Archives of Current Research International

Volume 25, Issue 5, Page 103-123, 2025; Article no.ACRI.134584
ISSN: 2454-7077

A Machine Learning Perspective on the Impact of Cybercrime on Performance in the Nigerian Banking Industry

Chikelue Chiebuka Nwabuike [a*], Vincent. A. Onodugo [b++] and Madu Ikemefuna [c]

[a] Department of Management Sciences, Coal City University, Enugu State, Nigeria.
[b] Department of Management, Faculty of Business Administration, University of Nigeria, Enugu State, Nigeria.
[c] Department of Business Administration, Federal University Gashua, Yobe State, Nigeria.

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: https://doi.org/10.9734/acri/2025/v25i51192

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://pr.sdiarticle5.com/review-history/134584

Original Research Article

Received: 16/02/2025
Accepted: 20/04/2025
Published: 29/04/2025

ABSTRACT

This study strives to establish salient relationship between cyber crime and business performance, the 4th industrial revolution (4IR or Industry 4.0) surely has Artificial intelligence (AI) embedded in it, a key subset of AI that is shaping and will further shape the marketplace is Machine learning (ML). This study has leveraged ML in establishing key performance relations in the Nigerian banking industry amidst growing impedance of cyber crime against the maximization of stakeholders and shareholders returns. By mining data from past data patterns of data gotten from the Nigerian banks annual report from 2013 to 2019 and Nigerian electronic fraud forum (NEFF) and analyzing using

[++] Ph.D. Professor of Management and Dean;
**Corresponding author: Email: chikelue.nwabuike@ccu.edu.ng;*

Cite as: *Nwabuike, Chikelue Chiebuka, Vincent. A. Onodugo, and Madu Ikemefuna. 2025. "A Machine Learning Perspective on the Impact of Cybercrime on Performance in the Nigerian Banking Industry". Archives of Current Research International 25 (5):103-23. https://doi.org/10.9734/acri/2025/v25i51192.*

linear regression algorithm, our study was able to establish relationships between ; ATM card crime/ Profit After Tax (PAT), PoS crime/ Earnings Per Share (EPS), and E-commerce crime/ Profit Before Tax (PBT), providing a correlation fit between these pairs with correlation coefficient values of 0.89, 0.99 and 0.99 respectively implying a very strong positive correlation between the pairs. This study concluded that there is a strong correlation between cyber crime and performance in the Nigeria banking industry, anchoring on fiedler's contingency theory that there is no one best way to manage cyber crime.With innovative recommendations like robust cyber security systems which are new economic knowledge (knowledge-shift), the study predicts a re-shape of growth in the Nation's banking industry while consolidating on technological competitive advantage.

Keywords: Cybercrime; banking industry; business performance; Nigerian banks.

1. INTRODUCTION

"Our world has a wealth of different types of data like internet of things (IoT) data, cyber security data, smart city data, business data, smart phone data, social media data, health data, covid-19 data and more" (Sarker, 2021). "Derived insights from these data could be used in creating diverse intelligent applications in their relevant industries" (Sarker et al., 2020) for example to create a data-driven intelligent and automated cyber security system, relevant cyber security data could be used.

"The idea of computer learning like humans do constantly has been existing since the 1950s when the first neural networks were developed" (Kleene, 1951). "Right before then, other methods such as Bayesian statistics and Markov chains were used with similar purpose. Machine learning (ML) a subset of Artificial intelligence has grown sporadically in recent years through data analysis and computing that allows applications to function intelligently" (Sarker, 2021). "ML provides the ability to learn and improve systems from experience automatically without being programmed, thus ML is referred to as the most famous new technologies in the fourth industrial revolution" (Industry 4.0) (Sarker et al., 2020, Sarker et al., 2020).

"Cybercrime can be defined as criminal activities which computers or computer networks are tools, and targets" (Sumanjit and Nayak, 2013). "Hacking is the originating term of cybercrime, and hacking can be described as the activity of modifying a product or procedure to alter its normal function or to fix a problem" (Florida Tech, 2019). "The term was first used in the 1960s to describe the activities of a certain MIT model train enthusiasts who modified the operation of their model trains. These curious individuals went on to work on early computer systems by learning and changing the computer code that was used in early programs. Some of their hacks became so successful and outlived the original products such as the UNIX operating system developed as a hack by Dennis Ritchie and Keith Thompson of Bell labs" (Nwabuike, C. C. et al., 2020).

