International Journal of Innovative Finance and Economics Research 5(4):12-22, Oct.-Dec., 2017

© SEAHI PUBLICATIONS, 2017 www.seahipaj.org ISSN: 2360-896X

Evaluation of Cybersecurity Strategies Used in Combating Banking Fraud in the Banking Industry in Kenya

[1]Onchweri, Evans Ombati, (MSc.);
[2]Tobias Mwalili, (PhD)
[3]Makori Moronge, (PhD)

[1-3]Jomo Kenyatta University of Agriculture and Technology (JKUAT), Kenya

ABSTRACT
Banking institutions are currently grappling with increased incidences of banking fraud. Accordingly, banks have implemented cybersecurity strategies with the aim of protecting their banking information and transactions from banking fraud. This study aimed at evaluating cybersecurity strategies used in combating banking fraud in the Kenyan banking industry. The study examined the existing cyber risk management and oversight strategy and cybersecurity controls strategy in combating banking fraud. Additionally, the study assessed the current cyber threat intelligence as well as cyber incident and response strategies used by the Kenyan banking sector in dealing with banking fraud.). A sample of elen banks listed in the nairobi security exhange was selected and data collected from it department of the specific banks as they are assumed to possess special knowledge and experience of implementing and managing cybersecurity strategies. From the findings, R2 was .695 meaning that all independent variables (Cyber Incident Response and Resilience, Cyber Risk Management and Oversight, Cybersecurity Controls, Cyber Threat Intelligence and Collaboration) contributes 69.5% to the total variability in the dependent variable (Combating Banking Fraud). The Analysis of Variance shows that the p-value was .000 (below the 5% threshold) and hence, the Combined Independent Variables had a statistically significant influence on the Dependent Variable. Nevertheless, on their own each strategy was found to have a significant influence in combating banking fraud in Kenya. Therefore, it is important that the banks implement each of the strategies understudy so that the strength of one strategy could compensate for weaknesses in or possible failure of another strategy. In addition, the study recommends that the banks find other strategies that are not in this study so as to take care of the remainder 30.5% which is significant percentage, especially when it is associated with the banking sector.
Keywords: Cybercrime, Cybersecurity, Cybersecurity strategy

INTRODUCTION

While through internet banking, the banks are now able to give their customers faster services, the banks have on the other hand created several cybersecurity vulnerabilities. Cyber fraudsters can access banking systems with the main aim of stealing customers money. Faster payments allow people to move significant sums instantly, but also allow fraudsters to do the same. Bhasin (2015) remarked that fraud impacts organizations in several areas including financial, operational, and psychological. While the monetary loss owing to fraud is significant, the full impact of fraud on an organization can be staggering. In fact, the losses to reputation, goodwill, and customer relations can be devastating. As fraud can be perpetrated by any employee within an organization or by those from the outside, therefore, it is important to have an effective fraud management strategies in place to safeguard an organization's assets and reputation.

In today's volatile economic environment, the opportunity and incentive to commit frauds have both increased. According to PWC (2015) instances of asset misappropriation, money laundering, cybercrime and accounting fraud are only increasing by the day. With changes in technology, frauds have taken the shape and modalities of organized crime, deploying increasingly sophisticated methods of perpetration. As financial transactions become increasingly technology-driven, they seem to have become the weapon of choice when it comes to fraudsters. Brignall (2015) opined that online bank fraud was the UK's fastest growing area of crime – doubling from £60m in

2014 to an expected total beyond £130m by 2015. A survey conducted by Deloitte (2012) showed that banks had witnessed a rise in the number of fraud incidents and the trend was likely to continue in the near future (Mwaura & Thiong'O, 2013).

In U.K, the number of phishing attacks increased by 16% from 2008 to reach 51% in 2009. As a result, online banking losses totaled almost GBP 60 million (from GBP 52.5 million in 2008 and 23.2 million in 2005) (Hong, 2012). The amount of losses through fraud cases, in E.A.C by the banks and financial institutions for a period of time of 18 months (January 2011 to June 2012) is around USD 48.3 million. These losses occurred mostly through hacking, malicious insiders (employees and outsourcing); card skimming; electronic files manipulation and IT controls circumvention. According to Klein (2015), the business firms lose 5% of revenue each year to fraud. When applied to the 2013 estimated gross world product, this revenue loss translates to a global figure of nearly USD 3.7 trillion.

