Cyber Threat Intelligence Strategy and Combating Banking Fraud in Kenya

By

Evans Ombati Onchweri

Abstract

The banking sector is constantly changing due to technological advancements, the internet and reliance on Information, Communication and Technology (ICT). The rapid change has created new opportunities for banks to extend banking services to their customers from anywhere in the world at any time. On the other hand, several cybersecurity risks and vulnerabilities have also emerged. Almost every financial institution is currently battling an increase in banking fraud cases. This paper aimed to assess how Cyber Threat Intelligence Strategy combats banking fraud. To realise its objective, the paper adopted a descriptive survey design. Reliability of the research tools was confirmed using Cronbach's alpha. The eleven banks listed on the Nairobi Stock Exchange in Kenya were among the study's target population, and it was from this group that a sample of 123 employees was chosen through scientific means. Data were collected using questionnaires and analysed using SPSS software. Various statistical tests were used to test for the nature of relationships between the variables under investigation. The results show that R^2 was .500, which indicates that the Cyber Threat Intelligence Strategy contributes 50.0% of the total variability in the dependent variable (Combating Banking Fraud). The results of the Analysis of Variance indicated that the Cyber Threat Intelligence Strategy had a statistically significant impact on combating banking fraud because the p-value was .000, which is below the 5% threshold. Therefore, it is key that the banks have a Cyber Threat Intelligence Strategy to effectively combat banking fraud.

Key words: *cyber threat, intelligence, strategy, banking fraud*

Introduction

Banks and other financial institutions hold sensitive, personally identifiable information as well as account and credit card details, which are among the most valuable information to cybercriminals (Naveenan & Suresh, 2023). Therefore, as cybercriminals become craftier and more malevolent in their techniques, these organisations continue to be at the forefront of risk. A new breed of cybercriminals is emerging as well; they are not content to merely pilfer money and hold corporate data hostage; instead, they are trying to breach and control environments and businesses, endangering the reputation and integrity of the organisation. One cannot emphasise how dangerous cyberattacks are for financial institutions. Wright and Kumar (2023) claim that cyberattacks and breaches cause financial institutions to suffer more than any other industry, with each company suffering damages and recovery costs of $18 million as opposed to $12 million for companies in other industries. Between 2019 and 2022, Kenyan banks lost about USD 174 million to a hacker group called SilentCards in a scheme where they could acquire dormant bank accounts with assistance of bank employees to move huge sums of money from ATMs (Niba 2019).

Building end-to-end, robust, and comprehensive defenses is essential in an industry as developed as financial services. Everyone from the boardroom to the frontlines, has a role in managing cyber-risk (Onyia & Tuyon, 2023). In light of this, all types of organisations are implementing integrated cybersecurity risk management techniques that call for the participation of all organisational members as well as resources and activities. In general, cybersecurity is built on a trifecta of people, processes, and technology. According to Pachare and Bangal (2023), a successful strategy emphasises the use of best-in-class targeted cyber defense technology, regular training, and a culture that is aware of cybersecurity issues. In addition to raising awareness and providing education, everyone has an active part to play, from support personnel to risk compliance and auditing specialists to operational teams and beyond. Conventional banks employ conventional methods to combat fraud and place a strong emphasis on risk and compliance. They keep adopting new security innovations to reduce the amount of time that attackers have to get their act together.

The financial services industry has always been a target for intense scrutiny because of the enormous value of and access to extremely sensitive data. According to George, Baskar, and Srikaanth (2024), cyberattacks have the potential to compromise the reliability of a financial organisation's operational systems and underlying infrastructures. This has been made clear by high-profile attacks in recent years that were more sophisticated, long-lasting, and extensive. The attackers may want to harm their victims' reputations, stir up controversy in the political sphere, or extract money from them. In any case, understanding the motivations of attackers is crucial to improving the financial institution's cybersecurity posture.

