East African Scholars Journal of Education, Humanities and Literature

OPEN ACCESS

Abbreviated Key Title: East African Scholars J Edu Humanit Lit
ISSN: 2617-443X (Print) & ISSN: 2617-7250 (Online)
Published By East African Scholars Publisher, Kenya
Volume-8 | Issue-10 | Oct- 2025 | DOI: https://doi.org/10.36349/easjehl.2025.v08i10.006

Original Research Article

Cybercrimes and Bank Performance: A Study of Financial Technology Literacy Interventions in Cross River State

Martins Myke-okoi Okpa[1]*, Emmanuel Jabirwe Gwambeka[2], Mohammed Waziri[3], Solomon Mamman[4]

[1]Department of Sociology and Anthropology, Faculty of Social Sciences, University of Uyo, Uyo Nigeria
[2]Department of Criminology, Faculty of Social Sciences, Federal University of Kashere Gombe State, Nigeria
[3]Sa'adu Zungur University, Bauchi, Nigeria
[4]Department of Sociology, Faculty of Social Sciences, Federal University of Kashere Gombe State, Nigeria

Article History
Received: 04.07.2025
Accepted: 05.09.2025
Published: 21.10.2025

Journal homepage:
https://www.easpublisher.com

Quick Response Code

Abstract: Cybercrime has emerged as a pervasive and escalating challenge in Nigeria's banking industry, driven by the nation's increasing reliance on digital technologies. This study addressed critical gaps in understanding how cybercrimes impact bank performance, while also exploring the moderating roles of financial technology literacy interventions. The specific objective of this study is aimed to investigate the roles of financial technology (fin-tech) literacy interventions. The situational crime control theory was adopted. A descriptive survey research design was utilized, and the study's target population included bank employees and customers in Cross River State. The Godden formula for determining sample size in an infinite population was used in deriving a sample size of 384 respondents. Data were collected through questionnaire administered via personal contact, online methods (Google docs), and research assistants. Quantitative data were analyzed using SPSS Version 29. Descriptive statistics, correlation analyses, and Generalized Linear Model Multivariate Regression Analysis were employed to test the study hypotheses. The study revealed that financial technology literacy interventions, demonstrated a moderating effect reducing the negative impact of cybercrime on bank performance. Based on these findings, several recommendations were proposed. Financial institutions should prioritize cyber security measures and invest in financial technology literacy programmes for both employees and customers. Additionally, fostering collaborations with fin-tech companies can provide access to cutting-edge cyber security technologies and expertise.

Keywords: Cybercrimes, Bank Performance, Financial Technology, Literacy Interventions, Cross River State.

1. INTRODUCTION

Cyber attacks are becoming more frequent and sophisticated every year, with the financial industry consistently ranking as one of the most attacked industries. The rise of crypto universe has further increased the likelihood of hacks in the wider financial sector (Boissay *et al.*, 2022). Cybercrime refers to a series of organized criminal activities attacking both cyberspace and cyber security. In a broader sense it is defined as a criminal activity involving an information technology infrastructure: including illegal access or unauthorized access, illegal interception of data to or from within a computer system (Ehimen and Bola, 2009). Cybercrime may also be referred to as criminal activities that use a computer either as an instrumentality, target, or means of perpetuating further crime (Paranjape, 2012). Thus, cybercrime is an unlawful act wherein the computer is either a tool a target, or both.

There are various types of cybercrimes. Some of the more common types of cybercrime are phishing, demonstrated denial of service (DDOS) Attacks, hacking, and Identity Theft. Others are Web browser fraud, theft of monetary or card financial data, theft and selling of company data, cyber extortion (demanding money to avoid a threatened attack). Some of the most dangerous cyber hazards and strongest forms of Malware attacks are Ransom Ware, Trojan Horse Programs, Logic Bombs, Worms and Droppers (Gupta, 2012).

Attacks by cybercriminals pose a progressively more difficult problem, particularly for developing

***Corresponding Author:** Martins Myke-okoi Okpa
Department of Sociology and Anthropology, Faculty of Social Sciences, University of Uyo, Uyo Nigeria

nations. The goal of international cyber terrorism is to acquire sensitive information so that it can be used to gain complete control and substantial advantages. Different industries have been impacted by cybercrime, and the banking industry is one of them. This sector has seen various cybercrimes, such as ATM frauds, Phishing, identity theft, and denial of service attacks. In recent years, the banking industry has been hit by a global economic crisis that has forced it to restructure, particularly in some nations. Furthermore, both individual and industrial consumers have lost faith in the banking system, which has been severely harmed (Wada and Odulaja, 2012).

Computer criminals always seek unpermitted access to confidential data or financial falsified activity information. The implications of the rising cybercrime wave can make any country's biggest commercial decline, leading to financial damages, theft of trade secrets, negative impacts on financial institutions' goodwill and economic development. The loss of customer trust in the digital banking system is indirectly influenced by fraud and bribery across in both developed and developing nations (Buckley *et al*., 2019).

According to a study conducted by Akuta (2012), while the Internet has revolutionized modern society, most countries were not prepared for the unanticipated challenges of policing cyberspace with cybercrime on the rise. Now policing cybercrime has become a global problem that requires extensive resources. Over the past two decades, the world stage has observed the development of many policies and laws in support of promoting cyber safety. For Nigeria, cybercrime has become one of the most rapidly increasing types of crimes, particular among its unemployed younger population who possess college degrees (Hassan, Lass, and Makinde, 2012). Potential cyber criminals are readily persuaded because they believe they will not get caught or serve jail time due to the perception that cybercrime control has not been achieved (Okonji, 2015). Also, the significant financial gain is especially tempting (Drinkwater, 2014).

Cybercrimes have become a pressing concern for the banking sector worldwide. With the increasing reliance on digital technologies, banks are vulnerable to various forms of cyber threats, including phishing, identity fraud, hacking, and Demonstrated Denial of Service (DDoS) attacks. These cybercrimes not only jeopardize the security of financial institutions but also have the potential to significantly impact their performance. Understanding the dynamics between cybercrimes and bank performance is crucial in today's interconnected and technology-driven financial landscape. As cyber threats continue to evolve in sophistication, it is essential to explore how different dimensions of cybercrimes affect various aspects of bank performance, and how proactive measures, such as financial technology literacy interventions and collaboration with fin-tech companies, can mitigate these threats.

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 the $388 billion reported in 2011 (Nwogwugwu and Uzoechina, 2015).

Financial institutions bear the brunt of these cyber threats, making them primary targets for 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.

The banking sector faces an escalating risk of cybercrimes, including phishing attacks aimed at stealing sensitive customer information, identity fraud incidents that damage trust and financial stability, hacking events leading to data breaches, and disruptive DDoS attacks causing service interruptions. These cybercrimes can result in direct financial losses, regulatory fines, reputational damage, and reduced customer trust. To mitigate these risks, Nigerian banks have invested significant resources in security-monitoring tools, such as internal audits and employee checks. However, there remains a dearth of conclusive data regarding the precise financial toll of cybercrimes on the Nigerian banking sector. While it is challenging to quantify the losses accurately, it is essential to recognize that these cybercrimes also erode trust in financial institutions among both bank and non-bank populations. The erosion of trust negatively impacts market share and the reputation of banks, particularly in the realm of online payment platforms.

One critical issue exacerbating this problem is the lack of user awareness, leading to cyber vulnerability in Nigeria. Additionally, weak technical security processes and practices, such as outdated anti-virus software, mis-configured networks, and inadequate patch management, further expose organizations to cyber threats (Wolf Pack, 2014).

The study seeks to investigate the complex relationship between cybercrimes and bank performance including profitability, customer trust, and operational

efficiency. While it is evident that cybercrimes can have far-reaching consequences, a deeper understanding of how these crimes affect specific performance indicators is essential for devising targeted strategies to safeguard the banking sector.

