AN ASSESSMENT OF CYBER CRIME IN COMMERCIAL BANKS IN CALABAR METROPOLIS

Martins Myke-Okoi Okpa
Department of Sociology and Anthropology
University of Uyo, Nigeria
okpamartins@gmail.com
+2348067263539

https://doi.org/10.60787/ijsi.v11i2.44

Abstract

The incidence of cyber fraud and crimes has increased exponentially in the financial industry, with excruciating consequences on commercial banks as a result of technological advancements, adopted to meet customers' needs and gain competitive advantage. Due to the ever-increasing causes, this study examines the effects or impact of cybercrime on financial institutions performance. Specifically, the study investigates the prevalence of cybercrimes recorded by commercial banks and the effect on the performance of the banks. This paper is anchored on the differential opportunity theory. The survey research design was adopted, and questionnaires administered on 323 staff of sixteen (16) commercial banks located in Calabar Metropolis. Three hundred respondents completed and returned their questionnaires. The data collected were analysed using SPSS 26, with descriptive and correlation analyses performed on the data. The hypotheses were tested using Ordinary Least Square (OLS) regression technique. From the analyses, it was found that the four major cybercrimes recorded by commercial banks in Calabar were Phishing, Skimming, Malware and Distributed Denial of Service crimes. The test of hypotheses revealed that these four cybercrimes significantly jeopardize the performance of Commercial banks. The study concludes that cybercrimes expose commercial banks to liquidity shocks, increased credit risk, loss of business information, loss of reputation, financial losses and loss of operational efficiency. This study contributes to gaining more insight into the impact of cybercrime in the banking sector, and recommends that cyber risk management techniques be effectively implemented by banks, if they must continue in operation and earn returns on their investments.

Keywords: Cybercrime, Cybersecurity, Phishing, Skimming, Malware, CRMG, Bank Performance

Introduction

Many organizations have become increasingly virtual. As more daily activities migrate online and people's reliance on the internet grows, the potential of hacking, attacks and other security breaches by cyber criminals increase rapidly. These crimes have become an everyday reality and they are growing in an unprecedented dimension in line with technological developments (Bohme and Moore, 2012; Arachchilage*et al.* , 2014).

Cybercrime is now a formidable risk factor in the financial industry because the cash flows and growth of the banks and other financial institutions become more uncertain with changing and unpredictable threats in cyberspace (Teece, 2018; Gracie, 2015; Brown, 2015). Institutions are unable to assess the level of risk exposure arising from threats in cyberspace because cyber intelligence can identify a security threat but cannot assess the direct and indirect financial impact on the institutions. Currently, available cyber- intelligence software mostly identifies and controls suspicious communications in the network systems. Yet, the estimation of losses from a potential cyber breach is not easy since the cyber risk is different from other types of business and financial risks (Eling and Wirfs, 2019). Therefore, banks and other financial institutions are more fragile now due to cyber security risk (Shackelford, 2012) arising from rapid digital transformation in the industry.

It is an acknowledged fact among industry practitioners, managers, and academic researchers that cyber security breach contributes to the operational risks of banks and other financial institutions in the virtual environment. This is because the loopholes in cyber infrastructure and social engineering create opportunities for the hackers to infiltrate the banking network to disrupt operations (Longstaff *et al.* , 2020). A recent empirical study by Aldasoro *et al.* (2020a) documented that cybercrime risk accounts for significant operational value-at-risk. Therefore, the cyber risk management approach is now more a boardroom issue than merely a technological matter (Soomro *et al.* , 2016).

Cybercrime in the banking sector increases by the ongoing digitalization. More and more organizations rely on digital networks for their business operations. This increases the risk for organizations and their customers of becoming victims of cybercrime (Arachchilage *et al.* , 2014). In the bank virtual environment, institutions are vulnerable to system failure and programme error that may result from technical faults. However, as no technology is perfect and completely secured, the perpetrators get the opportunity to breach the system and inflict a colossal loss on the financial institutions by stealing money, confidential data and information. While the direct loss is measurable, the indirect financial damage from a data breach is enormous and hard to estimate. As observed by Gommans *et al.* (2015), cybercrime hazards escalate operational risk through the abuse of technology by humans.

Over the past few years, there were several cyber-attacks in the banking sector and on various components of online banking. Those attacks varied from stealing money to disabling online payment systems such as online banking through websites, mobile apps and iDeal. Cyber-attacks in the banking sector are mainly fraud related, because of the financial gain and have many forms (Lagazio *et al.* , 2014). These crimes include DDos attacks, phishing, skimming, hacking incidents, and malware (viruses), amongst others.

The impact of cybercrime has generated a significant risk exposure for individuals (personal harm) and organizations (reputational harm). It includes exposure to financial losses, regulatory issues, data breach liabilities, damage to brand and reputation, and loss of client and public confidence (Verma, Hussain and Kushwah, 2012). Cybercriminals can significantly threaten the finances and reputations of banks and other financial organizations. Moreover, it affects the relationship between the image of the bank and the trust that customers and other stakeholders have in that bank. This negative image can create some serious issues for bank when they become victims of cybercrime, such as deposit loss and withdrawal, liquidity shocks, credit risk escalation, and lower net income margins (Manzoor, 2014).