"Malicious association with hacking became pronounced in the 1970s" (Florida Tech, 2019) when early telephone systems became a target. Hackers impersonated operators, dug through bell telephone company garbage to find secret information, and performed experiments on telephone hardware in order to exploit the system. In 1986, the systems administrator at the Lawrence Berkeley National Laboratory, Clifford Stoll observed irregularities in accounting data inventing the first digital forensic techniques, he determined that an unauthorized user was hacking into his computer network. The Berkeley lab intrusion was followed by the discovery of the Morris worm virus created by Robert Morris a Cornel University student. This virus damaged more than 6000 computers and resulted in estimated damages of USD 98 million.

"This innovative crime type was a difficult issue for law enforcement, due to lack of legislation to aid criminal prosecution and a shortage of investigators skilled in the technology that was being hacked. United States congress passed its first hacking related legislation; The federal computer fraud and Abuse act in 1986. The act made computer tampering a felony crime punishable by significant jail time and monetary fines. Then in 1990, during a project operation sundevil, FBI agents confiscated 42 computers and over 20,000 floppy disks that were used by criminals for illegal credit card use and telephone services. Some of the major impacts of cyber crime include; socio-political impacts, private and public sector businesses, consumer behaviour impact, emotional impact, lost of sales, cost of security protection and many more" (Nwabuike,

C. C. et al., 2020). Cybercrime has grown more prevalent, and consumer confidence has plummeted.

"Banking can be described as the business activity of accepting and safeguarding money owned by individuals and entities otherwise called depositors, and lending this money out in order to earn profit and create financial multiplication in the economy through multiplier effect" (Oluduro, 2015). "He asserts that banking has come a long way in Nigeria, giving three basic phases of banking historical development/evolution in Nigeria as; The era of free and monoculture banking (1892-1954), the era of classical liberalism (1952-1985), and then 1986 to present as characterised by series of structural adjustment, reforms and consolidations in the banking industry for viability and customers/investors confidence in the system" (Nwabuike, et al., 2020).

2. LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

"The high prevalent internet fraud activities locally known as 'yahoo-yahoo' in Nigeria has continually discouraged online business activities not just in Nigeria but the world in its entirety as concluded" by Olayemi, (2014) in his study; A social technological analysis of cybercrime and cyber security in Nigeria. The basic mode of operation of internet fraudsters is anchored on Lin and Bergmann, (2016) three asset attributes of confidentiality, integrity, and accessibility.

As concluded by Sumanjit and Nayak, (2013), (Okeshola and Adeta, 2013), (Duah and Kwabena, 2015), cybercrime consequently affects profitability adversely while increasing costs through losees and also litigations against banks in the banking industry. Poor consumer confidence which could discourage patronage and thus diminish revenue in banks is another salient consequence of cybercrime.

Previous studies like (Balogun and Obe, 2010), (Arpana and Chauhan, 2012), (Okeshola and Adeta, 2013), (Kyalo and Kanyaru, 2015), examined the consequences, impacts, motives, factors and trends of cybercrime. Currently no known literature has modelled the relationship between cybercrimes and some key performance indicators in the banking industry like total revenue, profit after tax (PAT), earning per share (EPS), and the likes. This calls for detailed investigation with a study like this.

The general objective of this study was to determine the relationship of cybercrime and performance of Nigerian banking Industry. However the specific objectives were to;

i. Determine the degree of relationship between ATM card crimes and profit after tax (PAT) in Nigerian banks.

ii. Investigate the degree of relationship between Point of sales (POS) crime and earnings per share (EPS) in Nigerian banks.

iii. Ascertain the degree of relationship between e-commerce crime and profit before tax (PBT) in Nigerian Banks.

$H_{A1.}$ There is a significant relationship between ATM card crime and profit after tax (PAT) in the banking industry.

$H_{A2.}$ There is a significant relationship between Point of sales (POS) crime and earnings per share (EPS) in the banking industry.

$H_{A3.}$ There is a significant relationship between e-commerce crime and profit before tax (PBT) in the banking industry.