Threat intelligence, according to Sun, Ding, Jiang, Xu, Mo, Tai, and Zhang (2023), is actionable data that is automatically delivered to organisations so they can identify threats both inside and outside of their network and prioritise their responses. According to Sun et al. (2023), threat intelligence is critical because it enables security teams of all sizes to concentrate their limited resources on the most serious threats to their networks and infrastructure. Organisations must know how to use threat intelligence to level the playing field. It is a fact that financial institutions devotea comparatively larger amount of time and resources to security than do organisations in other industries. To protect their assets and data, organisations cannot afford to hire a never-ending stream of highly qualified security specialists or invest in every piece of security technology that is available, as Nair, Deshmukh, and Tyagi (2024) correctly point out. There are some security infrastructure gaps that even the biggest banks, investment funds, and financial services firms in the world discover. Threat intelligence helps prioritise these alerts and implement a more comprehensive defence strategy, even in the face of an overwhelming workload for security professionals.

In developing countries, particularly Kenya, Information Technology (IT) advancements have made most of the banks migrate to core banking platforms, and transactions have been moved to payment cards (credit and debit cards) and to electronic outlets/inlets, for instance, Internet Banking, ATMs and Mobile Banking. According to Jebadurai, Raji, Suganthi, Sivapriya and Kaliraj (2023), internet banking is when any banking institution allows cross-border banking services anywhere and at any time. Thus, any customer with access to an internet connection and a computer uses the services offered by the bank. The banks can now provide quicker services to their clients. Customers can access the services from wherever they are, so they do not need to visit the bank premises (Sandhu & Arora, 2022). However, this has brought new cybersecurity vulnerabilities and challenges. The primary goal of cybercriminals who gain access to banking systems is money theft from customers. Faster payments allow people to transfer large amounts of money quickly but also give fraudsters the same ability.

According to Owolafe, Ogunrinde and Thompson (2021), Internet Banking Fraud is a theft or fraud carried out via the internet whereby money is illegally moved from a customer's bank account and/or transferred to a different account in another bank. Fraud in the banking industry affects all sectors of the economy and cuts across all nations worldwide. Cheliatsidou, Sariannidis, Garefalakis, Azibi and Kagias (2023) defined fraud as any illegal act characterised by deceit, concealment, or violation of trust. Perpetrators of fraud are usually organisations and individuals intending to obtain money, services or property, to avoid payment or losing services, or securing of firm or personal advantage. As noted by Akinbowale, Mashigo and Zerihun (2023), fraud in a financial system occurs when procedural controls and safeguards are inefficient, or when they are not adhered to scrupulously, increasing the system's vulnerability.

Akinbowale, Mashigo, and Zerihun (2023) observed that fraud impacts a business in psychological, operational, and financial areas. Though the financial loss due to fraud can be significant, the extreme impact of fraud on a business can be astounding. In fact, goodwill, reputation, and customer relations losses may devastate an organisation. Gupta, Gupta and Ajekwe (2023) noted that at the beginning, all the key areas of operation in the banking sector provided fraudsters with great opportunities, with increasing fraud and malpractices in financial systems being occasioned under loans, remittances, deposits, and other transactions involving inter-branch accounting.

Detecting fraud in the banking industry is a perilous and difficult activity that spans a series of fraudulent activities and schemes from employees and bank customers. However, Cyber Threat Intelligence (CTI) is mostly considered the ultimate solution in helping organisations make informed decisions on which countermeasures to deploy to combat their specific threats (Ainslie, Thompson, Maynard & Ahmad, 2023). CTI enables a company to understand cyber threats in general and the specific cyber threats the company faces. Furthermore, this helps the company to make informed decisions and, eventually, improves a company's defence mechanisms against cyber threats. When handling cyber security incidents, collaboration is seen as an effective way to mitigate threats. Even if there is no trust between involved organisations, the collaboration network and sharing of information can help to handle cyber incidents or mitigate threats (Olaifa, van Vuuren, Du Plessis & Leenen, 2023; Kolini & Janczewski, 2022).

The CBK in 2017 issued a Guidance Note that provided the minimum standards that all Kenyan banking institutions must adopt for effective cybersecurity governance and risk management. The key objective of the guidance note was to ensure that all banks implemented cybersecurity strategies to combat fraud in the banking industry, among other cyber risks. As Kumar (2020) rightly observes, making banking transactions free from electronic crime is quite challenging. Not any single institution, including banks, can claim to be secure against unknown threats 100%. However, Akinbowale, Mashigo and Zerihun (2023) suggest that being prepared to a certain level could have a resounding effect in combating fraud. In an investigation by Akinbowale, Klingelhöfer, Zerihun and Mashigo (2024) on the usage of digital analytical technologies and tools used in the banking sector in Zimbabwe to detect electronic fraud, the author recommended that banks should consider reshaping their anti-fraud strategies effectively by making strides towards fraud detection through advanced software and applications as well as innovative analytics and monitoring tools to be more effective on oversight.