2. REVIEW OF RELATED LITERATURE

2.1 Cybercrime Overview

Cybercrime expands beyond traditional types of crime with threatening ramifications to nations. According to Henrie (2013), cyber threats have the distinct possibility for remote and anonymous entities to destroy an organization's, a city's, a state's or a nation's operations. According to the Council of Europe's Convention on Cybercrime (2001), as cited by Olayemi(2014), cybercrime is a term used to refer to various criminal activities including crimes committed against computer information and systems and computer-related crimes (Olayemi, 2014). Research has shown that computer-related crimes have become a phenomenon that is swiftly developing in the 21st century (Akuta, 2012). Thus, cybercrime is described as crimes committed against the confidentiality, integrity, and availability of computer information or data and systems such as unauthorized access, illegal interception, data or system disruption, and unauthorized access to devices as well as computer-related frauds (Olayemi, 2014). The primary goal of cyber criminals is to gain unauthorized access to sensitive information (Gottschalk, 2010) that can later be used for economic gain or other benefits. As such, financial institutions and systems are the key targets of cyber-criminal activities in which increasing use of electronic banking technologies has exposed banks and its customers to more cyber threats and vulnerabilities than ever before (Fiebelkorn and Taggart, 2014).

Cybercrime is the illegal activity of grabbing through profit-driven illegal activities in the finance and banking sectors, including identity theft, financial fraud, e-mails, and internet fraud, and attempts to steal data from consumers, relation to finance account, internet banking, credit card or other bank account details. The main financial sector-related cybercrimes include DOS virus attacks, unauthorized entry, hacking and website defacement, according to Gordon and Loeb (2003).

Cybercrimes come in various forms, such as ATM frauds, identity theft, phishing, denial of service, hacking (Rathore and Marwaha, 2015). No doubt the Internet has created enormous opportunities for social, commercial, and educational activities. Wada and Odulaja (2012) posited that few innovations have changed the dynamics of banking as much as the electronic banking revolution. However, the same Internet innovation has also created electronic crime that has adversely affected Nigeria's image (Ibikunle and Odunayo, 2013). Cybercrime consists of any crime committed with computers and networks and also traditional crimes carried out through the Internet (Aduge-Ani, 2015). The Internet and other technology usages have immensely enhanced the chances of attacks from cyber criminals around the world (Raghavan and Parthiban, 2014). Consequently, cybercrime can be committed from any part of the world. The era of criminals stealing cash with shotguns over a bank counter is largely over. In the 21st century, there have been enormous increases in sophisticated fraudsters working in groups and in organized crime to steal a substantial amount from their computer and the Internet without apprehension.

2.2 Cybercrimes in the Banking Sector

The growth of technology significantly impacts the banking industry's service standards. ATMs and bank machines allow customers to conduct banking transactions outside regular business hours (Creado and Ramteke, 2020). One of the most prevalent ways that fraudsters target banks is through customers. Hackers take advantage of the innocence and inexperience of persons who are uninformed of the dangers that exist in the digital world and whom the hackers can persuade to supply critical information (Rowley, 2020). Customers may verify their checking accounts and make online banking payments without visiting a branch (Creado and Ramteke, 2020). As a result, the realm is moving toward a cashless model where consumers no longer need to carry currency to make transactions. Transferring money from their bank accounts to buy products like tickets, clothing, meals, or participate in initial public offerings is an option for bank clients (Creado and Ramteke, 2020).

In banking, customers, partners, and employees rely on the e-banking system's ability to protect personal and financial information, and technology must protect customers' information (Equinix, 2021). Security is a claim made by every software and hardware provider. Due to the prevalence of smart phones, banks have begun offering mobile banking to serve clients better. Customers use mobile phones to check bank accounts' balances and make money transactions over banking apps or websites (Equinix, 2021). Since this technology breakthrough, banks have linked attacks to mobile money transfers to clients' accounts. This e-banking has made worldwide banking transactions more convenient but a vulnerability to banking (Equinix, 2021). Banks use a range of anti-malware and anti-virus products across digital platforms.

Firewalls are a starting position, but they are not always adequate for keeping attackers at bay (Rowley, 2020). Banks will not be able to guarantee the safety of their digital surroundings unless they utilize the right software. The right software can protect a bank's digital system from being harmed by potentially dangerous attacks. As a result, banks invest necessary funds regularly in specialist cyber security measures (Rowley, 2020). Over half of banks employ third-party services to improve the efficiency of serving their businesses.

However, partnering with third-party companies with weak cyber security may be devastating for banks. Even if a bank has cyber security protections in place, it does not ensure that the companies with whom it works have adequate cyber security methods (Rowley, 2020).

To understand the security issues and the need for corrective steps, there is a need to understand the techniques and strategies used by cyber fraudsters in obtaining unauthorized access and use the financial information for purpose of fraud. Identity theft is one of the common techniques used by computer hackers when dealing with online businesses, in particular online banking medium, where fraudulent use of the identity of another person or third party, such as with the identities bank card, name, date of birth for criminal actions. Any information collected by cyber criminals via identity theft can be used for whatsoever purpose such as applying for loans, opening of account, credit card application (Isa *et al*., 2021). Cybercriminals frequently target these less-secure third-party partners, bringing harm to the institution. Third-party vendors might potentially be the target of attacks against banks' IT infrastructure and staff. However, if those third-party providers do not have adequate cyber protection in place, the bank could be the one to suffer the impact of the damage. Before deploying third-party solutions, it is critical to consider how the vendors can defend themselves from security vulnerabilities (Rowley, 2020).

Financial cybercrime increases with 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. Over the past few years, there have been 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 financial gain and have many forms (Arachchilage *et al*., 2014).

The Internet has undeniably boosted businesses' and bank institutions' revenue with e-commerce industries thriving internationally. To protect traffic entering and exiting web space applications, Internet providers often use secure sockets layer/transport layer security (SSL/TLS). Although this protects data, it does not protect current web browsers from tricking unknowing customers into revealing financial or personal information via email messages or fraudulent websites. As customers are continually relying on the Internet for various business transactions and other personal financial activities, so are cybercriminals.

Financial institutions use a range of financial technology to improve customer service. Banking cyber-attacks that utilize botnets and Trojan horses to trick employees and customers into giving up their credentials are a growing problem for web applications (Creado and Ramteke, 2020). Denial-of-service attacks, which damage a company's reputation, are common against financial institutions, including banks and insurance firms (Creado and Ramteke, 2020). When cybercriminals attack, they can obtain sensitive information. In addition, the attacks can disrupt banking institutions using different methods such as phishing emails, impersonation, and account hacking, allowing them to steal money from personal accounts (Akinbowale *et al*., 2020). When it comes to illegal activities, cybercrime encompasses everything that involves computers or networks. Fraud, unsolicited emails, and unlawful intrusion into remote networks to steal bank businesses' secrets are possibilities (Alese *et al*., 2018). End-to-end customer appliances such as smart phones and tablets frequently are utilized to conduct digital transactions, and devices must be protected. Confidential data passes across these networks. If a customer device becomes infected with malware, it can pose a significant threat to the bank's network if it is not protected (Uddin *et al*., 2020).

Despite the fact that the term cybercrime has entered into 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 the 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.

As the financial sector globally relies more on cyber technology for operations and services delivery, banks and financial institutions increasingly expose 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 aftermath 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).

Cybercriminals generally infiltrate into the system and remain quiet to monitor user activities before the attack and reap their benefits with maximum damage for the institution at the right opportunity. Therefore, cyber hackers can disrupt the financial system to prevent fund transfers between banks, steal confidential data while transmitting through the banking system, and damaging the operations of other sectors that rely on the integrated banking services (Duran and Griffin, 2019).

Therefore, the Basel committee suggests banks and financial institutions globally to 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).