Since an increasing number of financial organizations are the target of cyber criminals, there is need to provide answer to the research question, “to what extent does cybercrime affect financial institutions”? To answer this question, this paper examines these two objectives:

1. to investigate the prevalence of cybercrimes among Nigerian commercial banks;
2. to find out the effects of cybercrimes on the performance of Nigerian commercial banks

Literature Review

The Concept of Cybercrime

Despite the fact that the term cybercrime has become common usage, many people find it hard to define cybercrime precisely. In addition, there is no universally accepted definition of cybercrime (Kraemer-Mbula *et al.* , 2013). The definition of cybercrime depends on its final purpose, means and classifications. According to Leukfeldt *et al.* (2013) cybercrime is defined as a form of criminality that targets an ICT system or the information it processes. In other words, cybercrime describes all kinds of crime and other illicit activities that involve the use of telecommunications networks, in which computers or computer networks are a tool, a target, or a locale of criminal activity.

Cybercriminals attack systems, or gain access to confidential information and data from users, through the use of a wide range of techniques (Arachchilage *et al.*, 2014). They use techniques such as a set of computer programmes which can disturb the normal behaviour of computer systems (viruses), malicious software (malware), unsolicited email (spam), monitoring software (spyware), attempting to make computer resources unavailable to its intended users (Distributed Denial- of-Service or DDos-attack), the art of human hacking (social engineering) and online identity theft (phishing)" (Arachchilage *et al.*, 2014). These types of attacks are frequently used and pose a serious threat to public and private organizations, including the banking sector (Stokkel *et al.*, 2013; Bhasin, 2007, Choo, 2011). It also impacts the daily activities of businesses and government.

Cyber Security and Systemic Risk of Technology

As the financial sector globally relies more on cyber technology for operations and services delivery, banks and financial institutions are increasingly exposed to the systematic risk of technology that cannot be removed. It occurs because a single breach in a banking network could shake off the entire financial system and bring disastrous outcome as all banks and financial institutions are interconnected (Johnson, 2015). When a hacker infiltrates the banking network, the institutions linked to the system face disruption in operations (Tendulkar, 2013). Cyber criminals generally infiltrate the system and remain quiet to monitor user activities before they attack and reap their benefits with maximum damage on the institution at the right opportunity. Cyber hackers can disrupt the financial system to prevent fund transfers between banks, steal confidential data while transmitting through the banking system, and damage the operations of other sectors that rely on the integrated banking services (Duran and Griffin, 2019). In this regards, the Basel committee suggests that banks and financial institutions globally should increase their institutional capacity to withstand the shocks of uncontrollable cyber threats, as the systemic risk of cyber technology cannot be eased up without capacity building (Boer and Vazquez, 2017).

According to Boer and Vazquez (2017), cyber security breaches become a systemic phenomenon in the financial industry which is a part of the need for technological dependence. Geyres and Orozco, (2016), and Gopalakrishnan and Mogato (2016) consider that investment in cyber technology is becoming imperative for the financial institutions in tandem with the advancement of the digital economy, which makes cybercrimes unavoidable as a result of substantial growth of investments in the IT security systems. Caron, (2015) Ahmad and Schreyer, (2016) also indicate that cyber-security risk cannot be mitigated merely by costly development of IT infrastructure - as it increases operational costs but cannot guarantee stoppage of cyber breaches.

Prevalence of Cybercrime and the Banking Sector

Cyber-security in the financial industry has emerged as operational issue since online-based criminal activities, fraud, and system failures can disrupt banking functions. Criminal activities such as theft of confidential personal identification number (PIN) of a bank manager may lead to several fraudulent transactions in the banking system (Gommans *et al.*, 2015). Similarly, criminals can steal customers' identity and PIN to access banking services and withdraw cash. These types of criminal activities involving fraudulent transactions may have litigation risks for financial institutions besides direct economic losses (Hon and Millard, 2018).

The intentional IT system failure or breakdown in the bank and financial institutions is another dimension of cyber risk. For example, distributed denial of services (DDoS) attacks may completely shut down banking services, allowing the criminals to plant malware or other spyware within the banking system (McConnell *et al.,* 2013). The system failure can occur for many reasons, but the operational consequence of an intentional system failure initiated by cybercriminals is challenging because malware can damage critical computer hardware,

including the server and networks, while spyware and phishing attacks can steal confidential information. Distributed Denial of Service is a term for a type of attack in which a particular service (e.g. a website) becomes unavailable to the usual consumers of the service. DDoS attacks on websites are often performed by bombarding websites with huge amounts of network traffic, so that they become unavailable. As a generic term, malware currently includes infection of computers with viruses, worms and Trojans

An increasing number of banks become the target of phishing attack by cyber criminals (Manzoor, 2014). Phishing has affected financial organizations, especially banks worldwide. Phishing and malware are forms of online banking fraud, whereby criminals steal confidential information and online banking details from its victims (Arachchilage *et al.* , 2014). Phishing is an umbrella term for digital activities with the object of tricking people into giving up their personal data. This personal data can be used for criminal activities such as credit card fraud and identity theft.

Cybercrime has evolved into a pervasive and continually escalating challenge in Nigeria, particularly within the context of the banking industry. The nation's growing reliance on the internet and digital technologies has created an environment where cybercriminal activities thrive unabated. Addressing cybercrimes in Nigeria is imperative, given the substantial impact they have on the nation's economy. Globally, cybercrimes are on the rise, with estimations reaching staggering figures, such as $388 billion reported in 2011 (Nwogwugwu and Uzoechina, 2015).