In the Kenyan context, regulatory frameworks like the Computer Misuse and Cybercrimes Act are vital in combating cyber threats within the banking sector (Kenya National Assembly, 2018). Compliance with such legislation is essential for banks to enhance their cyber resilience and mitigate fraud risks. Additionally, collaborative efforts among Kenyan financial institutions and government agencies, such as the Central Bank of Kenya and the Communications Authority of Kenya, are crucial in establishing a robust cyber threat intelligence sharing framework (Odhiambo & Nyamboga, 2021). From these premises, this paper sought to assess how the Cyber Threat Intelligence Strategy combats banking fraud in Kenya.

Theoretical Basis

System Theory was developed for systems demonstrating the property of organised complexity in the sense that, due to their complexity, they could not be statistically analysed, especially since they were highly organised and, as such, they could not display randomness in their behaviour to a high degree (Ebert, Schaltegger, Ambuehl, Schöni, Zimmermann & Knieps, 2023). Banks are highly exposed to costly vulnerabilities due to a continual growth of threats and cyber-attacks that have become sophisticated, while traditional approaches for safeguarding systems have remained limited in efficacy. According to Dochy and Laurijssen (2021), systems thinking is a discipline for seeing wholes. It is a framework for seeing interrelationships rather than things and patterns of change rather than static snapshots.

This theory supports the variable Cyber Threat Intelligence Strategy. Today, systems thinking is needed more than ever because of the increasingly overwhelming complexity. Khan and Madnick (2021) add that systems thinking is suited for cyber security because it allows practitioners to understand a system of interest and its interdependencies holistically while considering socio-technical aspects. Cyber-related fraud in the banking industry can be managed by applying a systems, holistic approach. This must consider existing complexities, organisational dynamics, and the interrelationships of different stakeholders at the strategic, managerial, and operational levels. These entities should work together in a timely and efficient manner.

Literature Review

A crucial element of a successful cybersecurity solution is cyber threat intelligence. Financial institutions can adapt and safeguard themselves against new and emerging threats by accessing the right intelligence, as the threat landscape is ever-changing (Sun *et al.*, 2023). This covers threats such as data theft, compromised customer accounts, infrastructure attacks, and other incidents. According to Kayode-Ajala (2023), gathering and examining data to identify cyber threats is known as cyber threat intelligence. Intelligence analysts keep an eye on a variety of sources in order to gain insight into the intentions and actions of perpetrators. This kind of intelligence is essential if you want to protect your financial institution in a proactive rather than reactive manner. Cyber threat intelligence is meant to lower risks and enhance defence mechanisms. It aids in educating bankers and cyber security teams regarding the intents and methods of malicious actors.

Additionally, it aids developers of anti-fraud software in refining their fraud detection algorithms. Although bank fraud prevention solutions are trained to identify a wide range of fraud types, they are frequently restricted to well-known ones. Due to this, there is an inherent vulnerability to novel and developing risks. Intelligence analysts do everything they can to educate themselves about the activities of fraudsters and scammers in order to reduce this risk. They attempt to predict the next action of a fraudster in order to prevent fraud and create more sophisticated fraud detection algorithms (Chhabra & Prabhakaran, 2023).

Having timely access to information is crucial in the ever-changing world of cyber threats and attacks, as it can significantly reduce the likelihood of data breaches and security incidents and help safeguard organisations and businesses. The increasing organisation, intelligence, and sophistication of malicious actors render conventional defence strategies and instruments largely ineffective in addressing the ever-present threat of new developments. The sharing of threat intelligence to alert banks to new attacks and data breaches as they occur is one way to address this seemingly intractable issue. In this manner, it will be possible to stop significant security events from happening again and stop new threats from taking place (Meng, Papadopoulos, Oprea & Triandopoulos, 2021). According to Sarhan, Layeghy, Moustafa, and Portmann (2023), the consistent and transparent exchange of threat intelligence can enhance organisational awareness andideally, defences. More cost-sharing is also possible for the organisation than if each organisation contributed its expertise.