Boer and Vazquez (2017) analyze that 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. Ahmad and Schreyer, (2016) explain 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.

Cyber-security in the financial industry has emerged as an operational issue since online-based criminal activities, frauds, 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). Likewise, criminals can steal customers' identity and PIN to avail banking services and withdraw cash. These types of criminal activities involving fraudulent transactions may have litigation risks for financial institutions besides direct economic losses.

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 and Blacker,2013). The system failure can occur for many reasons, but the operational consequence of an intentional system failure initiated by cybercriminals is challenging to estimate 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 (example, 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. Malware refers to a contraction of 'malicious' and 'software'. 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 criminals (Manzoor, 2014). Phishing affects financial organizations, in particular 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. Another form of cybercrime is skimming. Skimming refers to stealing customer card information and Personal Identification Numbers (PINs). Criminals installed skimming devices at Automatic Teller Machines (ATM's) to steal this kind of confidential information (Choo, 2011). Skimming is the illegitimate copying of data from an electronic payment card such as a cash point card or a credit card. Skimming often involves the theft of pin codes with the final objective of making payments or to draw money from the victim's account.

According to Adeyemi (2022) findings show that as more Nigerians are embracing e-transactions daily, so is the surge in cybercrimes, as cybercriminals are getting adept in the clean sweep of bank accounts of unsuspecting users. While banks are facing a dearth of IT staff to promptly respond to cyber threats, bank account compromises are expected to get worse as the festive season approaches. Already, the Nigerian Communications Commission (NCC) has issued 10 cyber alerts to warn Nigerians about the possible danger associated with or targeted at some platforms, including Cisco and lately telegram, which these cyber criminals exploit to cause havoc.

Indeed, cybercrime has been projected to worsen as e-payment transactions gain more patronage. Statistics from the Nigeria Inter-Bank Settlement Systems (NIBSS) showed that transactions worth N32.3 trillion were performed electronically in August, a volume that has been on steady monthly growth through the NIBSS Instant Payment platform (NIP), bringing the total value of e-payment deals in the first nine months of the year to N271.5 trillion. According to NIBSS, the value of the e-payment recorded was a reflection of the increase in the volume of deals within the month. The NIP volume rose to 448 million in August, showing a 10.6 per cent increase over 405 million recorded in the preceding month. Activities of cybercriminals have taken a new turn, as they become more daring and innovative and subsequently unleash more terror on their prey. Almost on a weekly basis, bank customers complain of hacked accounts, where criminals wipe out all their life savings. The Guardian checks showed that this is not peculiar, but cuts across the entire banking sector.

Between July and September 2020, Nigerian banks, according to NIBSS, lost N3.5 billion to fraud-related incidents, representing a 534-per cent increase from the same period in 2019, when it was N552 million.

Though the latest data have yet to be confirmed, stakeholders are worried that the losses would be huge compared to previous years.

Cyber crimes occurrence within financial institutions and banks particularly had continued to record increase in its occurrences and rates. According to a punch newspaper report published in December 2022 shows that cyber crime is really prevalent in the country, as data from Economic and Financial Crime Commission indicates that the commission secured 3,440 convictions on financial and cyber crimes across the country from January to November 2022.

2.3 Cybercrime and Bank Performance

Menon and Guan-Siew (2012) discussed how the increase in cybercrime is posing a significant concern globally. Economic crimes distort the smooth flow of investment and trade, and it also threatens the integrity of financial markets and world security through financing terrorism (Menon and Guan-Siew, 2012). According to Nabi and Islam (2014), a secure cyberspace is a major element of protecting national security in the age of globalization. It plays a huge role in accomplishing economic prosperity and integrity defense of a country. Therefore, it is vital for a nation to build a strong, modern, and industrial society with enhanced technology awareness. However, with the enhanced and rapid development of ICTs, cyber attacks have equally become a global problem. This study presents various types of cybercrimes that are impacting the nation's economy and its financial system either directly or indirectly.

Cyber-attacks are key financial sector operational risks because economic sectors are increasingly dependent on other industries to carry out its operations successfully. Ultimately, security is a huge factor that can determine the success of electronic banking (Usman and Shah, 2013). The connection between cybercrime and the banks' effectiveness in managing available resources to combat these crimes is critical.

Aduge-Ani (2015) reported that about 2.4% of banking revenue went to fraud cases in 2015, with Nigerian banks losing N159 Billion Naira to electronic bank frauds between 2000 and the early part of 2013 (Aduge-Ani, 2015). As such, increasing use of electronic banking technologies has exposed banks and their customers to more cyber threats and vulnerabilities than ever before (Fiebelkorn and Taggart, 2014). For example, a cybercriminal gaining access to vital information could potentially steal confidential customer financial and personal records (Zelleand Whitehead, 2014). Also, a computer virus could cripple critical operating systems and shut down an organization for days or even weeks.

Kopp *et al*., (2017) highlighted that security system breakdown may signal the cyber-infrastructure vulnerability which has appeared as a new risk factor in the financial industry (Macaulay, 2018). Therefore, system vulnerability creates an opportunity for hackers to exploit the system and inflict both direct and indirect losses for the financial institutions that would impact earnings, growths, and risks of the breached institutions (Juma'h and Alnsour, 2020; Kamiya *et al*., 2021). The vulnerability of the security system affects earnings because of the loss of operational efficiency affecting productivity, which in turn negatively influences the growth and overall business risk of an institution.

The effects of a cyber breach and malicious activities may reach far away from the measurable direct financial losses due to the direct and indirect costs for the loss of customers' confidence, opportunity costs for service breakdown, costs for incidence detection and cleaning up in the aftermath of cybercrime, costs associated with the loss of confidential business information and intellectual property, and loss of reputational damage of the hacked institution (Horne, 2014). Therefore, both expected and unexpected losses for cyber-security incidences could impact banks and financial institutions. Importantly, the unexpected losses from cyber-security breaches increase earnings uncertainty, and thus investors in the financial market respond negatively to publicly announced cyber breaches (Das *et al*., 2012). Overall, as the losses from cyber breaches are so pervasive, cyber insurance alone cannot mitigate the cyber-security risk of an institution (Low, 2017).

Banks and financial institutions also 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. Therefore, the adverse effect of cyber-security hazards on banks' corporate earnings is a concern for researchers and practitioners.

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.

According to Eze (2021) cyber-attacks pose a very real risk in their potential for crime and for imposing economic costs far out of proportion to the price of launching the attack. Hurricane Andrew, the most expensive natural disaster in U.S history caused $25 billion dollars in damage and the average annual cost from tornadoes; hurricane and flood damage in the U.S is estimated to be $11 billion. In contrast, the love bug virus is estimated to have cost computer users around the world somewhere between $3 billion and $15 billion.

The financial costs to economies from cyber-attack include the loss of intellectual property, financial fraud, damage to reputation, lower productivity and third party. Commercial banks experience huge financial loses each year which are often kept hidden from the public to prevent investors and customers from being alarmed by the high level of insecurity or to protect their reputation. For instance, in 2019 Apex bank (CBN) confirmed that transaction valued at N6.5 trillion was stolen by hackers of commercial banks in Nigeria. Similarly, Nigeria inter-bank system (NIBSS) states that, between 2014-2018 commercial bank lost over N12.30 billion to internet fraud in Nigeria (Internet World Statistics, 2018).

African Academic Network on Internet Policy (2020) assets that point of sales (POS) might be susceptible to data breaches as a result of its global growth. In 2013, a Trojan POSRAM malware was used to steal payment card information of about 70 million customers belonging to a retail giant, banking with a commercial bank in Nigeria. Such huge losses are not good for the economy of the country and make one wonder how banks are able to recover from such. The Economic and Financial Crimes Commission Report (EFCC, 2015) places Nigeria as third among the top ten sources of cyber crime in the world with 8 percent, following after United States with 65 percent of cyber-criminal activities and the United Kingdom with 9.9 percent.

