228

Henry Kiptum Yatich
College of Graduate Studies and Research, Mount Kenya University
P.O Box 342-001000 Thika Kenya
Tel: +254- 731 303 105, Email address yatich2002@gmail.com, hyatich@mku.c.ke
ORCID No. 0000-0002-7887-1549

Abstract

The rapid rise in Internet banking and mobile banking transactions has led to a new challenge facing the banking sector through cybersecurity threats. Forensic accountants' understanding of cyber security is key to winning the fight against fraud. This study sought to evaluate the effect of integrating cybersecurity into Forensic accounting on the detection of Fraud in the financial sector in Kenya. The study is anchored on Unified Technology Acceptance and Use Theory (UTAUT) and uses panel data collected on the number of cybersecurity advisories, the reported number of cyberattacks, and the percentage of fraud detections by four Forensic Accounting Techniques. The study findings showed that there was a strong positive correlation between cyber security and fraud detection and integration of cyber security and forensic accounting enhanced fraud detection. The study concluded that the integration of cybersecurity and forensic accounting enhanced fraud detection and contributed positively to financial performance. The study recommended that cyber security skills be integrated into forensic accounting training to enhance fraud detection among forensic accountants to enhance fraud detection.

Keywords: Fraud Detection; Cyber Security; Forensic Accounting Techniques
DOI: 10.7176/EJBM/16-5-03
Publication date: June 30th 2024

1. Background

The importance of financial institutions in the economy cannot be overemphasized. They ensure liquidity, guarantee money supply in the economy, provide loans, savings, and deposits, and ensure payments and settlements are made. As Rayaan et al., (2016) posit, financial institutions strengthen the national economy through fiscal and monetary policy formulation, credit facilities, and interest rate frameworks. For this reason, an attack on the financial sector is an attack on the entire economy. In the recent past, the institutions have steadily moved away from conventional banking hall services to Internet and mobile banking platforms which has come with a new danger in the form of cyber-attacks. The PwC Global Economic Crime Survey of 2016 indicated that an increase in cyber fraud is directly proportional to the deployment of technology in the business area. The Aviva Fraud Report 2021, showed that the banking industry was disproportionately affected by fraud cases with, a 1,318% year-on-year increase in ransomware attacks in the first half of 2021. This therefore shows the vulnerability of these firms to cyber-attacks. While these institutions use forensic accounting techniques in detecting fraud, the introduction of technology in the banking services complicates the war and calls for a need to relook into the effect of enhancing these techniques by integrating them into cybersecurity.

Empirical evidence across the globe shows that Cyber fraud is not only a local problem but a global one. The Indian government reported 1,160,000 cyber-attacks in 2022 which was a marked increase from 2019. The banks in the same country reported 248 successful attacks between 2018 and 2022 In Kenya, the economic survey of 2023 shows that the total number of reported online crimes more than doubled from 339.1 million in 2021 to 700.0 million in 2022. While system vulnerability rose from 58.0 million in 2021 to 452.4 million in 2022. This showed that the attempts on systems were on the rise. On the other hand, the same report showed that the reported web application attacks declined from 7.0 million in 2021 to 1.0 million in 2022. The decline was attributed to huge investments in application security and greater awareness of potential threats. The presence of cyber security was therefore seen as a major deterrent and protection of financial systems from external attacks.

Empirical studies show that Kenya has had several reported cases of Fraud that have led to losses of funds in the financial sector. The PWC, Global Economic Crime and Fraud Survey Kenya report of 2020 showed that 58% of respondents in the survey had experienced financial crimes in the past two years. The survey further showed that 36% of the respondents who had experienced economic crimes lost over 10 million Kenya Shillings whereas 2% of the victims had lost above Kenya Shillings 500 million. These studies showed that fraud was not only a threat to financial institutions alone but also to their customers and the public at large. Further, modern-day frauds are highly skewed to cyber-related attacks. The United Kingdom Crown Prosecution Service (CPS) estimated that 86% of reported fraud is now cyber-related. This therefore puts the load on the financial institutions to find appropriate techniques to curb the risk. Studies by Mosoti, Wafula, and Nyangau (2023) showed that forensic accounting techniques were effective in detecting fraud, and contributing to financial performance. The rise in the risks posed by cybersecurity threats calls for a need to find suitable techniques for fighting the menace. This study therefore sought to find out the effect of integrating cyber security into forensic accounting techniques in the detection of fraud.