2.1 Machine Learning

Machine learning (ML) a subset of Artificial intelligence has grown sporadically in recent years through data analysis and computing that allows applications to function intelligently (Sarker, 2021). ML provides the ability to learn and improve systems from experience automatically without being programmed, thus ML is referred to as the most famous new technologies in the fourth industrial revolution (Industry 4.0) (Sarker et al., 2020, Sarker et al., 2020). The effectiveness and efficiency of a machine learning model is dependent on the nature and characteristics of data used and the performance of the learning algorithm (Sarker, 2021). Data can be of various forms like structured, semi-structured or unstructured also metadata (Mecallum, 2005).

2.2 Types of Real World Data

Structured: Structured data are organized and follow a standard order that makes them easily accessible and used by an entity or computer program. In relational databases, structured data are stored in tables for example; names, dates,

addresses, credit card numbers, stock information, geolocation, financial income, financial expenditures etc are all forms of structured data.

Unstructured: Unstructured data have no pre-defined format, unorganized and thus difficult to be captured, processed and analyzed. Unstructured data mostly contain text and multimedia materials like sensor data, e-mails, wikis, pdf files, blog entries, videos, images, audio files, web pages and many more.

Semi-Structured: Semi-structured data unlike structured data are not stored in a relational database but have some organizational properties that make it easy to analyze. Some good examples of semi-structured data are; HTML, XML, JSON documents, NOSQL databases e.t.c.

Metadata: Metadata are data of data. They give insight about data. The major difference between "metadata" and "data" is that while data are the material that can classify, measure or document relations to an organization's data properties, metadata describes relevant data information giving more insight for data users. Some examples of metadata are; author, file size,data generated by the document, keywords e.t.c. (Sarker, 2021) further recorded four machine learning techniques namely; Supervised learning, Unsupervised learning, Semi-supervised learning and Reinforcement learning.

2.3 Supervised Learning

Badillo et al., (2020) computers are fed training data with observations and corresponding known output values. (Han et al., 2011) Supervised learning is the activity of machine learning to learn functions that map inputs to outputs according to sample input-output pairs. The two most basic supervised learning tasks are classification and regression.

Classification: This is a supervised learning technique in machine learning also known as predictive modelling where class labels are predicted for some given samples (Han et al., 2011). mathematically, classification maps a function (f) from input variables (x) to output variables (y) as label, target or categories. Classification can be carried out on structured or unstructured data sets like spam detection "spam" and "non spam" in e-mail services.

Classification can be binary classed (two classes) true or false, and multiclassed (having more than two class labels). Some classification algorithms proposed in the machine learning and data science literature (Witten and Frank, 2005) are:

- Naive Bayes (NB)
- Linear Discriminant Analysis (LDA)
- Logistic Regression (LR)
- K-Nearest Neigbors (KNN)
- Support Vector Machine (SVM)
- Decision Tree (DT)
- Random Forest (RF)
- Adaptive Boosting (Ada Boost)
- Extreme gradient boosting (XG Boost)
- Stochastic Gradient Descent (SGD)
- Rule-based Classification

Regression Analysis: This involves several methods of machine learning that allow the prediction of continuous (y) result variable based on the value of one or more (x) predictor variables. (Han et al., 2011). The salient difference between regression and classification is that while the latter predicts distinct class labels, the former facilitates the prediction of continuous quantities. Regression models are used largely in various fields like financial forecasting, financial prediction, cost estimation, performance forecasting and prediction, trend analysis, time series estimation, marketing and more. The famous types of regression are linear, polynomial, lasso and ridge regression. The most popular being simple and multiple linear regression in machine learning. This technique has a continuous dependent variable, a discrete or continuous independent variable(s). linear regression creates a relationship between the dependent variable (y) and one or more independent variable (x) using the best fit straight line (Han et al., 2011) as indicated in equations 1a and 1b below;

$$Y = a + bx + c \quad \text{equ (1a)}$$

$$Y = a + b_1x_1 + b_2x_2 + \ldots\ldots b_nx_n + c \quad \text{equ (1b)}$$

while for polynomial regression, the relationship between the independent variable (x) and the dependent variable (y) is not linear but with the polynomial degree of nth in x (Pedreosa et al., 2011). The polynomial regression equation is derived from the linear regression equation (1) to get equation (2) below;

$$Y = b_0 + b_1x + b_2x^2 + b_3x^3 + \ldots.b_nx^n + c \quad \text{equ (2)}$$

2.4 Unsupervised Learning

Badillo et al., (2020) Exploratory data analysis often do not give true data labels or when we have need to examine the natural emergence of patterns in data we use unsupervised learning. Unsupervised learning analyzes unlabeled data sets with or without need for human interference (data driven process) (Han et al., 2011). Unsupervised learning is typically applied in identifying meaningful trends, patterns and structures, extracting generative features, exploratory purposes and grouping in results.