The incident of cybercrime has also given Nigeria a bad image as one of the most corrupt nations in the world. This tarnished national image affects the way Nigerians are treated abroad with suspicion and extreme caution as Nigerians are stereotyped to be 419ers. More so, private companies around the world are beginning to take steps geared towards blocking e-mail originating from the country and financial instrument are accepted with extreme caution. Foreign investors are also scared of the country, considering it as risky and unattractive business zone. In the same vein, identity takeover affect online banking, thereby affecting the economy. This is because new accounts can be taken over by identity thieves, thus raising concerns regarding the safety of financial institutions in Nigeria (Eze, 2021).

The Central Bank of Nigeria recently reported that the banking industry has lost well over N20 billions Naira on cybercrime (Odeyemi, 2013). Furthermore, cybercrime has left the level of subsistence and has penetrated into a very high-level commercial scale by well-connected and highly organized professionals, and in some cases, by big organizations (Odeyemi, 2013). Nwadike (2014) stated that the Central Bank received and processed well over 6,274 complaints from various financial crimes in 2012, which were mostly in advance fee frauds. In 2013, actual loss due to fraud was N485.194 billion, and N6.216 billion, Naira in 2014. According to Nwadike (2014), Nigerian banks should wake up to the realities of cybercrime in the industry, emphasizing the need for banks to consider internal and external factors when planning on implementing security mechanisms.

In 2019 the Apex bank (CBN) confirms that transaction values at N6.5 trillion were stolen by hackers on commercial banks in Nigeria. Nigeria Inter-bank System (NIBSS) states that between 2014–2018, commercial banks have lost over N12.30 billion to internet fraud in Nigeria. Recent report says that point of sale (POS) might be susceptible to data breach as a result of its global growth. In 2013, a Trojan POSRAM malware was used to steal payment card information of about 70 million customers belonging to a retail giant, banking with a commercial bank in Nigeria. (African Academic Network on Internet Policy, 2020).

According to Adams and Benham (2016), cyber security lapses are likely to affect financial institutions' reputation and this could have a devastating effect on corporate institution identity. George, Owoyemi and Onakala (2012) make an assessment that good corporate image, aims and corporate core values help to promote a sense of belonging for customers and other corporate stakeholders alike, they conclude that, reputation is directly correlated to the corporate identity.

According to Horne (2014), the magnitude of cybercrime on financial institutions goes beyond simply financial loses. The author argues that, there are intangible costs associated with the loss of stakeholders' confidence, as well as the opportunity costs of service disruptions and damage control after cyber incidents, and many other costs such as increased cyber security mechanisms are all regarded as critical risks to financial institutions' reputation.

According to Brockett, Golden and Wolman (2012), cyber risk remains the key problem to every organization, be it public or private, due to its impact on the core of an institution's information and reputation. They are of the view that when a network attack happens, it creates massive problems for the institution's brand image which becomes a tangible loss, which may have a negative effect on the financial reports of the institution in question.

The threat of cyber assault is increasing. As banks roll out more digital services, and as more customers use technology to handle their money, this advancement has made it easy for fraudsters to attack and extract customers' information at any stage of the financial transactions (Howarth, 2015). The author adds that banks have recorded an increase in cybercrime which has put them in a high-risk bracket for network breaches.

2.4 Financial Literacy

The internet is already turning into a global network that brings together millions of computers located in different countries and exposes the wide chances of obtaining and exchanging data that so many are now using for illegal acts due to financial problems according to Baker and Glasser (2005), Cybercrime can be categorized as a technology-based crime, a PC and a web-based crime involving governments, commercial enterprises, including global citizens, and cybercrime, a system of piracy, free telephone calls, cyber-bullying, cyber-terrorism and cyber- pornography (Schell and Martin, 2004).

The knowledge of Internet banking is neglected among too many Southern African banks (Dzomira, 2016). On their websites, many companies have developed less than half of the mobile banking fraud awareness available. This indicates that, without comprehensive training of possible internet risks, most cash flow clients take an interest in Internet banking transactions. Most financial clients participate in Internet banking transactions without adequate knowledge of possible internet risks and attacks. As a result, there is a strong probability that Internet banking may be the target of fraud.

It is important in day-to-day lifestyle because it equips customers on knowledge and skills that we need to manage money effectively. Otherwise, with the lack of knowledge, any financial decision made is not success or even face losses to the individual or company. As an institution, it is therefore important to focus on financial knowledge in program will equip staff and clients of banks with the awareness of how they're being tricked to improve these habits. It is also critical to have intelligence with some well threats, regular vulnerability checks performed either by IT security team, including good cyber hygiene overall.

Similarly, As Internet users have increased considerably, so is cybercrime. So, it is the responsibility of one and those that use the internet to be aware of it. Cybercrime and cyber law have been developed to deal with cybercrimes. Various approaches are used to raise cyber security awareness, including corporate security awareness posters, security awareness material on the intranet website, and information on a screensaver, in-class training, videos, simulations and tests. That said, with the increase in cybercrime incidents, there is an urgent need for effective measures to tackle crime.

A simple training strategy aimed at improving the ability of consumers, employees, and the public to distinguish a fraudulent email from a real one could reduce a significant proportion of phishing-related cybercrimes. Education can help victims to be aware of cybercrime like phishing. This view was supported by (Abdul-Rasheed *et al*. 2016), who posited that education is a very important factor in combating cybercrime and that persons need to be educated on how to prevent cybercrime, how cybercrime works and the harmful effects of cybercrime in society.

From the above empirical literature, the following hypothesis is thus conjectured.

H_o: Fin-tech literacy interventions do not significantly reduce cybercrimes impact on bank performance in Cross River State.

2.6 Theoretical Framework

2.6.1Situational Crime Prevention Theory

This theory is credited to R. V. Clarke (1980), and looks to develop greater understanding of crime and more effective crime prevention strategies through concern with the physical, organizational and social environments that make crime possible. The crux or major assumption of this theory is concerned with (the immediate physical and social settings, as well as wider social arrangement). Clarke summarizes his theory as the science and art of decreasing the amount of opportunities to crime, using measures directed at highly specific forms of crime that involve the management, design or manipulation of the immediate environment in a systematic and permanent way.

The foundation of the situational crime concept relies also on the assumption that more opportunities lead to more crime, easier ones attracts more offenders and such existence of easy opportunities makes possible for a life crime. The theory goes further to propose that crime prevention or the intervention to prevent a crime from occurring can be achieved in two ways: (1) changing the offender's disposition or (2) reducing his or her opportunities. This is based on the premise that crime can be reduced effectively by altering situations rather than the offender's personal dispositions.

Clarke (1980) primarily divides crime prevention approaches into three categories of measures namely; degree of surveillance, target hardening measures and environmental management. These approaches are further summarized into sixteen (16) opportunity-reducing techniques as seen below: (Target hardening, Access control, Deflecting offenders, Controlling facilitators, Entry and exit screening, Formal surveillance, Surveillance by employees, Natural surveillance, Target removal, Identifying property, Reducing temptation, Denying benefits, Rule setting,

Stimulating conscience, Controlling dis-inhibitors, Facilitating compliance).

The situational crime prevention theory is relevant and explains well the phenomenon of cyber crime and financial institutions. This is so because, the theory presents assumptions that best explains and proposes the pathways to crime prevention, such as taking control of the physical, organizational and social environment that makes crime possible. Cyber criminals take advantage of the loopholes in the online banking platforms to carry out or perpetuate their activities. Therefore, applying the assumptions of the situational crime prevention theory which states that more opportunities leads to more crime and thus proposes opportunity reducing techniques such as target hardening, access control, deflecting offenders, surveillance amongst others.