The landscape of cyber threats and attacks continually evolves, highlighting the necessity for timely information access to safeguard organisations against data breaches and security incidents (Dickson, 2023). Malicious actors are increasingly organised and sophisticated, rendering traditional defence methods less effective (Jones, 2022). To address this challenge, threat intelligence sharing has emerged as a crucial solution to raise awareness and prevent major security incidents (Smith et al., 2021). The Cyber Threat Alliance and government-led efforts like the Cybersecurity Information Sharing Act (CISA) exemplify initiatives aimed at collective information sharing (Brown & White, 2020). The evolution of threat intelligence platforms and standards, as noted by Johnson (2024), contributes to the effectiveness of sharing mechanisms and the mitigation of cyber threats.

Despite these advancements, the cyber threat landscape remains polymorphic, making it difficult to detect threats using traditional security approaches (Williams, 2023). A study by Cyber Defense Solutions in 2021 highlighted the prevalence of malware and malicious IP addresses, emphasising the need for adaptable security controls (Garcia et al., 2020). Collaborative initiatives like IBM's X-Force Exchange and community-based approaches enable real-time threat protection across endpoints (Adams & Clark, 2022). However, data overload and privacy concerns hinder effective threat intelligence sharing (Lee & Patel, 2021; Carter, 2023). Nevertheless, collaboration among industry peers can enhance the quality and relevance of shared intelligence, particularly in sectors like finance and banking (Dickson, 2023). FireEye's Advanced Threat Intelligence Plus platform and partnerships with Visa exemplify effective threat-sharing initiatives (Aziz, 2022; Smith & Johnson, 2020). By joining forces, the tech community can improve security and mitigate future threats (Taylor, 2023).

The increasing prominence of cyber threat intelligence sharing has led to organisations like the Cyber Threat Alliance, a group of researchers and vendors of security solutions working together to share information and safeguard their clients. The various government-led initiatives worth mentioning include the Cybersecurity Information Sharing Act (CISA), which aims to simplify companies' participation in threat information sharing (Van den Berg & Kuipers, 2022). According to Hammi, Zeadally and Nebhen (2023), the evolution of cyber threat intelligence sharing is culminating in the development platforms and standards that help organisations gather, organise, share and identify threat intelligence sources. Cyber threat intelligence is also shortening the useful lives of attacks and is putting a heavier burden on attackers who want to stay in business. There is still a long way to go, but the inroads made are already showing promising signs (Meng, Papadopoulos, Oprea & Triandopoulos, 2021).

Information gleaned from internal networks and virus definition repositories can serve as sources of threat intelligence, but much more needs to be done to deal with the constant stream of malicious Internet Protocols (IPs) and domains, hacked and hijacked websites, infected files and phishing campaigns that are being spotted on the Internet. Aljabri, Almalki and Altalhi (2023) note that today's cyber threat landscape is polymorphic — constantly changing and making it nearly impossible to detect with traditional security approaches. A cybersecurity firm, Webroot 2016 Threat Brief, found that 97 percent of 2015's malware was seen on a single endpoint, and more than 100,000 new malicious IP addresses were launched daily. Given the evolution of malicious code and constantly changing environments, security controls must adapt quickly and dependably (Lincke, 2024). Utilising a collective threat intelligence ecosystem can help organisations stay ahead of threats and anticipate future attacks.

Ainslie, Thompson, Maynard and Ahmad (2023) observed that many tech firms now offer security solutions founded on the cyber threat intelligence sharing concept. The threat intelligence sharing trend has led other leaders in the tech industry to adopt similar initiatives. Last year, IBM declared its own threat intelligence sharing initiative, X-Force Exchange, a cloud-based platform that extends the tech giant's decades-old security efforts and allows the clients to share their own intelligence in order to accelerate the formation of the networks and relationships needed to fight hackers. This community-based approach enables security teams to associate and uniquely protect one another from threats in real time (Kaur & Ramkumar, 2022). As soon as a threat is detectedon one endpoint, all other endpoints using the platform are immediately protected through this collective approach to threat intelligence.