Financial institutions bear the brunt of these cyber threats, making them primary targets of cybercriminals. Banks, besides safeguarding financial assets, hold crucial information about consumers and businesses. The rise of online banking and payment systems has provided cybercriminals with opportunities to engage in illicit activities, leading to illegal fund transfers from unsuspecting customer accounts to fraudulent accounts (Hastings, 2015). The severity of the issue is evident from Kaspersky Lab's (2022) estimate that cyber-attacks on banks and financial institutions cost these companies approximately $3 billion in 2021.

Cybercrimes and Bank Performance

Banks and other financial institutions are known to have the risk of liquidity crunch from public sentiment to cyber incidence news in the market (Hovav and D'Arcy, 2014). The affected bank may experience depositor runs, leading to funds shortages that require liquidation of the bank's investment before maturity by forgoing accrued earnings. It may happen because panicked depositors may switch to another financial institution by losing confidence in the affected banks despite that they have bank switching costs. The adverse effect of cyber-security hazards on banks' corporate earnings is a concern for not just the financial sector but researchers alike.

Sharma and Tandekar, (2018) posit that earnings uncertainty and loss of operational efficiency due to unavoidable cyber security risk resulting from the widespread application of technology adoption exist among financial institutions, despite its necessity, which adversely affect the longer-term growth and stability of the institution. Industry experts also observe that cybercriminals can infiltrate the financial data server and manipulate creditors' confidential data such as loans, default status, personal financial circumstances, and creditworthiness (Langton, 2018). Therefore, financial institutions are exposed to higher credit risk because of the probability of selecting wrong borrowers based on manipulated data. Hence, cyber-security risk could affect the stability of banks and financial institutions through the liquidity shocks and increased credit risk.

From the above empirical literature, it is thus conjectured in the alternative that:

i. cybercrimes related to Phishing negatively affect commercial banks' performance;
ii. cybercrimes related to Skimming negatively affect commercial banks' performance;

iii. cybercrimes related to Malware negatively affect commercial banks' performance;

iv. cybercrimes related to DDos negatively affect commercial banks performance.

Cyber Risk Management Approach

In recent times, managers, regulators, and international organizations emphasize the effective management of cyber risks in IT-based banking systems since cybercrime and risk are a new critical factor that can adversely affect the soundness of the banks and financial institutions (Kopp *et al.*, 2017). Effective cyber risk management could reduce operational uncertainties in the digital banking environment, facilitate the liberalization of the banking sector, promote banking integrations, and expand financial networks. Overall, it is well recognized that cyber security risk management is critically important, but the primary focus is still given to technological solutions because of the rapid growth of cyber incidents across the world (Morton *et al.*, 2018). Nevertheless, researchers and practitioners now emphasize the non-technical approach as an additional measure to overcome the pervasive effects of cyber security incidents (Herath and Rao, 2009).

The managerial approaches to control cyber risk include policy formulation, regulatory compliance, external collaboration, organizational restructuring, and capacity building. Soomro *et al.*, (2016) suggest that institutions should define their cyber-security policies that will provide clear guidelines to address cyber breaches promptly at the operational level. The guidelines give an idea about early identification of security threats and preventive measures, as well as financial provisions to compensate losses. Eling and Lehmann (2018) emphasize full compliance with institutions' policy and regulatory guidelines on cyber risk management as it is essential to safeguard stakeholders' assets and reduce operational risks. Donge *et al.* (2018) recommend active collaboration between banks and external agencies dealing in technology services since unscrupulous perpetrators intrude on the banking system through black spots in technology infrastructure. Since banks and institutions still rely on the technology firms to outsource technology-based operational support, there is need to enact personal data protection laws that make technology firms (as the data processor) accountable for data breaches. It helps to improve customer confidence in electronic commerce and business transactions, given the rising number of cyber-security incidences.

To Granasen and Andersson (2016), banks need to create a separate unit within the risk management department that combines expertise in both technical and non-technical fields. The IT experts can provide technical support to detect black spots in the system. At the same time, personnel with banking knowledge can assist in identifying risky zones dealing with cash and data. The legal experts can suggest litigations and compensations if a cyber-breach occurs. Finally, Mayahi and Humaid (2016) emphasize the building of capacity through well-planned employee training on IT operations and ethical standards improvement, as well as timely acquisition or up-grade of technology infrastructure.

Theoretical Framework

This section focuses on presenting and adopting a theory to aid in understanding the concept of cybercrime as it relates to commercial banks. The adopted theory for this paper is the Differential Opportunity theory developed by Richard A. Cloward and Lloyd E. Ohlin, published in 1960 "Delinquency and opportunity". This theory was published to report on the nature and activities of juvenile gangs. The theory is, however, an offshoot of the dominant strain theory as it derived its ideas from it.

According to the proponents Cloward and Ohlin, there are two types of socially structured opportunities for success, illegitimate and legitimate. The legitimate opportunities are generally available to individuals born into middle-class culture, whereas participants in the lower-class subcultures are often denied access to them. As consequence, illegitimate opportunities for

success are often seen as quite acceptable by participant in so called illegitimate subcultures. The term "illegitimate opportunity structure" was used to describe preexisting sub-cultural paths to success that are not approved by the wider culture.