The above proposition calls on financial institution and banks generally to be proactive and invest more in securing and continually updates all its internet platforms so as to prevent encroachment from cyber criminals. Also, as preventive measure, it is important that stringent laws and rules with appropriate sanctions are put in place by concerned organizations, but most importantly financial institutions should adopt a partnership approach with the security authorities already in place to achieve meaningful success.

The study therefore, adopts both the Institutional Anomie Theory and the Situational Crime Prevention Theory based on the premise that all theories provides explanations on not just opportunities leading to crime causation, but also proposes ways on how to tackle and prevent crime. The issue of cybercrime is a serious one and continually affecting institutions and individual in many negative dimensions. It is therefore pertinent that a holistic approach is adopted towards tackling the menace called cyber crime.

3. METHODOLOGY

This study adopts a descriptive and survey research design, this research design is considered for the study in view of the fact that the study seeks to investigate on cyber crimes and bank performance with focus on financial technology literacy intervention in Cross River State and drawing inferences from selected commercial banks across the state.

The population of this study was made up of residents of Cross River State; respondents were drawn from the three senatorial districts of the state, through a sampling method (Cross River South 154, Cross River Central 115, and Cross River North 115). The target population for this study included staff and customers of banks located in Cross River State. The banks studied include: Access Bank Plc, Ecobank Nigeria Plc, Fidelity Bank Plc, First Bank Nigeria Limited, First City Monument Bank Plc, Globus Bank Limited, Guaranty Trust Bank Plc, Heritage Banking Company Ltd, Keystone Bank Limited, Polaris Bank Plc, Stanbic IBTC Bank Plc, Sterling Bank Plc, Union Bank of Nigeria Plc, United Bank for Africa Plc, Unity Bank Plc, Wema Bank Plc, Zenith Bank Plc.

The multistage sampling technique was adopted. The study area was stratified into three regions based on their senatorial district. Furthermore, one local government area was selected from each of the senatorial district. Respondents were drawn from three local government areas (Calabar, Ikom, and Ogoja) which are urban centers and commercial hubs.

Due to the unknown nature of the population, the sample size of the study was determined using a formula for an unknown population as suggested by Godden (2004).

The formula is expressed as:

$$n = \frac{Z^2PQ}{e^2}$$

Where:
n = Sample size
Z = Percentage point for the standard normal probability distribution at the specific confidence interval (e.g. Z value 1.96 for 95% confidence level).
P = Percentage of picking a choice.
Q = Percentage of not picking a choice (I – P)
e = Margin of error (5%)

$$n = \frac{(1.96)^2 0.50(1 - 0.50)}{0.05^2}$$

$$n = \frac{3.8416 * 0.50 (1 – 0.50)}{0.5^2}$$

$$n = \frac{1.9208 * 0.50}{0.0025}$$

$$n = \frac{0.9604}{0.0025}$$

n = 384

Thus, the sample size used for the study is three hundred and eighty four (384). Three local government areas (Calabar, Ikom and Ogoja) which are urban centres and commercial hubs in each of the senatorial districts were purposively selected; these local government areas served as strata's for the study. Furthermore, a total of seventeen (17) commercial banks were selected for the study, (7) banks in Calabar and (5) each from Ikom and Ogoja local governments areas. 22 questionnaire were distributed to each 7 selected banks in a Calabar, summing up to 154, while 23 questionnaire were distributed to each of 5 selected banks in Ikom, summing total of 115, and 23 questionnaire were also administered to each of the 5 selected banks in Ogoja, summing up to 115. This brings to a total of 384 questionnaires administered to respondents.

The data drawn from the field through questionnaire was analyzed by the use of descriptive statistics using Statistical Package for Social Sciences

(SPSS Version 29). Descriptive statistics and correlation analyses were performed on the data collected. Generalized Linear Model and Multivariate Regression Analysis were employed to test the study hypotheses.

The formulated hypotheses were tested with the Generalized Linear Model Regression. The analytical model for testing the research hypotheses is specified below:

To test hypotheses, the model below was specified:

$BANKP = \beta_0 + \beta_1 CYBER + \beta_2 FTLI + \beta_3 CYBER*FTLI + \varepsilon_t$

Where:

CYBER denotes combined cybercrime (measured average of all four types of cybercrimes)

FTLI denotes Financial Technology Literacy Intervention (moderating variable)

4. RESULTS AND DISCUSSIONSOF FINDINGS

4.1 Socio-Demographic Data of Respondents

Table 1: Demographic Data

Variable	Options	Frequency	Percentage
Gender	Male	183	52.3
	Female	167	47.7
	Total	**350**	**100.0**
Age	Less than 21	45	12.9
	21-25	55	15.7
	26-30	35	10.0
	31-35	65	18.6
	36-40	50	14.3
	41-45	35	10.0
	46-50	40	11.4
	Above 50	25	7.1
	Total	**350**	**100.0**
Education	Bachelors	130	37.1
	Masters	110	31.4
	Doctorate	40	11.4
	Other Degrees	40	11.4
	Professional Qualifications	30	8.6
	Total	**350**	**100.0**
Respondent Category	Bank Staff	163	38.9
	Bank Customer	214	61.1
Cross River South	**Total**	**350**	**100.0**
	Bank Staff	56	16
	Bank Customer	85	24.2
Cross River Central	Bank Staff	40	11.4
	Bank Customer	62	18
Cross River North	Bank Staff	40	11.4
	Bank Customer	67	19
	Total	**350**	**100**

Source: Field Survey, 2024

Table 1 presents the demographic data of 350 sampled respondents. Of the 384 sampled respondents, completed questionnaires were collected from 350. This number formed the basis for the analysis in this study. The results indicate that there are 183 male respondents representing 52.3 percent of the total respondents, with 167 female respondents representing 47.7 percent of the total respondents.

In terms of age distribution, the highest representation in the study was observed among respondents between the ages of 31 to 35 years, comprising 18.6 percent of the total sample. The second highest representation was observed among respondents between the ages of 21 to 25 years, accounting for 15.7 percent of the total sample. The third highest representation was among respondents between the ages of 36 to 40 years, comprising 14.3 percent of the total sample. Those below 21 years of age made up about 12.9 percent of the sample size, and the number of respondents between 46 and 50 years represented 11.4 percent of the total sample. Additionally, there were an equal number of respondents in the age categories of 26 to 30 years and 41 to 45 years, with each representing 10.0 percent of the total sample. The least-represented age group in the study was respondents above 50 years of age, representing 7.1 percent of the total sample.

Regarding educational qualification, the most represented group were respondents holding bachelor's degrees, with a total of 130 respondents, making up 37.1 percent of the total sample. The second most represented group were respondents holding master's degrees, with a total of 110 respondents, representing 31.4 percent of the total sample. The number of respondents holding doctorate degrees was equal to the number of respondents holding other degrees, with each group comprising 40 respondents, representing 11.4 percent of the total sample. Respondents holding professional qualifications were 30, making up 8.6 percent of the total sample.

Regarding the category of the respondents, 142 respondents representing 40.6 percent were bank staff (including managers and employees), while, 208 respondents, making up 59.4 percent of the total sample were bank customers.

4.2 Presentation of Responses Regarding Performance of Bank

Data in Table 2 presents the responses regarding poor bank performance.

Table 2: Responses to Bank performance (Poor performance Indicators)

Items	BANKPv1	BANKPv2	BANKPv3	BANKPv4	BANKPv5	BANKPv6
	(%)	(%)	(%)	(%)	(%)	(%)
SA	15.7	24.3	31.4	32.3	27.7	20.0
A	61.4	37.1	50.0	39.1	42.3	51.4
U	14.3	22.9	7.1	18.6	18.6	20.0
D	7.1	8.6	7.1	8.6	5.7	5.7
SD	1.4	7.1	4.3	1.4	5.7	2.9
Total	100.0	100.0	100.0	100.0	100.0	100.0

Source: Field Survey, 2024

BANKPv1 = Cyber attacks have led to high cost of financial transactions among banks
BANKPv2 = Cyber attacks have led to lower levels of profitability of banks
BANKPv3 = Cyber attacks have resulted in the loss of huge sums of money by banks
BANKPv4 = Cyber attacks have led to service unavailability and business disruptions for banks
BANKPv5 = Cyber attacks have led to operational inefficiencies for banks in an attempt to patch vulnerabilities
BANKPv6 = Cyber attacks have led to reputational damage for banks due to loss of confidence in banks' digital platforms.