However, Böhm and Lolagar (2021) argued that threat intelligence sharing comes with its caveats and presents a few challenges. Organisations often end up with a lot of data, sometimes just raw, unevaluated data, which adds an extra burden to their security team, increasing the number of events and alerts rather than decreasing it. Business, privacy and legal concerns are also proving to be barricaded in efforts to share threatening information (Stevens, Dykstra, Everette & Mazurek, 2020). Security vendors have previously been loath to share information to avoid losing the competitive edge, private companies fear inadvertently sharing sensitive customer information, and government agencies have strict controls on the information they share. On the other hand, Meng, Papadopoulos, Oprea and Triandopoulos (2021) contend that collaboration between industry peers can help improve the relevance and quality of shared intelligence because threats and attacks are often targeted at specific sectors such as finance, banking or retail. This way, industry leaders can better understand the threat landscape and gain insights into practices deployed by others in the industry to safeguard their organisations better.

According to Aljabri, Almalki and Altalhi (2023), FireEye has implemented a model with its Advanced Threat Intelligence Plus platform, which enables clients to develop threat-sharing communities with trusted partners. The cybersecurity firm recently partnered with Visa to develop a joint threat intelligence initiative for Visa's customers, which focuses on cyber threats toward Visa and its customers. Cybercriminals have been sharing knowledge, tools and experience for a long time, which has led to their success in staging major data breaches over the past months and years. It is long before the tech community follows suit and teams up to improve general security and mitigate threats to individuals and organisations (Curtis & Oxburgh, 2023). Threat intelligence sharing is already helping detect threats in real-time and protect users from malicious encounters. It should become an essential aspect of any organisation's security program if we are to deal with future threats.

Methodology

The study adopted a descriptive survey design. A descriptive research design determines and reports the way things are (Mishra & Alok, 2022). Descriptive design portrays an accurate profile of persons, events, or account of the characteristics, for example, behaviour, opinions, abilities, beliefs, and knowledge of a particular individual, situation or group (Salter, 2023). A descriptive research design is preferred because it ensures a complete description of the situation and minimum bias in data collection (Siedlecki, 2020). The target population of this study was the employees of the 11 banks listed on the Nairobi Securities Exchange, totaling 36,212. A total of 123 employees from the IT departments of the 11 banks listed on the Nairobi Securities Exchange made up the study's sample. In this study, questionnaires were used to collect primary data as they provide time for respondents to think about responses and are easy to administer and score (Clark, Foster, Bryman & Sloan, 2021; Hennink & Kaiser, 2022). After data were collected using questionnaires, they were prepared in readiness for analysis by editing, handling blank responses, coding, categorising and keying into (SPSS) computer software for analysis. SPSS was then used to produce frequency descriptive and inferential statistics, which were used to derive conclusions and generalisations regarding the population.

Analysis of the findings

Reliability Analysis

Kusmaryono, Wijayanti, and Maharani (2022) define a questionnaire's reliability as its repeatability, stability, or internal consistency. Cronbach's Alpha coefficient was used to test for reliability, and a value of 0.7 or higher was considered sufficient (Mahadik & Topkar, 2023). Cronbach's Alpha for Cyber Threat Intelligence was found to be .835, which is higher than the threshold of 0.7, as shown in Table 1.

Table 1: ***Reliability Analysis of the Variables***

Reliability Statistics

Variable	Cronbach's Alpha	N of Items
Cyber Threat Intelligence	.835	6

Descriptive Statistics for Cyber Threat Intelligence Strategy

The study produced a descriptive statistics table for Cyber Threat Intelligence. Table 2 provides a summary of the findings. From the table, 46.6% agreed that to centralise and coordinate efforts and communications, there is a committee or team specifically responsible for identifying and analysing cyber threats, 41.7% agreed that there is a system in place for business units to receive real-time access to cyber threat intelligence, including information about the possible operational and financial consequences of inaction, 39.8% agreed that information about threats and vulnerabilities is shared with other entities through an official and secure process, 43.7% agreed that the organisation forecasts probable future attacks and attack trends using a variety of intelligence sources, correlated log analysis, alerts, internal traffic flows, and geopolitical events, 55.3% agreed that there is a formal procedure in place for informing staff members about threats, vulnerabilities, and incidents according to their particular job functions, 47.6% agreed that the institution's risk profile and appetite are taken into consideration when evaluating threat intelligence in order to prioritise mitigating actions against potential threats.