1.1. Objective of the study

The study aimed to analyze the effect of integrating cybersecurity into forensic accounting techniques in enhancing fraud detection in the financial sector in Kenya.

1.2. Significance of the study

The study findings will be of use to the developers of forensic accounting curriculums who will design curriculums that will address the current challenges facing organizations, especially financial institutions. Further, it will enhance forensic accounting training to respond to the current financial improprieties facing institutions and governments and produce employable graduates.

On the other hand, the top-level managers of organizations and financial institutions in particular will find the study significant in suggesting ways they can blend forensic accounting and cyber security techniques to combat the fraud menace.

Lastly, the findings of this study will find use among future researchers who will make use of the literature generated and either support or refute the findings of this study.

2. Literature Review

2.1. Unified Technology Acceptance and Use Theory (UTAUT)

The Unified Technology Acceptance and Use Theory (UTAUT) was developed in 2003 by Venkatesh, Morris, Davis, Davis, and Dan as an extension of the Technology Acceptance Theory. The theory posits that the actual use of technology depends on the behavioral intention. The perceived likelihood of adopting the technology swirls around the direct effect of four key constructs: performance expectancy, effort expectancy, social influence, and facilitating conditions (Venkatesh et al., 2003).

The adoption of Cyber security in the fight against fraud is influenced by financial institutions' expectancy of its ability to solve the fraud menace, the effort it requires to perform, and the social and facilitating conditions to make it work. According to Venkatesh et al (2003), performance expectancy is the degree to which individuals believe that by using the system, they will reach their goals and improve their job performance. Venkatesh, Thong & Xu, (2016) added that perceived usefulness, extrinsic motivation, job fit, relative advantage, and outcome expectations were the strongest predictors of technology adoption and acceptance.

The main assumption of the theory is that, by users embracing the implemented technology or approach, and using it, the success rate of the proposed technology will be improved. This theory therefore helps to explain the expected success of the integration of forensic accounting and cyber security in the fight against fraud when implemented in the financial sector.

2.2. Forensic Accounting and Fraud Detection

Hossain, (2023) explains forensic accounting as an essential discipline that combines accounting, auditing, and investigative skills to detect and prevent fraud, corruption, and financial crimes. With the emergence of technology, Forensic accounting has evolved to incorporate the threats posed by technology such as data analytics, cyber forensic accounting, cryptocurrencies, and blockchain technology. These emerging trends have become essential tools for forensic accountants to identify, investigate, and prevent financial fraud. Financial fraud, which falls under the category of monetary fraud, has emerged as a severe economic threat, calling for the expertise of professional forensic accountants and traditional auditors (Oyebisi et al., 2018). The negative impact of financial fraud on the global economy and socioeconomic environment is well documented (Saddiq & Abu Bakar, 2019). As a result, fraud detection and prevention have become essential components of the accounting function, with internal and external auditors expected to contribute (Kassem & Turksen, 2021).

Okoye, Adeniyi, and James (2019), did a study on the Effect of forensic accounting on fraud management on selected firms in Nigeria. The study assessed the effect of Forensic Accounting on fraud management. The objectives of the study were to find the effectiveness of forensic accounting in fraud prevention and the positive effect of forensic litigation on the recovery of funds lost to fraud. The study used a Survey design and a Questionnaire was used to collect data from the accounting staff of Nigeria Breweries Plc, Cadbury Nigeria Plc, Nigeria Bottling Company, and Dupril Forma Nigeria Ltd, all in Aba, Abia State. A sample of 190 was used for the study. The study adopts descriptive statistics involving mean and standard deviation while regression analysis was adopted to test the stated hypotheses. The findings of the study revealed that forensic accounting significantly influenced fraud detection and prevention. The study also revealed that forensic litigation had no significant positive effect on the recovery of funds lost to fraud. Based on the above, the study recommended that companies in Nigeria step up their forensic accounting practices to deter fraud.