Regarding item BANKPv1, 15.7 percent strongly agreed, 61.4 percent agreed, 14.3 percent were undecided while 7.1 percent and 1.4 percent disagreed and strongly disagreed respectively. The responses indicate that cyberattacks have led to high costs of financial transactions among banks.

Regarding item BANKPv2, 24.3 percent strongly agreed, 37.1 percent agreed, 22.9 percent were undecided while 8.6 percent and 7.1 percent disagreed and strongly disagreed respectively. The responses indicate that cyber attacks have led to lower levels of profitability for banks.

Regarding item BANKPv3, 31.4 percent strongly agreed, 50.0 percent agreed, 7.1 percent were undecided while 7.1 percent and 4.3 percent disagreed and strongly disagreed respectively. The responses indicate that cyber attacks have resulted in the loss of huge sums of money by banks.

Regarding item BANKPv4, 32.3 percent strongly agreed, 39.1 percent agreed, 18.6 percent were undecided while 8.6 percent and 1.4 percent disagreed and strongly disagreed respectively. The responses indicate that cyber attacks have led to service unavailability and business disruptions for banks.

Regarding item BANKPv5, 27.7 percent strongly agreed, 42.3 percent agreed, 18.6 percent were undecided while 5.7 percent and 5.7 percent disagreed and strongly disagreed respectively. The responses indicate that cyber attacks have led to operational inefficiencies for banks in an attempt to patch vulnerabilities.

Regarding item BANKPv6, 20.0 percent strongly agreed, 51.4 percent agreed, 20.0 percent were undecided while 5.7 percent and 2.9 percent disagreed and strongly disagreed respectively. The responses indicate that cyber attacks have led to reputational damage for banks due to loss of confidence in banks' digital platforms.

4.3 Presentation of Responses Regarding the Moderating Variables of the Study

Data in Table 3 presents the responses regarding financial technology literacy interventions.

Table 3: Responses to Financial Technology Literacy Intervention.

Items	FLTIv1		FLTIv2		FLTIv3	
	Freq.	(%)	Freq.	(%)	Freq.	(%)
SA	108	30.9	80	22.9	18	5.1
A	147	42.0	165	47.1	222	63.4
U	65	18.6	70	20.0	45	12.9
D	20	5.7	20	5.7	40	11.4
SD	10	2.9	15	4.3	25	7.1
Total	350	100.0	350	100.0	350	100.0

Source: Field Survey, 2024

FLTIv1 = Banks regularly send emails regarding keeping financial information safe.
FLTIv2 = Banks frequently send emails on how to identify possible cybercrimes and attacks.
FLTIv3 = Banks have included in their apps information regarding cybercrimes.

Regarding item FTLIv1, 30.9 percent strongly agreed, 42.0 percent agreed, 18.6 percent were undecided while 5.7 percent and 4.3 percent disagreed and strongly disagreed respectively. The responses indicate that banks regularly send emails regarding keeping financial information safe.

Regarding item FTLIv2, 22.9 percent strongly agreed, 47.1 percent agreed, 20.0 percent were undecided while 5.7 percent and 2.9 percent disagreed and strongly disagreed respectively. The responses indicate that banks frequently send emails on how to identify possible cybercrimes and attacks.

Regarding item FTLIv3, 5.1 percent strongly agreed, 63.4 percent agreed, 12.9percent were undecided while 11.4 percent and 7.1 percent disagreed and strongly disagreed respectively. The responses indicate that banks have included in their mobile apps information regarding cybercrimes.

4.4 Test of Hypotheses

Table 4: Test of Hypothesis (Moderating role of fin-tech literacy intervention)

	Coefficient	Std Error	t-statistics	p-value
Constant	-.541**	.142	-3.796	.000
CYBER	.764**	.071	10.50	.000
FTLI	-.794**	.072	-11.02	.000
CYBER*FTLI	-.099 **	.015	-6.330	.000
R-SQD	.928			
F-Statistic	1495.40			
F (p-value)	.000			

Table 4 shows the role of financial technology literacy intervention in moderating the relationship between cybercrimes and dwindling bank performance. Similar to the direction of the effects of individual variables of cybercrimes in Table 4, the combined cybercrime variable (CYBER) has a positive effect on bank poor performance. The coefficient for CYBER is 0.764, indicating that a one-unit increase in CYBER is associated with a 0.764 unit increase in the banks' poor performance. This reinforces the positive relationship between cybercrimes and banks' poor performance. The very low p-value (< 0.001) indicates that this relationship is statistically significant.

The coefficient for FTLI is -0.794, indicating that a one-unit increase in FTLI is associated with a -0.794 unit decrease in banks' poor performance. This suggests that FTLI has a negative relationship with poor bank performance, meaning that higher levels of fin-tech literacy intervention are associated with better bank performance. The very low p-value (< 0.001) confirms the statistical significance of this relationship. This implies that banks' financial technology literacy interventions can improve their performance.

The interaction term CYBER*FTLI represents the combined effect of CYBER and FTLI on banks' poor performance. The coefficient of -0.099 indicates that for each one-unit increase in CYBER and FTLI, there is a -0.099 unit decrease in banks' poor performance. This interaction term measures the moderating effect of FTLI on the relationship between cybercrimes (CYBER) and poor bank performance. The negative coefficient suggests that FTLI moderates the relationship, meaning that the impact of CYBER on poor bank performance is reduced when FTLI is higher. The more the fin-tech literacy interventions undertaken by banks, the less the incidence of cybercrimes, which further improves the performance of banks.

Ho*: Fin-tech literacy interventions do not significantly reduce cybercrime impact on bank performance in Cross River State*

Hi*: Fin-tech literacy interventions significantly reduce cybercrime impact on bank performance in Cross River State*

The coefficient of -0.099 on the CYBER*FTLI variable has a p-value of 0.000, which is significant at the 0.05 level. Again, the t-calculated (t-cal) absolute value of 6.33 exceeds the t-critical (t-crit) value of 1.97 (350-4 df0.05). A significant p-value less than 0.05 and a t-cal value exceeding the t-crit indicate that the null hypothesis five is rejected. Thus, fin-tech literacy interventions significantly reduce cybercrime impact on bank performance in Cross River State.

4.2 DISCUSSION OF FINDINGS

The objective of the study sought to look at the moderating role of financial technology literacy intervention on bank performance. The objective looked at the role of financial technology literacy intervention (FTLI) in improving bank performance. The regression analysis indicates a coefficient of -0.794, indicating a negative association. Meaning that as financial technology intervention (FTLI) increases, bank performance improves. Additionally, the interaction term CYBER*FTLI is significant, with a coefficient of -0.099, suggesting that FTLI moderates the relationship between cybercrimes (CYBER) and poor bank performance.

The hypothesis which states *Ho: Fin-tech literacy interventions do not significantly reduce cybercrime impact on bank performance in Cross River State* The coefficient of -0.099 on the CYBER*FTLI variable has a p-value of 0.000, which is significant at the 0.05 level. Again, the t-calculated (t-cal) absolute value of 6.33 exceeds the t-critical (t-crit) value of 1.97 (350-4 df 0.05). A significant p-value less than 0.05 and a t-cal value exceeding the t-crit indicate that the null hypothesis five is rejected. Thus, fin-tech literacy interventions significantly reduce cybercrime impact on bank performance in Cross River State.