Cloward and Ohlin describe three types of delinquent subcultures: (a) criminal subculture (b) conflict subculture (c) retreatist subculture. They argue that criminal subculture explains a situation where criminal role models are readily available for adoption by those being socialized into the subculture. In the conflict subculture participants seek status through violence, while in the retreatist subculture; participants withdraw from the wider societal norms to illegitimate means of success.

According to Cloward and Ohlin delinquent behaviour may result from the availability of illegitimate opportunities and the effective replacement of the norms of the wider culture with expedient sub cultural rules. Hence, delinquency and criminality may become all right or legitimate in the eyes of those perpetrating it. Also, where illegitimate paths to success are not already in place, alienated individuals may undertake a process of ideational evolution through which a collective delinquent solution or a delinquent means of achieving success is agreed upon by members of a gang.

The theory of differential opportunity is relevant to the concept of cybercrime and financial institutions. The theory holds that societal means to success is partitioned into two patterns, that is socially structured opportunities for success is categorized into legitimate and illegitimate. Cybercrime is an unlawful and criminal act and thus seen as an illegitimate means to success. Those involved in cybercrime have seen an opportunity to commit crime because of the vulnerability of internet platforms.

The porous nature of internet platforms creates opportunity for the cybercriminal to commit internet crimes, knowing that the information communication technology (ICT) is not secure and one can commit crime and go unnoticed. A Cybercriminal takes advantage of the vulnerability of not just the internet platforms but also its users. Hence, an opportunity is seen to swindle money and material things from victims. Banks and their customers are the major targets of the cyber criminals; this is so because the banks' information is easily accessed by these internet fraudsters.

Furthermore, it is arguable that lack of laws against cybercrime and sometimes where such laws are enacted, lack of implementation by necessary institutions also presents an opportunity for cybercrime to perpetuate. Overtime persons arrested for cybercrime and related crimes are not prosecuted. This situation has created a tremendous increase in cyber criminality in Nigeria. More so, economic conditions such as poverty and unemployment are social factors that have created opportunity for the perpetration of cybercrimes. Several researches had indicated that poverty and unemployment situation in Nigeria are major factors for youth involvement in cybercrime. Just like the traditional strain theory holds, that individuals who cannot abide to the generally accepted and structured norms or laid down rules and regulations in attaining their goals and cannot adapt will seek alternative illegitimate means to attain such goals. Thus, an individual who is unemployed may see engaging in cybercrime as a way out of poverty.

This section dwells on the review of extant and related literature on this study in order to aid in understanding the phenomenon of cybercrime in commercial banks. Hence, a conceptual review was done. To fill a gap in literature; a review was done on cyber security and the systemic risk of technology, prevalence of cybercrime in the banking sector, cybercrime and bank performance, cyber risk management approach and lastly, the differential opportunity theory was adopted for the study.

Methodology

The study being an empirical one, adopted a quantitative survey research design. The target population of the study was banks staff within Calabar metropolis, there were about sixteen (16) commercial banks located in Calabar. The estimated target staff population is presented below:

SN	Bank	Estimated Target Population	Number of Branches
1	First Bank	105	5
2	GTB	38	2
3	Access bank	72	4
4	Union Bank	47	3
5	UBA	37	2
6	Wema Bank	19	1
7	Zenith Bank	51	3
8	Sterling Bank	24	1
9	Polaris Bank	33	2
10	FCMB	18	2
11	Fidelity Bank	41	2
12	Stanbic IBTC	37	2
13	Keystone Bank	15	1
14	Unity Bank	34	2
15	Eco Bank	79	4
16	Heritage Bank	31	2
Total Target Population:		**681**	**38**

Source: Field Report, 2021

Given that prior studies such as Aldasoro et al (2020) and Boer and Vazquez (2017) show that the proportion of the population that is effectively included in a study of this magnitude is 30 percent using Z-score distribution, $n = \frac{Z^2Xp(1-p)}{e^2}$. We therefore, estimate that, where: Z= Z score at 95% confidence level = 1.96, P = 70% estimated population interest = 0.7%, e = margin of error = 0.05%, the sample size derived with the above formula was 323 from the population of 681 staff.

A well-structured questionnaire was administered to respondents using the convenience sampling method. The data collected were analysed using SPSS 26, with descriptive and correlation analyses performed on the data. The hypotheses formulated were tested using Ordinary Least Square (OLS) Regression Technique, specified as $PERF_t = \beta_0 + \beta_1PHIS + \beta_2SKIM + \beta_3MALW + \beta_4DDoS + \varepsilon_t$ (1), Where: PERF = Bank Performance indicators (This represents the dependent variable), PHIS = Phishing related Cybercrimes, SKIM = Skimming related Cybercrimes, MALW= Malware related Cybercrimes, DDoS = Distributed denial of services related Cybercrimes (These represent the independent variables) and β_0 = Constant, $\beta_1 - \beta_4$ = Coefficients of the variables, ε_t= Stochastic Term.