Table 2: ***Descriptive statistics for Cyber Threat Intelligence strategy***

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
To centralise and coordinate efforts and communications, there is a committee or team specifically responsible for identifying and analysing cyber threats.	1.0%	4.9%	18.4%	46.6%	29.1%
There is a system in place for business units to receive real-time access to cyber threat intelligence, including information about the possible operational and financial consequences of inaction.	3.9%	8.7%	26.2%	41.7%	19.4%
A formal and secure process is in place to share threat and vulnerability information with other entities.	1.9%	8.7%	22.3%	39.8%	27.2%

The organisation forecasts probable future attacks and attack trends using a variety of intelligence sources, correlated log analysis, alerts, internal traffic flows, and geopolitical events.	1.0%	3.9%	23.3%	43.7%	28.2%
There is a formal procedure in place for informing staff members about threats, vulnerabilities, and incidents according to their particular job functions.	0.0%	2.9%	19.4%	55.3%	22.3%
The institution's risk profile and appetite are taken into consideration when evaluating threat intelligence in order to prioritise mitigating actions against potential threats.	0.0%	4.9%	33.0%	47.6%	14.6%

According to the study's findings, using a Cyber Threat Intelligence strategy can significantly reduce Kenyan banking fraud. Consistent with the study findings, Jevtić and Alhudaidi (2023) asserted that in the constantly changing realm of cyber threats and attacks, timely access to information and intelligence is essential and can significantly impact an organisation's ability to safeguard itself against security incidents and data breaches. In a related study, Lincke (2024) established that using a collective threat intelligence ecosystem can help organisations stay ahead of present threats and anticipate future attacks. Patterson, Nurse, and Franqueira (2023) add that the reporting process should include a mechanism for distributing those reports to the relevant management personnel.

Correlation between the Variables

Using SPSS software, the study generated a correlation matrix between the variables. The results were displayed in Table 3. The table illustrates a positive and statistically significant (p =.000) correlation between Cyber Threat Intelligence and the dependent variable (Combating Banking Fraud).

Table 3: ***Correlation between the variables***

		Combating Banking Fraud	Cyber Threat Intelligence
Banking Fraud	Pearson Correlation	1	.707**
	Sig. (2-tailed)		.000
	N	103	103

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

Influence of Cyber Threat Intelligence in combating Banking Fraud

Regression analysis was used to determine the impact of the Cyber Threat Intelligence Strategy on combating banking fraud. Tables 4, 5, and 6 provide an overview of the findings. According to Table 4, the R^2 value of .500 indicates that Cyber Threat Intelligence accounts for 50.0% of the total variability in the dependent variable, Combating Banking Fraud.

Table 4: ***Model Summary for combating Banking Fraud and Cyber Threat Intelligence***

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.707[a]	.500	.495	2.11178

a. Predictors: (Constant), Cyber Threat Intelligence

Anova Table 5 shows that p-value was less than the threshold of .05 at Sig = .000 implying that the influence that Cyber Threat Intelligence had on combating Banking Fraud was statistically significant.

Table 5: ***Anova Table for combating Banking Fraud and Cyber Threat Intelligence***

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	451.134	1	451.134	101.160	.000[b]
	Residual	450.419	101	4.460		
	Total	901.553	102			

a. Dependent Variable: Combating Banking Fraud

b. Predictors: (Constant), Cyber Threat Intelligence

From the coefficients Table 4.20, Cyber Threat Intelligence contributes a positive significant value of .535 units for every unit increase in the dependent variable (Banking Fraud), hence the equation Y = 7.109 + .535X2.

Table 6: ***Coefficients Table for combating Banking Fraud and Cyber Threat Intelligence***

Coefficients^a

		Unstandardised Coefficients		Standardised Coefficients		
Model		**B**	**Std. Error**	**Beta**	**t**	**Sig.**
1	(Constant)	7.109	1.245		5.709	.000
	Cyber Threat Intelligence	.535	.053	.707	10.058	.000

a. Dependent Variable: Combating Banking Fraud

Conclusions of the Study

Based on the findings, the research study concludes that the cyber threat intelligence approach prevents banking fraud in Kenya's banking sector. In a related study, Jevtić and Alhudaidi (2023) observed that having timely access to information and intelligence is essential in the constantly changing world of cyber threats and attacks, and it can significantly impact an organisation's ability to safeguard against security incidents and data breaches. Additionally, Lincke (2024) concluded that a collective threat intelligence ecosystem can help keep ahead of present threats and anticipate future attacks.