Ezejiofor, Nwakoby, & Okoye (2016) carried out a study on the Impact of Forensic Accounting on combating fraud in the Nigerian banking industry. The study aimed to determine the impact of forensic accounting in combating fraudulent activities to ensure good corporate governance practices in the Nigerian banking sector. The survey method was adopted and data were collected through the use of a questionnaire. Data collected from a sample of fifty-five (55)

respondents from commercial banks in Awka, Anambra state were analyzed with a five-point Likert scale. The two hypotheses formulated were tested using t-test statistical techniques with the aid of SPSS version 20.0. The study found among others Forensic accounting is an effective tool for addressing financial crimes in the banking system. Based on this, the study recommended that the apex bank should engage the service of forensic accounting to complement the efforts of other professionals in reducing fraudulent activities to ensure corporate governance in
the financial sector.

2.3. Cybersecurity

Financial institutions face unique challenges of cybercrimes because of handling liquidity which is easy to transfer or conceal the possession. Not only do financial institutions need to combat cyber threats such as web application attacks; bad bots; ransomware; and phishing attacks – but they must also consider how to maintain uptime before, during, and after the attacks to enable them to provide seamless service to customers and maintain compliance with regulators. The use of cyber security to combat cybercrimes in financial institutions is not only a Kenyan situation but a global one. With the surge in cybercrime prevalence, there is a need for cyber forensic accounting to be of importance to combat these crimes. Cyber forensic accounting is the use of forensic accounting principles to investigate and prevent cybercrimes. Cyber forensic accounting is critical in analyzing cybercrimes and identifying the perpetrators. It entails the application of various techniques such as data analytics, digital forensics, and financial investigations to identify cyber-attack sources and recover stolen assets (Law, 2011). In addition to this, Cyber forensic accounting is also critical in preventing future cyber-attacks by ascertaining the feebleness in the cyber security of the organization as well as enabling firms to come up with measures and appropriate controls to counter them (Moid, 2018).

The Cybercrimes committed by the infiltrators of the system may take many forms, such as hacking, identity theft, cyberstalking, and phishing. Hacking is gaining unauthorized access to a computer system, while identity theft involves stealing personal information to impersonate someone else. Cyberstalking involves the use of electronic communication to harass or threaten someone, while phishing involves the use of fake emails or websites to steal personal information (Tonellotto, 2020). These crimes are not easy to investigate for several reasons such as the ever-changing nature of the cyber-attacks which make it almost impossible to stay ahead of the
cybercriminals (Law, 2011). In addition to this, Cavusoglu (2004) cited another challenge as the anonymity nature of the criminals who always operated from remote locations. Furthermore, the
existence of enormous volumes of data dealt with by these criminals makes it harder for investigators and security operations of the organization to extract relevant information and identify patterns (McGuire & Dowling, 2013). These and many others have led to the ever-increasing demand for cyber security more so in the financial sector.

2.4. Forensic Accounting and Cyber Security

With the increased use of technology in business and the digitalization of business processes, cybercrime has become a noteworthy threat to organizations, leading to the increased need for the combination of cybersecurity and forensic accounting. While cyber security focuses on curbing threats of cybercrimes such as hacking, identity theft, and data breaches, forensic accounting focuses on collecting analyzing, and interpreting digital evidence from various sources such as networks, electronic devices, and servers to conclude the various financial crimes (Prasanthi,2016).

3. Methodology

3.1. Data Collection

The data for the study was collected using available data on the economic survey, and the economic crimes survey. The economic survey reports provided data on the number of cybersecurity advisories and the number of reported cyber-attacks between 2018 and 2022. These were obtained from the economic survey of 2022 and the findings are shown in Appendix 1 and Appendix 2 annexed at the end of the document. The advisories and attacks for cyber security involved in the study were Malware, Botnet/DDoS2, Website Application, and System Vulnerability. The effectiveness of forensic accounting techniques was obtained from the PWC Global Economic Crime and Fraud Survey of 2020.