Data Analysis and Results

Table 1: Demographic Characteristics of Respondents

N = 300	Category	Frequency	Percentage
Gender	Male	199	66.3
	Female	101	33.7
Age	Less than 36	21	7.0
	36-40	89	29.7
	41-45	103	34.3

	46-50	45	15.0
	51-55	25	8.3
	Above 55	17	5.7
Educational Level	HND/BA/BSc	193	64.3
	MSc/MA/MBA	76	25.3
	PhD	31	10.3
Years of Working	Less than 3	34	11.3
	4-6	95	31.7
	7-9	76	25.3
	10-12	45	15.0
	13-15	29	9.7
	Above 15	21	7.0

Source: Field Report, 2021

As presented in Table 1, 66.3% of respondents were male (n=199). Males constituted the majority at 66.3% of the valid responses while females were 33.7% (n=101) of the valid responses. For the research, there is likely to be a balanced opinion on matters being discussed as there is enough of each gender. The age distribution revealed that 7.0% of the participants were less than 36 years (n=21). 29.7% were 36-40 years old (n=89). 34.3% were between 41-45 years (n=103). 15.0% were between 46-50 years old (n=45) while 8.3% were between 51-55 years old (n=25). And those above 55 years were 5.7% (n=17). The majority age group here ranged from 36 years to 50 years. From the distribution, the organizations' workforce has all working ages represented. This indicates that there is no bias by one age group and the responses are therefore valid as they will reflect all ages.

In terms of the educational level of respondents, 64.3% have HND, BA or BSC (n=193), 25.3% have M.Sc, MA or MBA (n=76), while 10.3% have a PhD (n=31). The educational levels of the staff of the sampled banks in Calabar revealed that the respondents are educated and well informed, and can therefore provide data for the study. The years of working experience revealed that 11.3% had worked for less than 3 years (n=34), 31.7% had worked for 4-6 years (n=95), 25.3% had worked for 7-9 years (n=76), 15.0% had worked for 10 – 12 years (n=45), 9.7% had worked for 13 – 15 years (n=95). Those who had worked above 15 years were 7.0% (n=21). The distribution captured respondents at all levels of job tenure.

Table 2: Descriptive Statistics:

Variable	Mean	Std	Skewness	Kurtosis	Obs
PHIS	3.99	.89054	-.596	-.285	300
SKIM	3.82	.57101	-.623	1.650	300
MALW	3.91	.72902	-1.097	1.981	300
DDoS	3.89	.75775	-.652	.322	300
PERF	3.80	.80980	-.679	.236	300
CRMG	3.60	1.10861	-.518	-.964	300

Denotations: PHIS = Phishing related Cybercrimes, SKIM = Skimming related Cybercrimes, MALW= Malware related Cybercrimes, DDoS= Distributed denial of services related Cybercrimes, PERF = Bank Performance indicators, CRMG = Cybercrime Risk Management. *Hint: Mean value>3.0 = high and acceptable threshold*

Table 2 provides discussions on the descriptive characteristics such as the mean, standard deviation, skewness, kurtosis and total observations. The table revealed that the mean value of PHIS was 3.99 with a standard deviation of 0.89, which suggests that there is high incidence of phishing related cybercrimes among sampled banks. The data is negatively skewed (skewness=-0.596) and generally flat, that is platykurtic, as K=-0.285 is less than 3.

The mean value of SKIM is 3.82 with a standard deviation of 0.571, which suggests that there is also a high prevalence of skimming related cybercrimes faced by Nigerian commercial banks. The data is negatively skewed (skewness=-0.623) and generally flat, that is platykurtic, as K=1.671 is less than 3.

MALW also had a mean value of 3.91 with a standard deviation of 0.729, which indicates high level of malware related cybercrimes faced by Nigerian commercial banks. The data is negatively skewed (skewness=-1.097) and generally flat, that is platykurtic, as K=1.981 is less than 3.

DDoS had a mean value of 3.89, with a standard deviation of .758. This indicates a high presence of distributed denial of service cybercrimes. The data is negatively skewed (skewness= -0.652) and generally flat, that is platykurtic, as K=0.322 is less than 3.

PERF had a mean value of 3.80 and a standard deviation of 0.809. The result indicates a high-level of poor performance associated with cybercrimes among commercial banks in Nigeria. The data is negatively skewed (skewness=-0.679) and generally flat, that is platykurtic, as K=0.236 is less than 3.

CRMG also revealed a mean value of 3.60 and a standard deviation of 1.109. The data is negatively skewed (skewness=-0.518) and generally flat, that is platykurtic, as K=-0.964 is less than 3.

Table 3: Matrix Moment Correlation

Variable	PHIS	SKIM	MALW	DDoS	PERF	CRMG
PHIS	1					
SKIM	0.525** (0.000)	1				
MALW	.371** (0.000)	.596** (0.000)	1			
DDoS	.348** (0.000)	.547** (0.000)	.686** (0.000)	1		
PERF	-.373** (0.000)	-.571** (0.000)	-.371** (0.000)	-.398** (0.000)	1	

CRMG	-.337** (0.000)	-.221** (0.000)	-.344** (0.000)	-.125* (0.031)	.390* (0.001)	1

Denotations: PHIS = Phishing related Cybercrimes, SKIM = Skimming related Cybercrimes, MALW= Malware related Cybercrimes, DDoS = Distributed denial of services related Cybercrimes, PERF = Bank Performance indicators, CRMG = Cybercrime Risk Management.

To examine whether there were associations between the constructs adopted in this study, the Pearson's moment correlation coefficient matrix analysis was employed. All Pearson correlation coefficients among the six study variables of the study were significant as seen in table 4 above. Although these correlation coefficients alone do not provide a full test of the hypothesized relationships, they generally support the expected pattern of results.