The fraud incidents are on the rise year after year despite the fact that still a significant number of fraud cases are hidden by the banking sector for various reasons such as, inefficiency of the police and the judiciary system and to protect banks image and reputation (Olingo, 2014). As Pasricha and Mehrotra (2014) rightly observed, it is quite challenging to make banking transactions free from electronic crime. Although banks cannot be 100% secure against unknown threats, a certain level of preparedness can go a long way in countering fraud risk (Bhasin, 2016). Dzomira (2014) investigated the use of digital analytical tools and technologies in electronic fraud and detection used in the Zimbabwean banking industry. He concluded that banking institutions should reshape their anti-fraud strategies to be effective by considering frauds detection efforts using advanced analytics and related tools, software and application to get more efficient oversight. On this note therefore, this study sought to evaluate cybersecurity strategies used in combating banking fraud in the banking industry in Kenya.

REVIEW OF RELATED LITERATURE

Cyber Risk Management and Oversight

Assessing risk management allows management to determine the maturity of their risk identification, assessment, and mitigation process as well as the adequacy of audit's review of key controls. The assessment of resources determines if there are adequate staff and tools to adequately manage the risk environment. The organization stakeholders must determine if the Board and management have implemented policies and strategies for an effective cybersecurity program. Additionally, management must assess the institution's process for managing IT assets (Cory, n.d.). Herrygers (2016) observed that perhaps no area of risk management presents a greater challenge to boards than that of cyber risk. With the proliferation of cybercrime and recently proposed legislation related to cyber-risk reporting and disclosures, organizations are under intense pressure from stakeholders to respond to inquiries on the effectiveness of their cyber risk management programs. Even though cyber risk is on many boardroom agendas, there is a growing need for much greater transparency around an organization's cyber-risk management program.

The American Institute of Certified Public Accountants (AICPA) (2016), developed a new attestation guidance specifically focused on reporting on an entity's cyber-risk management program. The AICPA cybersecurity examination engagement was intended to expand cyber-risk reporting to address expectations of greater stakeholder transparency by providing a range of stakeholders, both internal and external, with information about an entity's cyber-risk management program effectiveness. From this, organizations may realize the following benefits; Independent and objective reporting, providing a higher degree of assurance to key stakeholders; Operational efficiencies from having a single reporting mechanism addressing the information needs of a broad range of users; Greater transparency around the effectiveness of the entity's cyber-risk management program to internal and external stakeholders (e.g., security agencies, boards, regulators, etc.); and Greater economic value for intended users of the report by obtaining information about an entity's cyber-risk management program that would be useful in making informed and strategic decisions.

Threat Intelligence and Collaboration

Threat intelligence sharing has risen in prominence, giving birth to initiatives such as the Cyber Threat Alliance, a conglomeration of security solution vendors and researchers that have joined forces to collectively share information and protect their customers. Also to be noticed are the numerous government-led efforts, such as the

Cybersecurity Information Sharing Act (CISA), which is meant to ease the way for businesses to join the threat information sharing movement (Contreras, DeNardis, & Teplinsky, 2012). According to Barnum (2012), the evolution of cyberthreat intelligence sharing is culminating in the development of platforms and standards that help organizations gather, organize, share and identify sources of threat intelligence. Cyberthreat intelligence is also shortening the useful lives of attacks and is putting a heavier burden on attackers who want to stay in business. There's still a long way to go, but the inroads made are already showing promising signs (Dickson, 2016).

In the ever-shifting landscape of cyberthreats and attacks, having access to timely information and intelligence is vital and can make a big difference in protecting organizations and firms against data breaches and security incidents. Malicious actors are getting organized, growing smarter and becoming more sophisticated, which effectively makes traditional defense methods and tools significantly less effective in dealing with new threats constantly appearing on the horizon. One solution to this seemingly unsolvable problem is the sharing of threat intelligence in order to raise awareness and sound the alarm about new attacks and data breaches as they happen. This way major security incidents can be avoided from recurring and prevent emerging threats from claiming more victims (Dickson, 2016). Doug (2015) offered that consistent and open sharing of threat information promises to be a way to improve organization awareness and hopefully defenses. It also allows the organization to spread the costs around more than if each organization provided its own expertise.