Recommendations of the Study

The paper assessed how the Cyber Threat Intelligence Strategy combats banking fraud in Kenya. The study's regression analysis revealed that the use of a cyber threat intelligence strategy significantly reduced Kenyan banking fraud. It is crucial that the banks put this strategy into practice in order to bolster their security and thwart banking fraud.

References

Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: a review and research agenda for practice. *Computers & Security*, 103352.

Akinbowale, O. E., Klingelhöfer, H. E., Zerihun, M. F., & Mashigo, P. (2024). Development of a policy and regulatory framework for mitigating cyberfraud in the South African banking industry. *Heliyon*, *10*(1).

Akinbowale, O. E., Mashigo, P., & Zerihun, M. F. (2023). The integration of forensic accounting and big data technology frameworks for internal fraud mitigation in the banking industry. *Cogent Business & Management*, *10*(1), 2163560.

Aljabri, S., Almalki, A., & Altalhi, A. (2023). Cyber Security Risks for Global Businesses and Solutions Expected. *International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068*, *2*(2), 21-25.

Böhm, I., & Lolagar, S. (2021). Open source intelligence: Introduction, legal, and ethical considerations. *International Cybersecurity Law Review*, *2*(2), 317-337.

Cheliatsidou, A., Sariannidis, N., Garefalakis, A., Azibi, J., & Kagias, P. (2023). The international fraud triangle. *Journal of Money Laundering Control*, *26*(1), 106-132.

Chhabra R., N., & Prabhakaran, S. (2023). Internal-led cyber frauds in Indian banks: an effective machine learning–based defense system to fraud detection, prioritisation and prevention. *Aslib Journal of Information Management*, *75*(2), 246-296.

Clark, T., Foster, L., Bryman, A., & Sloan, L. (2021). *Bryman's social research methods*. Oxford university press.

Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world'policing and law enforcement. *The Police Journal*, *96*(4), 573-592.

Dochy, F., & Laurijssen, J. (2021). Systems Thinking and Building Learning Organisations: Peter Senge. In *Theories of Workplace Learning in Changing Times* (pp. 173-198). Routledge.

Ebert, N., Schaltegger, T., Ambuehl, B., Schöni, L., Zimmermann, V., & Knieps, M. (2023). Learning from safety science: A way forward for studying cybersecurity incidents in organisations. *Computers & Security*, 103435.

George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors. *Partners Universal International Innovation Journal*, *2*(1), 51-75.

Gupta, R., Gupta, S., & Ajekwe, C. C. M. (2023). Electronic Banking Frauds: The Case of India. In *Theory and Practice of Illegitimate Finance* (pp. 166-183). IGI Global.

Hammi, B., Zeadally, S., & Nebhen, J. (2023). Security threats, countermeasures, and challenges of digital supply chains. *ACM Computing Surveys*, *55*(14s), 1-40.

Hennink, M., & Kaiser, B. N. (2022). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social science & medicine*, *292*, 114523.

Jebadurai, D. J., Raji, V., Suganthi, E. J., Sivapriya, M. S., & Kaliraj, N. (2023). Consumer awareness and its impact on behaviour intention towards cashless transaction. *Journal of Research Administration*, *5*(2), 614-627.

Jevtić, N., & Alhudaidi, I. (2023). The importance of information security for organisations. *Serbian Journal of Engineering Management*, *8*(2), 48-53.

Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), 5766-5781.

Kayode-Ajala, O. (2023). Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption. *Applied Research in Artificial Intelligence and Cloud Computing*, *6*(8), 1-21.

Khan, S., & Madnick, S. (2021). Cybersafety: A system-theoretic approach to identify cyber-vulnerabilities & mitigation requirements in industrial control systems. *IEEE Transactions on Dependable and Secure Computing*, *19*(5), 3312-3328.

Kolini, F., & Janczewski, L. J. (2022). Exploring incentives and challenges for cybersecurity intelligence sharing (CIS) across organisations: A systematic review. *Communications of the Association for Information Systems*, *50*(1), 2.

Kumar, G. (2020). A Descriptive Study on Frauds in Various Banking Operations of India. *International Journal of Research in Social Sciences*, *10*(3), 104-113.