Specifically, PERF was found to be significantly and negatively related to phishing related cybercrimes (r=-.373; *p=0.000*), skimming related cybercrimes (r=-.571; *p=0.000*), malware related cybercrimes (r=-.371; *p=0.000*) and DDoS related cybercrimes (r=-.398; *p=0.000*). The results indicate that cybercrimes negatively relate with bank performance, suggesting that higher rates of cybercrimes emanating from these four dimensions are associated with lower bank performance.

The correlation among the dimensions of cybercrimes in the study indicate that all cybercrimes have positive and significant associations. Phishing crimes have positive and significant relationship with Skimming crimes (r=.525; *p=0.000*), malware crimes (r=.371; *p=0.000*), and DDoS crimes (r=.348; *p=0.000*). Skimming crimes also have positive and significant relationship with malware crimes (r=.596; *p=0.000*) and DDoS crimes (r=.547; *p=0.000*). Malware crimes also have positive and significant relationship with DDoS crimes (r=.686;*p=0.000*).

Finally, the correlations revealed that cybercrime risk management approaches have negative correlations with the incidences of fraud, with correlation of -.337 (*p=0.000*) for phishing crimes, correlation of -.221 (*p=0.000*) for skimming crimes, correlation of -.344 (*p=0.000*) for malware crimes, and correlation of -.125 (*p=0.031*) for DDoS crimes.

Table 4: Prevalence of Cybercrimes in the Nigerian Banking Sector

Cybercrimes	Acceptance Frequency (Percentage)	Rejection Frequency (Percentage)	Remark
Phishing	291 (97.0%)	9 (3.0%)	Significant
Skimming	288 (96.0%)	12 (4.0%)	Significant
Malware	271(90.3%)	29 (9.7%)	Significant
DDoS	263 (87.7%)	37 (12.3%)	Significant

Source: Field Survey, 2021

Table 4 provides a summary of the responses of respondents with regard to the prevalence of cybercrimes perpetrated against commercial banks and their customers. The results show that on average, 291 respondents representing 97.0 percent posited that they had been involved in or have witnessed cybercrimes related to Phishing in their bank. Regarding cybercrimes related to Skimming, 288 respondents representing 96 percent claimed to have experienced it within their bank. 271 respondents representing 90.3 percent asserted the existence of cybercrimes related to malware, with 263 respondents representing 87.7 percent claiming that cybercrimes related to DDOs exist and are prevalent in their bank. The results indicate that cybercrimes are prevalent among commercial banks in Nigeria. Thus, the first

objective of the study is achieved.

Table 5: Regression Analysis

$PERF_t = \beta_0 + \beta_1 PHIS + \beta_2 SKIM + \beta_3 MALW + \beta_4 DDoS + \varepsilon_t$

Intercept	Coefficient	-0.325
	(t-statistics)	(-5.058)
	p-value	*0.000*
PHIS	Coefficient	-0.267
	(t-statistics)	(4.635)
	p-value	*0.000*
SKIM	Coefficient	-0.224
	(t-statistics)	(2.815)
	p-value	*0.006*
MALW	Coefficient	-0.591
	(t-statistics)	(10.431)
	p-value	*0.000*
DDoS	Coefficient	-0.269
	(t-statistics)	(3.191)
	p-value	*0.002*
R-Squared		94.9
F-Statistics (*p-value*)		372.048 (*0.000*)
Dependent variable		Bank Performance (PERF)

Denotations: PHIS = Phishing related Cybercrimes, SKIM = Skimming related Cybercrimes, MALW= Malware related Cybercrimes, DDoS = Distributed denial of services related Cybercrimes, PERF = Bank Performance indicators, CRMG = Cybercrime Risk Management.

The ordinary least square regression test reveals the following:

1. Cybercrimes related to phishing have negative effect on bank performance, with a negative coefficient of -0.267. The coefficient of -0.267 indicates that cybercrimes related to phishing decrease the performance of commercial banks by about 26.7%. The t-statistics value of 4.635>1.96, and a p-value=0.000 indicate that the effect is significant at 0.05 level of significance. Thus, it is upheld that cybercrimes related to phishing have significant reducing effect on the performance of commercial banks in Nigeria.
2. Cybercrimes related to skimming have negative effects on bank performance, with a negative coefficient of -0.224. The coefficient of -0.224 indicates that cybercrimes related to skimming decrease the performance of commercial banks by about 22.4%. The t-statistics value of 2.815>1.96, and a *p-value= 0.006* indicates that the effect is significant at 0.05 level of significance. Thus, it is upheld that cybercrimes related to skimming have significant negative effects on the performance of commercial banks in Nigeria.
3. Cybercrimes related to malware have negative effects on bank performance, with a negative coefficient of -0.591. The coefficient of -0.591 indicates that cybercrimes related to malwares decrease the performance of commercial banks by about 59.1%. The t-statistics value of 10.431>1.96, and a *p-value= 0.000* indicate that the effect is significant at 0.05 level of significance. Thus, it is upheld that cybercrimes related to malware have significant reducing effects on the performance of commercial banks in Nigeria.
4. Cybercrimes related to DDoS have negative effects on bank performance, with a negative coefficient of -0.269. The coefficient of -0.269 indicates that cybercrimes related to DDos decrease the performance of commercial banks by about 26.9%. The t-statistics value of 3.191>1.96, and a *p-value= 0.000* indicate that the effect is significant at 0.05 level of significance. Thus, it is upheld that cybercrimes related to DDoS have significant negative

effects on the performance of commercial banks in Nigeria.