Cyber Security Controls

According to Stouffer, Falco and Scarfone (2011), it is important to have a layered control system, which deploys different controls at different points of a business process and throughout an IT system so that the strength of one control can compensate for weaknesses in or possible failure of another control. Therefore, layered controls function in an integrated fashion to more effectively mitigate risk. Compensating controls are controls that adjust for weaknesses within the system or process. An example of compensating controls would be a review of activity logs for applications that do not allow proper segregation of duties.

Magomelo, Mamboko and Tsokota (2014) argued that management should implement controls that align security with the nature of the institution's operations and strategic direction. Based on the institution's risk assessment, the controls should include, but may not be limited to, patch management, asset and configuration management, vulnerability scanning and penetration testing, end-point security, resilience controls, logging and monitoring, and secure software development (including third-party software development). In implementing controls, management should ensure it has the necessary resources, personnel training, and testing to maximize the effectiveness of the controls. The level at which controls are implemented should depend on the institution's size, complexity, and risk profile, but all institutions should implement appropriate controls. In light of increasing cybersecurity risks, management should implement risk-based controls for managing cybersecurity threats and vulnerabilities, such as interconnectivity risk. Management should review and update the security controls as necessary depending on changes to the internal and external operating environment, technologies, business processes, and other factors (Cybersecurity, 2014).

Cyber Incident Response and Resilience

Management should have effective log retention policies that address the significance of maintaining logs for incident response and analysis needs (Johnson *et al.*, 2016). Log files are critical to the successful investigation and prosecution of security incidents and can potentially contain sensitive information. Intruders often attempt to conceal unauthorized access by editing or deleting log files. Therefore, institutions should strictly control and monitor access to log files whether on the host or in a centralized logging repository. Khan *et al.* (2016) observed that, regardless of the method of log management, management should develop processes to collect, aggregate, analyze, and correlate security information. Policies should define retention periods for security and operational logs. Institutions maintain event logs to understand an incident or cyber event after it occurs. Monitoring event logs for anomalies and relating that information with other sources of information broadens the institution's ability to understand trends, react to threats, and improve reports to management and the board (Bollinger, Enright & Valites, 2015).

METHODOLOGY

The study adopted a descriptive survey design. The target population of this study were the 11 banks listed in Nairobi Securities Exchange, Kenya with a total employee population of 36,212. The sample was purposively drawn from IT Department of the specific banks as they are assumed to possess special knowledge and experience of implementing and managing cybersecurity strategies used in combating banking fraud. In this study, a total of 123 questionnaires were distributed and 103 were duly filled and returned. This represented a response rate of 83.7%. According to Rea and Parker (2014), a response rate of above 50% is adequate for analysis and therefore, a response rate of 83.7 % was considered as being excellent for analysis.

RESULTS AND DISCUSSION

Reliability Analysis

Bolarinwa (2015) defines reliability as the repeatability, stability or internal consistency of a questionnaire. To test for reliability, Cronbach's Alpha type of reliability coefficient was used, taking into account a value of 0.7 or higher as being sufficient. From the results presented in Table 1, all the variables were found to be reliable at a Cronbach's Alpha .710, .835, .791, .855 and .756 (as shown in Table 1) which were higher than the threshold of 0.7.

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

Reliability Statistics		
Variable	**Cronbach's Alpha**	**N of Items**
Cyber Risk Management and Oversight	.710	6
Cyber Threat Intelligence and Collaboration	.835	6
CyberSecurity Controls	.791	6
Cyber Incident Response and Resilience	.855	7
Combating Banking Fraud	.756	5

Descriptive statistics for Cyber Risk Management and Oversight

The study sought to determine the descriptive statistics for Cyber Risk Management and Oversight. From Table 2, 45.6% agreed that management has a formal process to continuously improve cybersecurity oversight, 40.8% agreed that the board committee discusses ways for management to develop cybersecurity improvements that may be adopted sector-wide, 53.4% agreed that designated members of management are held accountable by an appropriate board committee for implementing and managing the information security and business continuity programs, 40.8% agreed that at least annually, the board committee reviews and approves the institution's cybersecurity program, 40.8% agreed that management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity, and 43.7% agreed that the board or an appropriate board committee has cybersecurity expertise or engages experts to assist with oversight responsibilities.