The moderating role of financial technology literacy intervention, the regression results indicate that fin-tech literacy intervention (FTLI) has a negative coefficient of -0.794, implying that as FTLI increases, bank performance improves. Additionally, the interaction term CYBER*FTLI is significant, with a coefficient of -0.099, suggesting that FTLI moderates the relationship between cybercrimes (CYBER) and poor bank performance. This means that when banks invest in fin-tech literacy interventions, they can mitigate the negative impact of cybercrimes on their performance.

The findings of the study are in line with the assertion of Abdul-Rasheed *et al*. (2016) who posited that education is a very important factor in combating cybercrime and that persons need to be educated on how to prevent cybercrime, how cybercrime works and the harmful effects of cybercrime in society. A simple training strategy aimed at improving the ability of consumers, employees, and the public to distinguish a fraudulent email from a real one could reduce a significant proportion of phishing-related cybercrimes. Education can help victims to be aware of cybercrime like phishing.

5. CONCLUSION AND RECOMMENDATIONS

One of the primary ways FTLI improves bank performance is by enhancing cyber security awareness and preparedness. Financial institutions are prime targets for cyber attacks due to the vast amounts of sensitive customer data they handle. FTLI programs provide bank employees with comprehensive training on recognizing and responding to cyber threats, including phishing attempts, malware, and hacking incidents. Similarly, customers who are financially technology-literate are less likely to fall victim to cybercrimes. They are more cautious about sharing personal and financial information online, protecting themselves from identity theft and financial fraud. This reduction in vulnerabilities results in fewer successful cyber attacks on banks. Perhaps one of the most significant impacts of FTLI is its ability to moderate the relationship between cybercrimes and poor bank performance. As employees and customers become more cyber-aware, the success rate of cybercrimes decreases. Even if cybercrimes occur, their severity and financial impact are reduced due to the proactive measures taken by individuals.

Trust is paramount in the banking industry. FTLI demonstrates a bank's commitment to customer security. When customers perceive that their financial institution takes cyber security seriously, they are more likely to trust the bank with their assets and sensitive information. This trust fosters long-term customer relationships and customer loyalty.

The moderating effect of FTLI is crucial in an era where cybercrimes are evolving in sophistication and scale. By reducing vulnerabilities and enhancing incident response, FTLI acts as a shield against the adverse effects of cybercrimes, ultimately safeguarding the financial health of banks. Effective FTLI can result in cost savings for banks. Preventing cybercrimes is often more cost-effective than dealing with the aftermath, which may involve reimbursing customers for losses, legal fees, and reputational damage control. FTLI investments translate into long-term cost savings and business continuity.

Lastly, Banks should develop customer-focused Fin-tech literacy programs to help them recognize and protect themselves from cybercrimes, and, continuously assess the effectiveness of Fin-tech literacy interventions and adapt them to address evolving threats. Banks should leverage Fin-tech collaborations to develop customized cyber security solutions that align with the bank's specific needs and infrastructure.

REFERENCES

- Adams, M., and Benham, J. (2016). Reputation and Identity in the Face of Cybersecurity Lapses: A Financial Institution Perspective. *Journal of Corporate Identity*, 12(4): 78 – 92.

- Adams, M., and Benham, J. (2016). Reputation and Identity in the Face of Cyber security Lapses: A Financial Institution Perspective. *Journal of Corporate Identity*, 12(4): 78 – 92.
- Adeyemi, A. (2022, November 23). Cyber crimes raise concern for N30.2tr monthly e-payments. *The Guardian*.https://guardian.ng/technology/why-cybercrime-menace-may-not-abate-soon
- Aduge-Ani, D. I. (2015). Electronic Banking and Fraud in Nigeria: Challenges of Conformity and Challenges to Conformity. *European Scientific Journal*, 11(17): 142 – 162.
- African Academic Network on Internet Policy. (2020). Data Breaches and Cyber security Incidents in the Financial Sector. *African Journal of Internet Policy and Law*, 4(2): 78 – 94.
- Ahmad, N., and Schreyer, P. (2016). *Measuring GDP in a Digitalized Economy.* OECD Publishing, Paris. doi: doi.org/10.1787/18152031
- Akinbowale, O. E., Klingelhöfer, H. E., and Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: A survey of literature. *Journal of Financial Crime,* 27(3): 945 – 958.
- Akuta, M. C. (2012). *Policing the cyberspace: Challenges and strategies. In The Road to Democracy in* Nigeria (pp. 151-170). Springer.
- Alese, B. K., Thompson, A. F. B., Alowolodu, O. D., & Blessing, E. O. (2018). Multilevel authentication system for stemming crime in online banking. *Interdisciplinary Journal of Information, Knowledge, and Management*, 13: 79 – 94.
- Arachchilage, N. A. G., and Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38: 304 – 312.
- Baker, K. A., and Glasser, B. J. (2005). *Cybercrime: Cyber terrorism and Cyber security*. Pearson Prentice Hall.
- Boer, M., and J. Vasquez. (2017). *Cyber Security and Financial Stability: How Cyber-Attacks Could Materially Impact the Global Financial System*. Institute of International Finance, Washington, DC.
- Boissay, F., Fahri, E., and Veldkamp, L. (2022). The rise of crypto and cyber-attacks. *Journal of Economic Theory*, 107054. https://doi.org/10.1016/j.jet.2022.107054
- Brockett, P., Golden, L., and Wolman, S. (2012). Cyber Risk and Its Impact on Financial Institutions. *Journal of Risk and Insurance*, 79(3): 547 – 563.
- Buckley, R. P., Arner, D. W., Zetzsche, D. A. and Weber, R. H. (2019). Cyber security Risks in the Financial Sector: Challenges and Solutions. *Journal of Banking Regulation*, 20(1): 75 – 92.
- Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers and Security*, 33(8): 719 – 731.
- Creado, A., and Ramteke, R. (2020). Hacking and Its Impact on the Banking Sector: A Case Study Analysis. *Journal of Information Security*, 7(4): 321 – 339.
- Das, S., *et al*. (2012). Investor Response to Public Announcements of Cyber security Breaches. *Journal of Information Security*, 6(2): 105 – 118.
- Drinkwater, A. (2014). Cyber-terrorism: Problems and prospects. *International Journal of Cyber Criminology*, 8(1): 19 – 32.
- Durun, R. E., and Griffin, P. (2019). Smart contracts: will Fin-tech be the catalyst for the next global financial crisis? *Journal of Financial Regulation and Compliance*, 29(1): 104 – 122.
- Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry Zimbabwe. *Risk Governance and Control: Financial Markets & Institutions*, 4(2): 17 – 27.
- Dzomira, S. (2016). Internet Banking and Cyber Fraud in Southern African Banks. *International Journal of Computer Applications*, 135(7): 7 – 12.
- Ehimen, O., and Bola, O. (2009). Cybercrime and the Nigerian society. *Library Philosophy and Practice*, 2009(10): 1 – 7.
- Equinix (2021). Keeping Critical Infrastructure Safe from Cyber Attacks. https://blog.equinix.com/blog/2021/09/07/keeping-critical-infrastructure-safe-from-cyber-attacks/
- Eze, U. (2021). Economic Costs and Implications of Cybercrime: A Case Study of Nigeria. *International Journal of Cyber security and Digital Forensics*, 10(1): 45 – 62.
- Fiebelkorn, N., and Taggart, R. (2014). Internet Banking Fraud Mitigation. *of Information Systems and Technology Management*, 11(3): 507 – 518.
- Fiebelkorn, N., and Taggart, W. (2014). Assessing Cyber security Risk in the Banking Sector. *Journal of Financial Regulation and Compliance*, 22(3): 259 – 269.
- George, T., Owoyemi, G., and Onakala, G. (2012). Corporate Reputation and Identity: Implications for Financial Institutions. *Journal of Reputation Management*, 9(1): 45 – 60.
- Geyres, S., and Orozco, M. (2016). Think banking cyber security is just a technology issue? Think again. accenture strategy. https://www.accenture.com/t20160419t004021__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). Bangladesh Bank official's computer was hacked to carry out $81 million heist: diplomat. https://www.reuters.com/article/us-cyber-heist-philippines-idUSKCN0YA0CH