Discussion of Findings

This section provides the discussion of the findings related to the objectives of the study. First, there is the prevalence of cybercrimes in Nigerian commercial banks. These cybercrimes include but are not limited to Phishing, Skimming, Malware and DDOs cybercrimes, which are all in practice. This finding is corroborated by Wakoli, Ogara and Liyala (2020) who found that cyber threats related to phishing, skimming, malware and DDos are increasing in the financial and banking industry.

Secondly, cybercrimes have significant effects on the performance and efficiency of the banking sector. The results revealed both positive and significant effects of the four dimensions of cybercrimes on the performance of banks in Nigeria. The results are confirmed by Uddin, Ali and Hassan (2021) who found that cybercrimes create operational risks for banks, and these cause losses, disrupts business operations, reduce public confidence, and create liquidity problems for banks as customers withdraw their deposits from such banks for fear of funds insecurity.

Conclusion and Recommendations

Cyber-security is unavoidable due to unknown loopholes in technological and online gateways. The security system always remains vulnerable to a certain extent due to its susceptibility to the growing and innovative cybercrime practices - given that insider risks could exist as cybercriminals can apply social engineering to trick users into releasing their confidential information. The failure of ensuring a fully secure cyber system imposes unexpected losses on the financial institutions.

This study has explained how cybercrimes related to phishing, skimming, malware and DDoS affect commercial banks' performance. The study concluded that these cybercrimes are powerful enough to reduce the performance, efficiency and competitive advantage of banks. Linking these areas has created a new study within the cybercrime discipline. This study thus contributes to gain more insight into the impact of cybercrime in the banking sector. Both customers and the bank can become cybercrime victims. The bank has several preventive measures, to minimize the risk of becoming a cybercrime victim and to create awareness among customers. Since the performances of commercial banks are daunted by the prevalence of cybercrimes in Nigeria, it is imperative that cyber risk management techniques be effectively implemented by banks, if they must continue in operation and earn returns on their services.

The study further recommends that banks should invest in advanced email security solutions to detect and prevent phishing attacks. Similarly, banks should introduce a multi factor authenticator for customers' account to aid extra layer security and prevent malware intrusion. Lastly, banks should also invest in DDOs mitigation services to protect against attacks that can disrupt banking services.

References

Ahmad, N., and Schreyer, P. (2016). *Measuring GDP in a Digitalised Economy.* Paris: OECD Publishing. doi:doi.org/10.1787/18152031

Aldasoro, I., Gambacorta, L., Giudici, P., and Leach, T. (2020a). Operational and cyber risks in the financial sector. *BIS Working Paper No. 840*. Basel, Switzerland: Bank for International Settlements.

Arachchilage, N. A. G., and Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behaviour*, 38: 304 – 312.

Bhasin, M. (2007). Mitigating cyber threats to banking industry. *The Chartered Accountant*, 55(10), 1618 – 1624.

Boer, M., and Vazquez, J. (2017). *Cyber Security and Financial Stability: How cyber-attacks could materially impact the global financial system.* Washington: The Institute of International Finance.

Böhme, R. and Moore, T. (2012). How do consumers react to cybercrime? *E-crime Researchers' Summit (E-crime), IEEE*, 1–12.

Brown, C. S. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology*, 9(01), 55 – 119. doi: 10.5281/zenodo.22387

Caron, F. (2015). *Cyber risk management in financial market infrastructures: elements for a holistic and risk-based approach to cyber security.* Belgium: National Bank of Belgium. Retrieved from https://lirias.kuleuven.be/1834699?limo=0

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers and Security*, 33(8), 719 – 731.

Cloward, R. A. and Ohlin, L. E. (1960). Delinquency and Opportunity: A theory of delinquent gangs. New York. The Free Press. In Schmalleger, F. (2006) *Criminology Today: An Integrative Introduction* (4th ed.). New Jersey: Pearson Prentice Hall. Pp. 323

Das, S., Mukhopadhyay, A., and Anand, M. (2012). Stock Market Response to Information Security Breach: A Study Using Firm and Attack Characteristics. *Journal of Information Privacy and Security*, 8(4), 27 – 55.

Donge, Z., Luo, F., and Liang, G. (2018). Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems. *Journal of Modern Power Systems and Clean Energy*, 1: 1 – 10.

Duran, R. E., and Griffin, P. (2019). Smart contracts: will Fintech be the catalyst for the next global financial crisis? *Journal of Financial Regulation and Compliance*, In Press.

Eling, M., and Lehmann, M. (2018). The Impact of Digitalization on the Insurance Value Chain and the Insurability of Risks. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 43(3), 359 – 396.

Eling, M., andWirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research*, 272(3), 1109 – 1119.

Geyres, S., and Orozco, M. (2016). *Think banking cyber-security is just a technology issue? Think again.* accenture strategy. Retrieved from https://www.accenture.com/t 20160419t004021_w_/us- en/_acnmedia/pdf-13/accenture-strategy-cybersecurity-in-banking.pdf

Gommans, L., Vollbrecht, J., Bruijn, B. G. D., and Laat, C. D. (2015). The Service Provider Group framework. A framework for arranging trust and power to facilitate authorization of network services. *Future Generation Computer Systems*, 45, 176 – 192.