Table 2: Descriptive statistics for Cyber Risk Management and Oversight

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Management has a formal process to continuously improve cybersecurity oversight	1.0%	8.7%	34.0%	45.6%	10.7%
The board committee discusses ways for management to develop cybersecurity improvements that may be adopted sector-wide	0.0%	10.7%	33.0%	40.8%	15.5%
Designated members of management are held accountable by an appropriate board committee for implementing and managing the information security and business continuity programs	0.0%	2.9%	14.6%	53.4%	29.1%
At least annually, the board committee reviews and approves the institution's cybersecurity program	1.9%	2.9%	15.5%	40.8%	38.8%
Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity	0.0%	3.9%	17.5%	40.8%	37.9%
The board or an appropriate board committee has cybersecurity expertise or engages experts to assist with oversight responsibilities	1.0%	8.7%	20.4%	43.7%	26.2%

Descriptive statistics for Cyber Threat Intelligence and Collaboration

The study generated a descriptive statistics table for Cyber Threat Intelligence and Collaboration. The results were summarized in Table 3. From the table, 46.6% agreed that a dedicated cyber threat identification and analysis committee or team exists to centralize and coordinate initiatives and communications, 41.7% agreed that a mechanism is in place for sharing cyber threat intelligence with business units in real time including the potential financial and operational impact of inaction, 39.8% agreed that a formal and secure process is in place to share threat and vulnerability information with other entities, 43.7% agreed that the institution uses multiple sources of intelligence, correlated log analysis, alerts, internal traffic flows, and geopolitical events to predict potential future attacks and attack trends, 55.3% agreed that a formal protocol is in place for sharing threat, vulnerability, and incident information to employees based on their specific job function, 47.6% agreed that threat intelligence is

Table 3: Descriptive statistics for Cyber Threat Intelligence and Collaboration

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
A dedicated cyber threat identification and analysis committee or team exists to centralize and coordinate initiatives and communications	1.0%	4.9%	18.4%	46.6%	29.1%
A mechanism is in place for sharing cyber threat intelligence with business units in real time including the potential financial and operational impact 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 institution uses multiple sources of intelligence, correlated log analysis, alerts, internal traffic flows, and geopolitical events to predict potential future attacks and attack trends	1.0%	3.9%	23.3%	43.7%	28.2%
A formal protocol is in place for sharing threat, vulnerability, and incident information to employees based on their specific job function	0.0%	2.9%	19.4%	55.3%	22.3%
Threat intelligence is viewed within the context of the institution's risk profile and risk appetite to prioritize mitigating actions in anticipation of threats	0.0%	4.9%	33.0%	47.6%	14.6%

viewed within the context of the institution's risk profile and risk appetite to prioritize mitigating actions in anticipation of threats.

Descriptive statistics for Cybersecurity Controls

The study sought to find the descriptive statistics of Cybersecurity Controls. The findings were summarized in Table 4. From the table 35.0% agreed that there is a firewall at each Internet connection and between any Demilitarized Zone (DMZ) and internal network(s), 35.9% remained neutral on the statement that Critical systems supported by legacy technologies are regularly reviewed to identify for potential vulnerabilities, upgrade opportunities, or new defense layers, 35.9% agreed that employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege, 42.7% agreed that security controls are used for remote access to all administrative consoles, including restricted virtual systems, 49.5% agreed that technical measures are in place to prevent the execution of unauthorized code on institution owned or managed devices, network infrastructure, and systems components, while 48.5% agreed that anti-spoofing measures are in place to detect and block forged source IP addresses from entering the network.