Most common modelling techniques for unsupervised learning are;

- Clustering
- Density estimation
- Feature learning
- Dimensionality reduction
- Anomaly detection

2.5 Semi-Supervised Learning

“This can be considered as a hybrid of supervised and unsupervised learning mainly because it operates on both labeled and unlabeled data” (Han et al., 2011, Sarker et al., 2020) therefore “it is in between learning without supervision and learning with supervision. Semi-supervised learning is useful in the real world applications where we have numerous unlabeled data and limited labeled data” (Mohammed et al., 2016). Semi-supervised learning is used in fraud detection, data labeling, text classification e.t.c.

2.6 Reinforcement Learning

“Reinforcement learning is a machine learning algorithm that enables softwares or machines with the automatic evaluation of the optimal behavior in a particular context or environment in order to enhance its efficiency. Reinforcement learning is environment – driven” (Kaelbling et al., 1996). “This type of learning uses a reward and penalty approach with ultimate goal of using insights obtained from environmental impulses to take action by increasing rewards or minimizing risks” (Mohammed et al., 2016). This is a powerful Artificial intelligence training tool for models that can help increase automation or optimize operational efficiency of complex systems like robots, autonomous driving tasks, manufacturing and supply chain logistics e.t.c.

2.7 Neural Networks

Badillo et al., (2020) “Neural Networks constitute a collection of neurons and edges with its origin from circuit analysis. Weight of different magnitude can be applied to each edge connecting the neurons, there is an activation function applied to weighed input signals at each neuron to generate an output signal. A sigmoidal function is often used which consists of a first order low pass filter of a unit step function. The neurons are further divided into an input layer, hidden layer(s) and the output layer. The hidden layers perform the layer of abstraction needed to go from the input layer to the output layer. The number of hidden layers define whether the system is a shallow learning system (one or few hidden layers) or deep learning (many hidden layers). The most basic type of neural networks is the feed forward neural network, however there is Recurrent neural networks (RNN), Convolutional neural networks (CNN), Long short-term memory networks (LSMT), Encoder-Decoder networks and more”.

2.8 Cyber Crime

Olusola et al., (2013) asserted that “cyber crime is any illegal behaviour committed by means of or in relation to a computer system or network, which includes illegal possession and offering or distributing information by means of a computer system or network”. (Olusola et al., 2013) “went further to list three major categories of cyber crime, which are all activities done with criminal intent in cyber space as; Crimes against persons, Crimes against business and non-business organizations then Crimes against the government”.

They also outlined some examples of cyber crimes to include spamming, identify theft, hacking, phishing, denial of service, advanced fee fraud 419 (aka yahoo-yahoo), credit card fraud, soft ware piracy, plagiarism, pornography etc.

Steve, (2002) opined that “cyber crime is used to broadly describe criminal activities in which computers or computer networks are tools, targets or a place of criminal activity and include everything from electronic cracking to denial of service attacks. They further categorized cyber crime as: Data crime (that is data interception, data modification and Data theft), Network crime (network interferences and Network sabotage), access crime (unauthorized access and virus

dissemination) and related crimes (computer related forgery and content related crime)". (Steve, 2002) "gave the following types of cyber crime:- Theft of telecommunications services, dissemination of offensive materials electronic money laundering and tax evasion, electronic vandalism, terrorism and extortion, sales and investment fraud, illegal interception of telecommunications, electronic funds transfer fraud".

They further enumerated some impacts of cyber crime to include; cyber crime as an evil factor of society, impact of cyber crime over socio- eco-political riders, impact of cyber crime over teenager, impact of cyber crime over private industry, impact of cyber crime over consumer behaviour, emotional impact of cyber crime, impact of cyber crime over business, cost of security or protection, lost sales, impact of cyber crime over youth, cyber bullying and sexual solicitation.