3.2. Model Specification

The model after the integration is represented by the following model:

$Y = (X_1*R^2+X_1) + (X_2*R^2+X_2) + (X_3*R^2+X_3) +(X_4*R^2+X_4)$

Where:

Y is fraud detection as measured by the number of successful attacks.

$X_{,1}$ =Suspicious Activity Monitoring

X_2 = Routine Internal Audits

X3 =Tip-offs

X4 = Fraud Risk Management

R = Cyber Security (number of advisories)

4. Findings and Discussion

4.1 Correlation Analysis for Cyber Security and Fraud Detections

To test the correlation between the combined data for advisories and threats for the five years, the study conducted a correlation analysis. The findings are shown in Table 1 below.

Table 1: Correlation Between Cyber Forensic Accounting and Fraud Detection

Correlations

		COMPOADV	COMPCRE
COMPOADV	Pearson Correlation	1	
	Sig. (2-tailed)		
	N	5	5
COMPCRE	Pearson Correlation	.979**	1
	Sig. (2-tailed)	.004	
	N	5	5

**. Correlation is significant at the 0.01 level (2-tailed).

COMPOADV= Composite Advisory

COMPCRE = Composite Cyber Crimes

Source: Research Findings 2023

Table 1 above shows the correlation between the cyber security threat advisories and the cyber security attacks. At a 2-tailed significant level of 0.979, the study findings as shown in Table 1 indicated that there was a strong positive correlation between the cyber security advisories and the detection of fraud as measured by cyber-attacks. Hence Cyber Forensic Accounting can be used to detect cyber-attacks.

4.2. Regression Analysis for Cyber Security and Fraud Detections

The first indicator in this study was shown by pairing the cyber security advisory and cyber-attacks for Malware. The model summary for the findings is shown in Table 2 below.

Table 2 Model Summary for Malware Advisory and Malware Attacks

Model Summary

Model	R	R Square	Adjusted R Square	Std. The error of the Estimate
1	.841[a]	.707	.610	23973039.82340

a. Predictors: (Constant), Malware advisory

Source: Research Findings 2023

Table 2 shows an R of 0.841 and an R square of 0.707, this shows that advisory by malware had a positive and significant effect on the malware attacks in Kenya. This means that cyber security as measured by Malware can block this kind of cyber threat. It shows that 70.1% of the changes in malware attacks are explained by cyber security and issued advisories of eminent attacks.

The second indicator in this study was shown by pairing the cyber security advisory and cyber-attacks for Botnet/DDS2. The model summary for the findings is shown in Table 3 below.

Table 3: Model Summary for Botnet/DDoS2 Attacks

Model Summary

Model	R	R Square	Adjusted R Square	Std. The error of the Estimate
1	.987^a	.975	.966	8448121.85323

a. Predictors: (Constant), BOTADV

Source: Research Findings 2023

Table 3 shows an R of 0.987 and an R square of 0.975. This shows that the advisory for Botnet/DDS2 had a positive and significant effect on the Botnet/DDS2 attacks in Kenya. This means that cyber security as measured by Botnet/DDS2 can block this kind of cyber threat. It shows that 97.5% of the changes in Botnet/DDS2 Cyber-attacks are explained by cyber security detection and advisory.

The third indicator in this study was shown by pairing the Website Application Attack advisory and the actual Website Application Attacks. The model summary for the findings is shown in Table 4 below.

Table 4: Model Summary for Website Application Attack

Model Summary

Model	R	R Square	Adjusted R Square	Std. The error of the Estimate
1	.657^a	.431	.241	3833906.05024

a. Predictors: (Constant), WEBADV

Source: Research Findings 2023

Table 4 shows an R of 0.657 and an R square of 0.431. This shows that the advisory for Website Applications had a positive and significant effect on the Website Application attacks in Kenya. This means that cyber security as measured by Website Application Advisory can detect this kind of cyber threat. It shows that 43.1% of the changes in Website Application Attacks Cyber-attacks are explained by cyber security detection and advisory.