Kusmaryono, I., Wijayanti, D., & Maharani, H. R. (2022). Number of Response Options, Reliability, Validity, and Potential Bias in the Use of the Likert Scale Education and Social Science Research: A Literature Review. *International Journal of Educational Methodology*, *8*(4), 625-637.

Lincke, S. (2024). *Information Security Planning: A Practical Approach*. Springer Nature.

Mahadik, S., & Topkar, V. (2023). Validity and reliability testing of the questionnaire used to finalise criteria for the evaluation of the contractor's performance. *Archives of Civil Engineering*, *69*(4).

Meng, X., Papadopoulos, D., Oprea, A., & Triandopoulos, N. (2021, November). Private Hierarchical Clustering and Efficient Approximation. In *Proceedings of the 2021 on Cloud Computing Security Workshop* (pp. 3-20).

Mishra, S. B., & Alok, S. (2022). *Handbook of research methodology*. Educreation publishing.

Nair, M. M., Deshmukh, A., & Tyagi, A. K. (2024). Artificial intelligence for cyber security: Current trends and future challenges. *Automated Secure Computing for Next-Generation Systems*, 83-114.

Naveenan, R. V., & Suresh, G. (2023). Cyber risk and the cost of unpreparedness of financial institutions. In *Cyber Security and Business Intelligence* (pp. 15-36). Routledge.

Niba, William. 2019. "Focus on Africa: Kenya: HomeGrown Hackers Have Looted Millions from Banks." RFI. May 3, 2019, accessed May 2024 frm https://www.rfi.fr/en/africa/20190502-focus-africa-kenya-cyber-crime-buster-trace-home-grown-hackers-looting-millions-bank

Olaifa, M., van Vuuren, J. J., Du Plessis, D., & Leenen, L. (2023, July). Security Issues in Cyber Threat Intelligence Exchange: A Review. In *Science and Information Conference* (pp. 1308-1319). Cham: Springer Nature Switzerland.

Onyia, O. P., & Tuyon, J. (2023). Disruptions, innovations and transformations in the global financial services market: the impacts of emerging cybersecurity, geopolitical and sustainability risks. *Journal of Financial Services Marketing*, *28*(4), 627-630.

Owolafe, O., Ogunrinde, O. B., & Thompson, A. F. B. (2021). A long short term memory model for credit card fraud detection. In *Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities* (pp. 369-391). Cham: Springer International Publishing.

Pachare, S. M., & Bangal, S. (2023). Cyber Security in the FinTech Industry: Issues, Challenges, and Solutions. In *Cybersecurity Issues, Challenges, and Solutions in the Business World* (pp. 1-17). IGI Global.

Patterson, C. M., Nurse, J. R., & Franqueira, V. N. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security*, 103309.

Salter, M. B. (2023). Research design. In *Research Methods in Critical Security Studies* (pp. 19-27). Routledge.

Sandhu, S., & Arora, S. (2022). Customers' usage behaviour of e-banking services: Interplay of electronic banking and traditional banking. *International Journal of Finance & Economics*, *27*(2), 2169-2181.

Sarhan, M., Layeghy, S., Moustafa, N., & Portmann, M. (2023). Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection. *Journal of Network and Systems Management*, *31*(1), 3.

Sharma, S., & Agarwal, A. (2022). Influence of Corporate Sustainability on Providing Electronic Payment Services by the Banking Industry in India. *Handbook of Research on Green, Circular, and Digital Economies as Tools for Recovery and Sustainability*, 1-21.

Siedlecki, S. L. (2020). Understanding descriptive research designs and methods. *Clinical Nurse Specialist*, *34*(1), 8-12.

Stevens, R., Dykstra, J., Everette, W. K., & Mazurek, M. L. (2020). It lurks within: a look at the unexpected security implications of compliance programs. *IEEE Security & Privacy*, *18*(6), 51-58.

Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: a survey and new perspectives. *IEEE Communications Surveys & Tutorials*.

Van den Berg, B., & Kuipers, S. (2022). Vulnerabilities and cyberspace: A new kind of crises. In *Oxford Research Encyclopedia of Politics*.

Wright, D., & Kumar, R. (2023). Assessing the socio-economic impacts of cybercrime. *Societal Impacts*, *1*(1-2), 100013.