Table 4: Descriptive statistics for Cybersecurity Controls

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
There is a firewall at each Internet connection and between any Demilitarized Zone (DMZ) and internal network(s)	6.8%	7.8%	30.1%	35.0%	20.4%
Critical systems supported by legacy technologies are regularly reviewed to identify for potential vulnerabilities, upgrade opportunities, or new defense layers	10.7%	10.7%	35.9%	26.2%	16.5%
Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege	3.9%	11.7%	35.0%	35.9%	13.6%
Security controls are used for remote access to all administrative consoles, including restricted virtual systems	0.0%	7.8%	35.9%	42.7%	13.6%
Technical measures are in place to prevent the execution of unauthorized code on institution owned or managed devices, network infrastructure, and systems components	0.0%	3.9%	23.3%	49.5%	23.3%
Anti-spoofing measures are in place to detect and block forged source IP addresses from entering the network	1.0%	1.0%	14.6%	48.5%	35.0%

Descriptive statistics for Cyber Incident Response and Resilience

The study generated descriptive statistics that were summarized in Table 5. From the table, 45.6% agreed that communication channels exist to provide employees a means for reporting information security events in a timely manner, 34.0% agreed that a strategy is in place to coordinate and communicate with internal and external stakeholders during or following a cyber attack, 41.7% agreed that methods for responding to and recovering from cyber incidents are tightly woven throughout the business units' disaster recovery, business continuity, and crisis management plans, 37.9% agreed that resilience testing is comprehensive and coordinated across all critical business functions, 34.0% remained neutral on the statement that recovery scenarios include plans to recover from data destruction and impacts to data integrity, data loss, and system and data availability, 36.9% agreed that the institution has documented how it will react and respond to cyber incidents, and 40.8% agreed that Cyber-attack scenarios are analyzed to determine potential impact to critical business processes.

Table 5: Descriptive statistics for Cyber Incident Response and Resilience

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Communication channels exist to provide employees a means for reporting information security events in a timely manner	0.0%	1.9%	22.3%	45.6%	30.1%
A strategy is in place to coordinate and communicate with internal and external stakeholders during or following a cyber attack	0.0%	2.9%	30.1%	34.0%	33.0%
Methods for responding to and recovering from cyber incidents are tightly woven throughout the business units' disaster recovery, business continuity, and crisis management plans	0.0%	3.9%	32.0%	41.7%	22.3%
Resilience testing is comprehensive and coordinated across all critical business functions	1.0%	7.8%	28.2%	37.9%	25.2%
Recovery scenarios include plans to recover from data destruction and impacts to data integrity, data loss, and system and data availability	1.0%	11.7%	34.0%	24.3%	29.1%
The institution has documented how it will react and respond to cyber incidents	1.0%	3.9%	24.3%	36.9%	34.0%
Cyber-attack scenarios are analyzed to determine potential impact to critical business processes	1.0%	7.8%	21.4%	40.8%	29.1%

Descriptive statistics for Combating Banking Fraud

Table 6: Descriptive statistics for Combating E-Banking Fraud

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
We have stringent administrative procedures to guard document availability, data integrity and confidentiality	0.0%	4.9%	29.1%	40.8%	25.2%
Systems are available that implement stringent processes to monitor and detect any breach of security	1.0%	2.9%	32.0%	45.6%	18.4%
All the data that is transferred from our customers to our office is encrypted to ensure that none of the data is deciphered	0.0%	4.9%	37.9%	33.0%	24.3%
Our systems enable customers to securely access information whenever needed	1.0%	3.9%	30.1%	36.9%	28.2%
Regular and routine system audits are conducted in our bank	0.0%	1.0%	15.5%	48.5%	35.0%

Using descriptive statistics Table 6 was generated from the data. From the table, 40.8% agreed that they have stringent administrative procedures to guard document availability, data integrity and confidentiality, 45.6% agreed that systems are available that implement stringent processes to monitor and detect any breach of security, 37.9% remained neutral on the statement that all the data that is transferred from their customers to their office is encrypted to ensure that none of the data is deciphered, 36.9% agreed that their systems enable customers to securely access information whenever needed, while 48.5% agreed that regular and routine system audits are conducted in their bank.