The fourth indicator in this study was shown by pairing the System Vulnerability advisory and the actual System Vulnerability Attacks. The model summary for the findings is shown in Table 5 below.

Table 5: Model Summary for System Vulnerabilities

Model Summary

Model	R	R Square	Adjusted R Square	Std. The error of the Estimate
1	.902^a	.813	.751	98589660.05488

a. Predictors: (Constant), SYSADV

Source: Research Findings 2023

Table 5 shows an R of 0.902 and an R square of 0.813. This shows that the advisory for System Vulnerability had a positive and significant effect on the System Vulnerability attacks in Kenya. This means that cyber security as measured by System Vulnerability Advisory can detect this kind of cyber threat. It shows that 90.2% of the changes in System Vulnerability Attacks Cyber-attacks are explained by cyber security detection and advisory.

To measure the combined effect of cyber security advisory and the combined fraud curbing as measured by cyber security attacks, the study paired the composite cyber security advisory and the composite cyber-attacks. The model summary for the findings is shown in Table 6 below.

Table 6: Model Summary for the Composite Effect of Cyber Security Advisory and Fraud Detections

Model Summary

Model	R	R Square	Adjusted R Square	Std. The error of the Estimate
1	.979[a]	.958	.945	59545134.45420

a. Predictors: (Constant), COMPOADV

Source: Research Findings 2024

Table 6 shows an R of 0.979 and an R square of 0.958. This shows that the advisory for composite cyber security had a positive and significant effect on curbing fraud as measured by the composite cyber-attacks in Kenya. This means that cyber security as measured by composite cyber security Advisory can detect this kind of cyber threat. It shows that 95.8% of the changes in incidences of fraud as measured by the composite Cyber-attacks are explained by cyber security detection and advisory.

To test the suitability of the model for predicting the dependent variables the study did an ANOVA, the results are shown in Table 7 below.

Table 7: ANOVA of Cyber Security and Fraud Curbing

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	245101592898262304.000	1	245101592898262304.000	69.128	.004[b]
	Residual	10636869111507542.000	3	3545623037169180.500		
	Total	255738462009769856.000	4			

a. Dependent Variable: COMPCRE

b. Predictors: (Constant), COMPOADV

Source: Research Findings 2024

Table 7 shows the computed F values and the p-value. The calculated value of F (1,3) = 69.128; p-value = .004). Using the p-value to check the model's fitness, showed that the predictor variable (cyber security advisory) and the dependent variable (fraud curbing) were fit for analyzing the relationship between the dependent and independent variables since the p-value obtained of 004< 0.05.

Table 8: Coefficients of Cyber Security and Fraud Curbing

Coefficients[a]

		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	t	Sig.
1	(Constant)	108014337.973	33789298.061		3.197	.049
	COMPOADV	39.527	4.754	.979	8.314	.004

a. Dependent Variable: COMPCRE

Source: Research Findings 2024

Table 8 shows the regression model coefficients for the relationship between Cyber Security and Fraud Curbing. The study findings showed a positive relationship between the advisories given and the fraud detections made. This is represented by the model *Y= 108014337.973+39.527X.* where Y stands for the detections and X is the number of cyber security advisories issued. The model shows that as more and more investments are made in cybersecurity to provide the advisories, the more fraud detection.

4.3. Forensic Accounting Techniques and Fraud Detections.

The data for the detection of fraud in the finance sector using the proxies for forensic accounting; techniques of suspicious activities monitoring, routine internal audits, tip-offs, and fraud risk management methods are shown in Table 9 below. The proxies were assigned weights using the percentages of the detection rates for 2020 as the average base.