Gopalakrishnan, R., and Mogato, M. (2016, May 19). Bangladesh Bank official's computer was hacked to carry out $81 million heist: Diplomat. *Reuters: Business News*. Thomson Reuters.

Gracie, A. (2015). *Cyber resilience: a financial stability perspective*: *Cyber Defence and Network Security conference.* London. Retrieved from https://www.bankofengland.co.uk/speech/2015/cyber- resilience-a-financial-stability-perspective

Granå sen, M., and Andersson, D. (2016). Measuring team effectiveness in cyber-defense exercises: a cross- disciplinary case study. *Cognition, Technology and Work,* 18(1), 121–143.

Hastings, B. (2015). Cyber-security: A growing concern for banking. *Journal of Investment Compliance*, 16(3), 5 – 7. https://doi.org/10.1108/JIC-01-2015-0005

Herath, T. and Rao, R. (2009) Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations. *European Journal of Information Systems*, 18, 106 – 125.

Hon, W. K., and Millard, C. (2018). Banking in the cloud: Banks' use of cloud services. *Computer Law and Security Review,* 34, 4 – 24.

Horne, R. (2014). *The cyber threat to banking.* PWC. Retrieved from https://www.bba.org.uk/wp-content/uploads/2014/06/BBAJ2110_Cyber_-report_May_2014_WEB.pdf

Hovav, A., and D'Arcy, J. (2004). The Impact of Virus Attack Announcements on the Market Value of Firms. *Information Systems Security*, 13(3), 32 – 40.

Johnson, K. N. (2015). Managing Cyber Risk. *Georgia Law Review*, 50(2), 548 – 592.

Juma'h, A. H., andAlnsour, Y. (2020). The effect of data breaches on company performance. *International Journal of Accounting and Information Management,* 28(2), 275 – 301.

Kamiya, S., KangJun-Koo, Jungmin, K., Milidonis, A., andStulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyber-attacks on target firms. *Journal of Financial Economics*, In Press.

Kopp, E., Kaffenberger, L., and Wilson, C. (2017). Cyber Risk, Market Failures, and Financial Stability, *Working Paper. International Monetary Fund (WP/17/185)*.

Kraemer-Mbula, E., Tang, P., and Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, 80(3), 541 – 555.

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

Langton, J. (2018, June 4). *Data breaches credit negative for BMO and CIBC: Moody's*. Retrieved from https://www.investmentexecutive.com/news/industry-news/data- breaches-credit-negative-for-bmo-and-cibc-moodys/

Lewis, J., and Baker, S. (2013). *The Economic Impact of Cybercrime and Cyber Espionage.* McAfee.

Longstaff, T., Chittister, C., Pethia, R., andHaimes, Y. (2020). Are we forgetting the risks of information technology? *Computer*, 33(12), 43 – 51.

Leukfeldt, R., Veenstra, S. andStol, W. (2013). High volume cyber crime and the organization of the police: The results of two empirical studies in the Netherlands. *Journal of Cyber Criminology,* 7(1).

Low, P. (2017). Insuring against cyber-attacks. *Computer Fraud and Security,* 4, 18-20.

Macaulay, T. (2018). *Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies* (1st ed.). Boca Raton: Taylor and Francis Group.

Manzoor, A. (2014). A Look at Efficiency in Public Administration: Past and Future. *SAGE Open*, 4, 1-5. https://doi.org/10.1177/2158244014564936

Mayahi, A., and Humaid, I. (2016). *Development of a Comprehensive Information Security System for UAE e-Government*. PhD thesis, Prifysgol Bangor University.

McConnell, Patrick, Blacker, and Keith. (2013). Systemic operational risk: does it exist and, if so, how do we regulate it? *The Journal of Operational Risk*, 8(1), 59 – 99.

Morton, M., Werner, J., Kintis, P., Snow, K., Antonakakis, M., Polychronakis, M., andMonrose, F. (2018). Security Risks in Asynchronous Web Servers: When Performance Optimizations Amplify the Impact of Data-Oriented Attacks. *IEEE European Symposium on Security and Privacy*, (pp. 167- 182).

Nwogwugwu, N., and Uzoechina, P. (2015).Cybercrime and Nigeria's economic development.

Journal of Humanities and Social Science, 20(5), 1 – 10.

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance? *Business Horizons,* 55, 349 – 356.

Sharma, A., and Tandekar, P. (2018). Cyber Security and Business Growth. *IGI Global*, 1208 – 1221.

Soomro, Z. A., Shah, M. H., and Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215 – 225.

Stokkel, M. and Smulders, A. (2013). Cyber-security: Hoe word het behapbaar? *Keynotes*, 42 – 26.

Teece, D. J. (2018). Profiting from innovation in the digital economy: Enabling technologies, standards, and licensing models in the wireless world. *Research Policy*, 47(8), 1367 – 1387.

Tendulkar, R. (2013). Cyber-crime, securities markets and systemic risk. *CFA Digest*, 43(4), 35 – 43.

Verma, M., Hussain, S.A. and Kuswah, S.S. (2012). Cyber Law: Approach to Prevent Cyber Crime. *IJRREST: International Journal of Research Review in Engineering Science and Technology*, 1(3), 123 – 129.