Correlation between the variables

The study generated a correlation matrix between the variables using SPSS Software. The findings were presented in Table 7. The table shows that all the independent variables had a positive and statistically significant (p = .000) correlation with the dependent variable (Combating Banking Fraud).

Table 7: ***Correlation between the variables***

Correlations

		Combating Banking Fraud	Cyber Risk Management and Oversight	Cyber Threat Intelligence and Collaboration	CyberSecurity Controls	Cyber Incident Response and Resilience
Combating Banking Fraud	Pearson Correlation	1	.345**	.707**	.688**	.804**
	Sig. (2-tailed)		.000	.000	.000	.000
	N	103	103	103	103	103
Cyber Risk Management and Oversight	Pearson Correlation	.345**	1	.289**	.288**	.344**
	Sig. (2-tailed)	.000		.003	.003	.000
	N	103	103	103	103	103
Cyber Threat Intelligence and Collaboration	Pearson Correlation	.707**	.289**	1	.774**	.731**
	Sig. (2-tailed)	.000	.003		.000	.000
	N	103	103	103	103	103
CyberSecurity Controls	Pearson Correlation	.688**	.288**	.774**	1	.671**
	Sig. (2-tailed)	.000	.003	.000		.000
	N	103	103	103	103	103
Cyber Incident Response and Resilience	Pearson Correlation	.804**	.344**	.731**	.671**	1
	Sig. (2-tailed)	.000	.000	.000	.000	
	N	103	103	103	103	103

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

Regression Analysis

From the Model Summary Table 8, R^2 was .695 meaning that all independent variables (Cyber Incident Response and Resilience, Cyber Risk Management and Oversight, Cybersecurity Controls, Cyber Threat Intelligence and Collaboration) contributes 69.5% to the total variability in the dependent variable (Combating Banking Fraud).

Table 8: ***Model Summary of Independent Variables and the Dependent Variable***

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.834[a]	.695	.682	1.67524

a. Predictors: (Constant), Cyber Incident Response and Resilience, Cyber Risk Management and Oversight, Cybersecurity Controls, Cyber Threat Intelligence and Collaboration

The Anova Table 9 shows that the p-value was .000 (below the 5% threshold) and hence, the Combined Independent Variables (Cyber Incident Response and Resilience, Cyber Risk Management and Oversight, Cybersecurity Controls, Cyber Threat Intelligence and Collaboration) had a statistically significant influence on the Dependent Variable (Combating Banking Fraud).

Table 95: ***Anova Table of Independent Variables and the Dependent Variable (Combating Banking Fraud)***

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	626.524	4	156.631	55.812	.000[b]
	Residual	275.030	98	2.806		
	Total	901.553	102			

a. Dependent Variable: Combating Banking Fraud

b. Predictors: (Constant), Cyber Incident Response and Resilience, Cyber Risk Management and Oversight, Cybersecurity Controls, Cyber Threat Intelligence and Collaboration

From the Coefficient Table 10, Cyber Risk Management and Oversight and Cyber Threat Intelligence and Collaboration variables were not statistically significant as their p-values were above the 5% threshold. However, Cybersecurity Controls and Cyber Incident Response and Resilience variables contributed significantly to the optimal model shown below;

$$Combating\ Banking\ Fraud\ (Y) = 3.052 + .143X_3 + .355X_4$$

Table 10: Coefficient Table of Independent Variables and the Dependent Variable (Combating Banking Fraud)

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	**Std. Error**	**Beta**	**t**	**Sig.**
1	(Constant)	3.052	1.376		2.217	.029
	Cyber Risk Management and Oversight	.053	.054	.059	.993	.323
	Cyber Threat Intelligence and Collaboration	.102	.075	.135	1.369	.174
	CyberSecurity Controls	.143	.067	.194	2.129	.036
	Cyber Incident Response and Resilience	.355	.055	.555	6.470	.000

a. Dependent Variable: Combating Banking Fraud

CONCLUSION

From the findings, the study concluded that Cyber Risk Management and Oversight strategy is key to combating banking fraud in the banking industry in Kenya. This finding confirms a study by Pitcock (2015) who observed that management's assessment of the Cyber Risk Management and Oversight strategy will allow for the identification of weaknesses and for plans to be established to improve the institution's cybersecurity preparedness. The author recommended that in assessing the domain, management should remember an effective cybersecurity program begins with a culture and management team dedicated to addressing cybersecurity. In a similar note, Sandra and Gaurav (2016) add that boards rely on a variety of cyber-risk monitoring and reporting mechanisms, including, but not limited to, risk and control self-assessments, internal audits, and crisis management simulation exercises.