Table 9: Detections of Fraud by Forensic Accounting Techniques

Forensic Accounting Techniques	Percentage of Detections	Weightage
Suspicious Activities Monitoring	12	0.12
Routine Internal Audits	10	0.10
Tip-offs	10	0.10
Fraud Risk Management	8	0.08
Total	**40**	**0.40**

Source: PWC's 2020 Global Economic Crime and Fraud Survey

Table 1 above shows that 12% of fraud detections were made through Suspicious activity monitoring which has been assigned the weight of 0.12. The routine internal audits had a detection of 12% and were assigned a weight of 0.1 which was the same weight assigned to the detections through tip-offs. Detection through Fraud Risk Management was assigned 0.08. These gave a combined total percentage of fraud detections of 0.4 the detections. This was therefore used as the indicator for forensic accounting techniques in the study.

4.4. Integrating Cyber Security into Forensic Accounting

The integration of forensic accounting and forensic accounting involved bringing together the two approaches to work together in the financial sector.

First, the percentages of the detection rates of various forensic accounting detections were converted into weights as shown in Table 9 above, then they were integrated by multiplying with the cyber security's R^2 as shown in Table 10 below.

Table 10: Integration of Forensic Accounting Techniques and Cyber Security

Forensic Accounting Techniques	Weightage (X)	Cyber Security R^2	Integrated data ($X*R^2+X$)
Suspicious Activities Monitoring	0.12	0.958	0.23496
Routine Internal Audits	0.10	0.958	0.1958
Tip-offs	0.10	0.958	0.1958
Fraud Risk Management	0.08	0.958	0.15664
Total	**0.40**		**0.7832**

Source: Research Findings 2024

Table 10 above shows that by multiplying the individual weights by the composite $R^{2\ of}$ 0.958, the integrated results show an improvement in the forensic accounting techniques indicators. Suspicious activity monitoring improved from 0.12 to 0.23496, routine internal audits improved from 0.10 to 0.1958, the same as the tip-offs while fraud risk management rose from 0.08 to 0.15664. The total of the four proxies of forensic accounting techniques added up to 0.7832, which showed that cyber security had a positive and significant effect on the relationship between the two.

this therefore resulted in the model of $Y = (X_1*R^2+X_1) + (X_2*R^2+X_2) + (X_3*R^2+X_3) +(X_4*R^2+X_4)$ being given as:

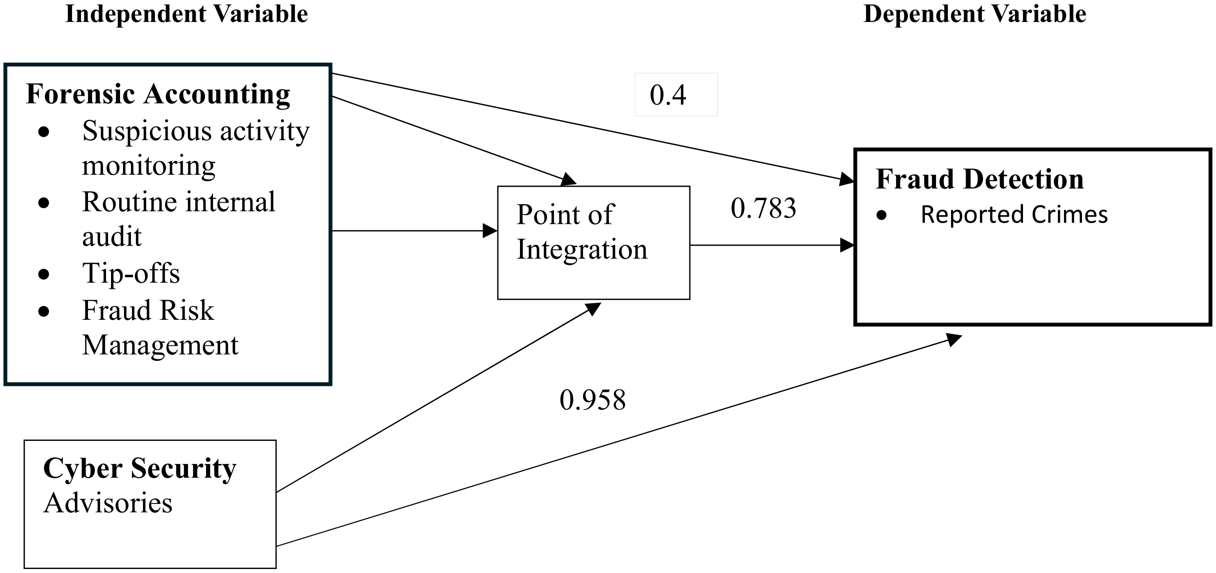
$$Y = (0.12*0.958+ 0.12) + (0.10*0.958 +0.1) + (0.1*0.958+0.1) + (0.08*0.958+0.08)$$
$$= 0.7832$$