- Gordon, L. A., and Loeb, M. P. (2003). Cyber security and economic incentives. *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, 9p.
- Gottschalk, P. (2010). *Information Security Governance*. Wiley.
- Gupta, S. (2012). Cybercrimes: A decade of IT and Law enforcement perspectives in India. *Procedia Technology*, 4: 115 – 120. https://doi.org/10.1016/j.protcy.2012.05.022
- Hassan, N. M., Lass, M. M., and Makinde, S. O. (2012). Cybercrime and its impacts on Nigerian society: An empirical study. *Information Management and Business Review*, 4(5): 265 – 272.
- 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
- Henrie, M. (2013). *Cyber security: The Essential Body of Knowledge*. Cengage Learning, Boston, 528p.
- Horne, C. (2014). The Costs and Consequences of Cyber security Breaches in Financial Institutions. *Journal of Financial Risk Management*, 3(4): 67 – 82.
- Hovav, A., and D'Arcy, J. (2014). Cyber security Threats in the Banking Industry: A Social Engineering Perspective. *Journal of Information Privacy and Security*, 10(2): 34 – 52.
- Howarth, J. (2015). The Growing Threat of Cyber Attacks in the Banking Sector. *Journal of Banking and Finance*, 9(1): 34 – 49.
- Ibikunle, F., and Odunayo, O. (2013). Identity Theft in Online Banking: A Comparative Analysis of Nigerian and South African Banking Sectors. *Journal of Financial Risk Management*, 4(2): 101 – 118.
- Internet World Statistics (2018). Re-Hashed: 2018 Cybercrime Statistics: A closer look at the "Web of Profit". https://www.thesslstore.com/blog/2018-cybercrime-statistics/ (Retrieved on February 12, 2023).
- Isa, M. Y. B. M., Ibrahim, W. N. R. W. and Mohamed, Z. (2021). The Relationship Between Financial Literacy and Public Awareness on Combating the Threat of Cybercrime in Malaysia. *The Journal of Industrial Distribution & Business,* 12(12): 1 – 10.
- Juma'h, A. H., and Alnsour, M. (2020). Cyber security Vulnerabilities and Their Effects on Financial Institutions. *Journal of Banking and Finance Security*, 8(2): 87 – 101.
- Kamiya, S., J. Kang, J. K., Andreas, M. and René, M. S. (2021). Risk management, firm reputation, and the impact of successful cyber attacks on target firms. *Journal of Financial Economics,* 139(3): 719 – 749.
- Kaspersky Lab. (2022). APT trends report Q4 2021. https://media.kasperskydaily.com/wp-content/uploads/sites/85/2022/02/17063001/APT-Trends-Report-Q4-2021.pdf
- Kopp, E., Kaffenberger, L. and Wilson, C. (2017). Security System Breakdown and Cyber-Infrastructure Vulnerability in the Financial Industry. *Journal of Cybersecurity*, 12(3): 245 – 261.
- 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
- Langton, R. (2018). Manipulation of Financial Data by Cybercriminals: Implications for Credit Risk in Banks. *Journal of Financial Crime*, 25(4): 100 – 116.
- Leukfeldt, R., Veenstra, S. and Stol, 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): 1 – 7.
- Low, A. (2017). The Limits of Cyber Insurance: Why Cyber security Risk Is Not Insurable. *Journal of Risk and Insurance*, 84(3): 865 – 892.
- Macaulay, J. (2018). The Impact of Cybersecurity Vulnerabilities on Financial Institutions. *International Journal of Information Security*, 21(5): 611 – 626.
- Manzoor, A. (2014). A Look at Efficiency in Public Administration: Past and Future. *SAGE Open*, 4: 1 – 5.
- McConnell, P. J. and Blacker, K. (2013). Systemic Operational Risk: Does it Exist and, If So, How Do We Regulate It? *Journal of Operational Risk*, 8(1): 59 – 99.
- Menon, S., and Guan-Siew, A. (2012). Cybercrime: Impact on Economic Crime. *International Journal of Economics, Commerce, and Management*, 1(10): 61 – 67.
- Nabi, S. A., and Islam, S. (2014). Cyber security and National Security: A Comprehensive Review. *International Journal of Computer Applications*, 97(12): 13 – 17.
- Nwadike, E. (2014). Cyber security Challenges and Responses in Nigerian Banks. *African Journal of Computer Science and Technology*, 8(3): 201 – 215.
- Nwogwugwu, N., and Uzoechina, P. (2015). Cybercrime and Nigeria's economic development. *Journal of Humanities and Social Science*, 20(5): 1 – 10.
- Odeyemi, A. (2013). The Rising Tide of Cybercrime in Nigeria: Implications for Banks. *Journal of Banking and Finance*, 7(2): 123 – 139.
- Okonji, S. M. (2015). *The menance of cyber crime and corruption in Nigeria. In Research on Corruption in Organizations* (Vol. 23, pp. 251-270). Emerald Group Publishing Limited.
- Olayemi, O. A. (2014). Cybercrime in Nigeria: Causes and Consequences. *International Journal of*

Information and Communication Technology Research, 4(5): 481 – 485.

- Paranjape, A. M. (2012). Cybercrime: Types, challenges, and responses. *International Journal of Cyber Criminology*, 6(1): 25 – 37.
- Raghavan, A. and Parthiban, L. (2014). The effect of cybercrime on a Bank's finances. *International Journal of Current Research and Academic Review,* 2(2): 173 – 178.
- Rathore, D. S. H. and Marwaha□, K. (2015). Cyber Crime in Banking Sector. *Law Mantra Think Beyond Others*, 2(7): 1 – 7.
- Rowley, L. (2020). RDPalooza: RDPs in the World of Cybercrime. https://securityboulevard.com/2020/12/rdpalooza-rdps-in-the-world-of-cybercrime/ (Retrieved on 12th February, 2023).
- Schell, B. H., and Martin, C. (2004). *Cybercrime: A Reference Handbook*. ABC-CLIO.
- Sharma, R., and Tandekar, S. (2018). Earnings Uncertainty and Loss of Operational Efficiency Due to Cyber security Risk in Financial Institutions. *International Journal of Financial Management*, 14(3): 45 – 61.
- Tendulkar, R. (2013). Cyber-crime, securities markets and systemic risk. *Chartered Financial Analyst (CFA) Digest*, 43(4): 35 – 43.
- Uddin, M. H., Ali, M H. and Hassan, M. K (2020). Cyber security Hazards and Financial System Vulnerability: A Synthesis of Literature. *Social Science Research Network Electronic Journal*, 22(4): 239 – 309.
- Usman, M. S., and Shah, S. A. (2013). The Role of Cyber security in Electronic Banking: An Integrated Framework. *Journal of Internet Banking and Commerce*, 18(3): 1 – 15.
- Wada, T., and Odulaja, D. (2012). The impact of cyber crime on banking operations in Nigeria. *Journal of Internet Banking and Commerce*, 17(3): 1 – 9.
- Wolf Pack. (2014). Cyber security in the Nigerian banking sector. http://www.wolfpackrisk.com/wp-content/uploads/2014/06/Wolf-Pack-Cyber-Security-White-Paper.pdf

Cite This Article: Martins Myke-okoi Okpa, Emmanuel Jabirwe Gwambeka, Mohammed Waziri, Solomon Mamman (2025). Cybercrimes and Bank Performance: A Study of Financial Technology Literacy Interventions in Cross River State. *East African Scholars J Edu Humanit Lit, 8*(10), 576-591.