From the results, the study also concluded that Cyber Threat Intelligence and Collaboration strategy had a great impact in combatting banking fraud in the banking industry in Kenya. In a similar study, Skopik, Settanni and Fiedler (2016) concluded that, in the ever-shifting landscape of cyberthreats and attacks, having access to timely information and intelligence is vital and can make a big difference in protecting organizations and firms against data breaches and security incidents. Further, Steer (2014) also concluded that there is a need to stay ahead of current threats and be able to predict future attacks, which can be achieved through the use of a collective threat intelligence ecosystem.

The findings led to the conclusion that the banks in Kenya have Cybersecurity Control measures in place ready to combat any information security risks they may encounter in their operations. In a similar study, Stouffer, Falco and Scarfone (2011) concluded that a layered control system is important because it deploys different controls at different points of a business process and throughout an IT system so that the strength of one control can compensate for weaknesses in or possible failure of another control. Abdou, English and Adewunmi (2014) added that for institutions that offer services to customers through remotely accessible technology, such as the Internet and mobile financial services, management should implement appropriate authentication techniques commensurate with the risk from remote banking activities.

the study resultthe further revealed that banks in Kenya have plans in place that include explicit steps to address information security incident as well as plans to respond to any information security event scenarios that may occur. The conclusion is confirmatory to that of Goodwin *et al.* (2015) who reported that risk reporting should describe any information security events that the institution faces and the effectiveness of management's response and resilience to those events. In addition, Tøndel, Line and Jaatun (2014) observes that the reporting process should provide a method of disseminating those reports to appropriate members of management.

Combined strategies under study would only succeed in combating banking fraud up to 69.5% level. Nevertheless, on their own each strategy was found to have a significant influence in combating banking fraud in the Kenyan banking sector. Therefore, the study recomends that it is important for the banks in Kenya to implement each of the strategies under study so that the strength of one strategy could compensate for weaknesses in or possible failures of the other strategy. In addition, the study recommends that the banks find other strategies that are not in this study so as to take care of the remainder 30.5% which is a significant percentage, especially when it is associated with the banking sector.

REFERENCES

Abdou, H., English, J., & Adewunmi, P. (2014). An investigation of risk management practices in electronic banking: the case of the UK banks. Banks and Bank Systems, 9(3).

AICPA. (2016). Cybersecurity Attestation Examination Engagement. Retrieved from https://www.aicpa.org/Research/Standards/AuditAttest/ASB/Documents/Mtg/1608/2016_08_ASB_Item5.pdf

Barnum, S. (2012). Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™). MITRE Corporation, 11.

Bhasin, M. L. (2015). An Empirical Study of Frauds in the Banks.

Bhasin, M. L. (2016). The Role of Technology in Combatting Bank Frauds: Perspectives and Prospects. *Ecoforum Journal*, *5*(2).

Bolarinwa, O. A. (2015). Principles and methods of validity and reliability testing of questionnaires used in social and health science researches. *Nigerian Postgraduate Medical Journal*, *22*(4), 195.

Bollinger, J., Enright, B., & Valites, M. (2015). Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan. " O'Reilly Media, Inc.".

Brignall, M. (2015, November 21). So you think you're safe doing internet banking? *The Guardian*, retrieved from https://www.theguardian.com/money/2015/nov/21/safe-internet-banking-cyber-security-online

Contreras, J. L., DeNardis, L., & Teplinsky, M. (2012). Mapping today's cybersecurity landscape. Am. UL Rev., 62, 1113.

Cory, R. L. (n.d.). Cybersecurity Assessment Tool: Focusing on Cyber Risk Management and Oversight. Retrieved from https://www.wolfandco.com/insight/cybersecurity-assessment-tool-focusing-cyber-risk-management-and-oversight-0

Cybersecurity, C. I. (2014). Framework for Improving Critical Infrastructure Cybersecurity.