The above model shows that an integration of cyber security and forensic accounting has a positive and significant effect on fraud detection.

5. The Resulting Conceptual Frame

Figure 1 below shows the correlation between forensic accounting techniques and the level of Fraud Detection after the integration of forensic accounting and Cyber Security.

Figure 1: Conceptual Framework



Source: Author 2024

Figure 1 above shows the integration to enhance fraud detection. In the model, Cyber forensic accounting is measured by suspicious activity monitoring with an index of 0.12, routine internal audits with an index of 0.10, tip-offs with an index of 010, and fraud risk management with an index of 0.08. giving a combined index of 0.4. Cyber security is measured by the number of advisories that had an index of 0.958. Fraud Detection was represented by the number of reports. After the integration of the two, the detection index for Forensic Accounting rises to 0.7832 thus showing that integration of Forensic Accounting and Cyber Security has a positive effect on fraud detection.

6. Conclusion

The objective of the study was to analyze the effect of integrating cybersecurity into forensic accounting techniques in enhancing fraud detection in the financial sector in Kenya. The study findings showed that there was a correlation between cybersecurity and curbing fraud as indicated by the number of advisories and the number of attacks for four different threats; Malware, System Vulnerability, Botnet/DDoS2, and Website Application. Further, the model summary for the four indicators and their composite showed that cyber security positively and significantly affected the curbing of fraud as measured by cyber security attacks. Similar results were obtained by Moid, S. (2018) who studied Fighting Cyber Crimes Using Forensic Accounting: this therefore led to the conclusion that cybersecurity positively and significantly affected fraud detection at an r of 0.958.

On the other hand, a consideration of the effect of the four forensic accounting techniques (suspicious activity monitoring, routine internal audit, tip-offs, and fraud risk management) on fraud detection showed a composite index of an r of 0.4 which showed a weak positive relationship. From the above findings, the integration of cybersecurity into the relationship led to the rise of the r for forensic accounting techniques from 0.4 to 0.7832. this therefore led to the conclusion that the integration of cyber security enhanced fraud detection by forensic accountants. The conclusion therefore is integration of Cybersecurity into forensic accounting positively and significantly influenced the effectiveness of forensic accounting techniques in the detection of fraud.

7. Recommendations

The study findings showed that cyber-security was effective in detecting cyber-attacks and curbing fraud with an index of 0.958. The switch of banking activities from conventional banking hall services to Internet and mobile banking increased the intensity and severity of cyber security threats. The use of conventional forensic accounting techniques in the detection of fraud in the banking sector is not sufficient to meet the current challenges. In the light of this, the study made the following recommendations:

1. Universities and Colleges to integrate cyber security training into forensic accounting curricula to give

birth to cyber security forensic accounting. This will equip learners in the field of accounting and forensic accounting with skills in both cybersecurity and conventional accounting and auditing skills to combat fraud.

2. The currently working accountants and forensic accountants be exposed to cyber security through training. This will equip them with cybersecurity skills to enable them to cope with the ever-evolving cybersecurity threats in the financial sector and curb fraud.
3. Policy makers and key decision makers to formulate policies that will foster the integration of forensic accounting and cybersecurity.
4. Future researchers to explore the effect of the integration of forensic accounting techniques and cybersecurity on fraud detection in other sectors of the economy such as manufacturing and government institutions

References

Aviva plc Annual Report and Accounts 2021

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 9(1), 70-104.