Dickson, B. (2016). How threat intelligence sharing can help deal with cybersecurity challenges. Retrieved from https://techcrunch.com/2016/05/15/how-threat-intelligence-sharing-can-help-deal-with-cybersecurity-challenges/

Doug, F. (2015). Threat Intelligence Collaboration Leads to More Efficient, Comprehensive Cybersecurity. Retrieved from https://securityintelligence.com/threat-intelligence-collaboration-leads-to-more-efficient-comprehensive-cybersecurity/

Dzomira, S. (2014). Electronic Fraud (Cyber Fraud) Risk in the Banking Industry, Zimbabwe. *Risk governance & control: financial markets & institutions*, *4*(4), 17-27.

Goodwin, C., Nicholas, J. P., Bryant, J., Ciglic, K., Kleiner, A., Kutterer, C., & Sullivan, K. (2015). A framework for cybersecurity information sharing and risk reduction. Technical report, Microsoft Corporation.

Herrygers, S. (2016, October 12). Raising the Bar for Cyber-Risk Management Oversight and Reporting. The Wall Street Journal, Retrieved from http://deloitte.wsj.com/riskandcompliance/2016/10/12/raising-the-bar-for-cyber-risk-management-oversight-and-reporting/

Hong, J. (2012). The state of phishing attacks. Communications of the ACM, 55(1), 74-81.

Chiezey, U., & Onu, A. J. C. (2013). Impact of fraud and fraudulent practices on the performance of banks in Nigeria. *British Journal of Arts and Social Sciences*, *15*(1), 12-25.

Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to cyber threat information sharing. NIST Special Publication, 800, 150.

Khan, S., Gani, A., Wahab, A. W. A., Bagiwa, M. A., Shiraz, M., Khan, S. U., & Zomaya, A. Y. (2016). Cloud log forensics: foundations, state of the art, and future directions. ACM Computing Surveys (CSUR), 49(1), 7.

Klein, R. (2015). How to avoid or minimize fraud exposures. *The CPA Journal*, *85*(3), 6.

Magomelo, M., Mamboko, P., & Tsokota, T. (2014). The Status of Information Security Governance within State Universities in Zimbabwe. Journal of Emerging Trends in Computing and Information Sciences, 5(8).

Mwaura, K., & Thiong'o, P. (2013, November 2). Shock as Kenyan bank losses to fraud triple to Sh1.6bn. *The EastAfrican*, Retrieved from http://www.theeastafrican.co.ke/news/Kenyan-banks-lose--18-8m-to-savvy-fraudsters/-/2558/2057524/-/gfy7g3z/-/index.html

Olingo, A. (2014, November 15). Kenya's commercial banks lose $9.4m to fraud in just six months. *The EastAfrican*, Retrieved from http://www.theeastafrican.co.ke/news/Kenyan-commercial-banks-lose--9-4m-to-fraud-in-just-six-months/2558-2523802-item-1-osg23dz/index.html

Pasricha, P., & Mehrotra, S. (2014). Electronic crime in Indian banking. *Sai Om Journal of Commerce and Management*, *1*(11).

Pitcock, R. W. (2015). *Evaluating the cyber security capabilities of senior managers employed by companies located in the United States* (Doctoral dissertation, Jones International University).

PWC. (2015). Current fraud trends in the financial sector. Retrieved from https://www.pwc.in/assets/pdfs/publications/2015/current-fraud-trends-in-the-financial-sector.pdf

Rea, L. M., & Parker, R. A. (2014). *Designing and conducting survey research: A comprehensive guide*. John Wiley & Sons.

Sandra, H. & Gaurav, K. (2016). Cyber-Risk Oversight. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-raising-the-bar-for-cyber-risk-management-oversight-and-reporting.pdf

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154-176.

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154-176.

Steer, J. (2014). The gaping hole in our security defences. Computer Fraud & Security, 2014(1), 17-20.

Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. NIST special publication, 800(82), 16-16.

Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. Computers & Security, 45, 42-57.