Ezejiofor, R. A., Nwakoby, N. P., & Okoye, J. F. (2016). Impact of Forensic Accounting on combating fraud in the Nigerian banking industry. International Journal of Academic Research in Management and Business, 1(1), 1-19.

Hossain, M. Z. (2023). Emerging Trends in Forensic Accounting: Data Analytics, Cyber Forensic Accounting, Cryptocurrencies, and Blockchain Technology for Fraud Investigation and Prevention. *Cyber Forensic Accounting, Cryptocurrencies, and Blockchain Technology for Fraud Investigation and Prevention (May 16, 2023)*.

Law, C. (2011). Journal of Digital Forensics, Security and Law, Vol. 6 (3).

McGuire, M., & Dowling, S. (2013). Cybercrime: A review of the evidence. Summary of key findings and implications. Home Office Research report, 75, 1-35.

Moid, S. (2018). Fighting Cyber Crimes Using Forensic Accounting: A Tool to Enhance Operational Efficiency. Wealth: International Journal of Money, Banking &amp; Finance, 7(3).

Mosoti, J., Wafula, J., & Nyangau, A. (2023). Fraud risk management and financial performance of microfinance institutions in Kenya. *International Journal of Research in Business and Social Science (2147-4478)*, *12*(10), 257-262.

Okoye, E. I., Adeniyi, S. I., & James, O. N. (2019). Effect of forensic accounting on fraud management on selected firms in Nigeria. International Journal of Economics, Business and Management Research, 3(12), 149-168.

Prasanthi, B. V. (2016). Cyber forensic tools: a review. International Journal of Engineering Trends and Technology (IJETT), 41(5), 266-271

PWC (2020), Global Economic Crime and Fraud Survey-Kenya Report

PwC (2016). Banking in Africa matters – African Banking Survey. Global Fintech Report, 1-100, [Online] Available at www.pwc.org, [Accessed: March 2021].

Rayaan, B., Samsudin, R.S., Che-Ahmed, A., & Popoola, O.M.J. (2016). The Moderating Role of Capability Element of Fraud on Internal Industry Factors and Fraud Prevention in Saudi Arabian Banking Sector. International Conference on Accounting Studies (ICAS), 1-9,

Tonellotto, M. (2020). Crime and victimization in cyberspace: a socio-criminological approach to cybercrime. In Handbook of Research on Trends and Issues in Crime Prevention, Rehabilitation, and Victim Support (pp. 248-264). IGI Global.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425-478.

Venkatesh, V., Thong, J. Y., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems*, *17*(5), 328-376.

Appendices

Appendix 1: Number of Cybersecurity Advisory

Type of Advisory	**Number of Advisories**				
	2018	**2019**	**2020**	**2021**	**2022**
Malware	5,452	5,951	5,810	193,595	283,101
Botnet/DDoS2	563	1,568	1,128	84,087	96,262
Website application attack	1,213	1,509	1,281	80,035	112,183
System vulnerabilities	14,360	43,034	72,076	7,615,412	13,255,964
Total	**21,588**	**52,062**	**80,295**	**7,973,129**	**13,747,510**

Source: Communication Authority of Kenya

Appendix 2 Reported Online Crimes

	Number of Reported Crimes				
Type of Crime	**2018**	**2019**	**2020**	**2021**	**2022**
Malware	1,18,233,047	85,416,510	124,168,113	181,879,153	163,880,687
Botnet/DDoS2	3,389,880	4,407,478	4,060,899	92,108,268	82,742,427
Web Application Attacks	3,842,609	10,284,596	11,589,947	7,033,604	1,000,284
System vulnerabilities	9,477	93,398	114,675,	58,045612	452,412,495
Total	**, 25,475,013**	**100,201,982**	**139,933,634**	**339,066,637**	**700,035,893**

Source: Communication Authority of Kenya