2.9 Automated Teller Machine (ATM)

"Automate Teller Machine (ATM) is a computerized telecommunications device which provides access to financial transactions in public places without the need for a human clerk or bank teller" (Adelowo and Mohammed, 2010). Bank customers are identified by insertion of a plastic ATM card with embedded microchip that contains a unique card number and some security codes. ATM stations can be located at shopping malls, airports, grocery stores, petrol/gas stations, restaurants, or any other public place that requires financial transactions (Steve, 2002). ATMs have also evolved to include other banking functions other than cash dispensing like paying of bills (example: Utility, fees), printing of bank statements, purchasing, cash deposits and more. Brain, (2000) itemized the following benefits of ATM; flexible account access allows clients to access their accounts at their convenience, bank personnel are not required to be present for transactions and have more time to serve clients, increased hours of operation fit client schedules, more clients can be reached beyond the branch network, more low-cost funds are available at ATMs make it easier for clients to deposit savings. Diebold, (2002) identified the following ATM frauds or crimes:

Card theft: This is the use of card trapping devices by cyber criminals to trap victim's cards in ATMs and then captures information illegitimately from the victim's trapped card to be used for criminal activities could also be termed skimming.

Shoulder surfing: This is the act of direct observation, watching what code the victim taps onto the keyboard. Criminals usually position themselves close to watch as the ATM user enters his/her pin. Sometimes miniature cameras are installed on the fascia or close to the pin pad to record the pin entry by the user.

Fake pin pad: This is when a fake pin pad is placed over the original keypad. This fake pad captures the pin data and stores in its memory. The criminal will retrieve the information from the fake pad memory and uses it to access victim's account.

Pin Interception: This is the act of cyber criminals intercepting communication handshake between the ATM data record and the host computer that validates user information, and uses the information for criminal acts.

2.10 Point of Sales (PoS)

Point of sales (PoS) is a system with combination of hardware and software used primarily by businesses to process customer purchases (Midhun et al., 2017). They further indicated that this combination can be as small as a smart phone with a credit card reader attached to an earphone jack of a large retail store with several checkout lines and back office filled with computer and network equipments.

Midhun et al., (2017) narrowed the definition of Mobile point of sales (MPOS) to be devices like tablets and other portable devices used to complete transactions. Sales associates can use (MPOS) to answer questions, provide information, and checkout customers anywhere. Mobile and stationary POS systems support flexible retail environments, enabling businesses to adapt easily to customer's needs and thus being competitive with online retailers.

Typical point of sales system has a computer, monitor, cash drawer, customer display, barcode scanner, debit and credit card reader, and receipt printer (Midhun et al., 2017). Modern PoS systems have touch-screen technology and configured to handle transactions like; Sales, returns, exchanges, gift cards, loyalty programs and gift registries. PayPal, (2013) opines that POS evolution will fundamentally disrupt the

nature of merchant-consumer interaction, stating that the combination of mobile devices, proliferation sensors, integration of different data and deep creativity will greatly impact consumer experience in the following ways; Interacting with consumers throughout a store floor, understanding how consumers engage with in-store products, empowering sales associates with individual customer profile data, providing context-aware customer interactions, engaging with customers throughout the shopping process, enhancing product discovery and research both in-store and offline, gratifying consumers with creative loyalty reward programs, encouraging more customer store visits, offering self-checkout and payments at locations other than fixed registers to speed up shopping process, and enabling new authentication mechanisms such as visual identification of the customer, voice recognition and biometrics.

2.11 Electronic Commerce (e-commerce)

Electronic commerce includes any form of economic activity conducted via electronic connections (Wigand, 1997), stating that electronic commerce (E-commerce) spans from electronic markets to electronic hierarchies and also incorporates electronically supported entrepreneurial networks and cooperative arrangements. Wigand, (1997) itemized the following effects of information technology on electronic commerce. The communication effect: Advances in information technology allow for more information to be communicated in the same unit of time, thus reducing transaction costs. The electronic integration effect: A tighter electronic linkage between buyer and seller is enabled. The electronic brokerage effect: An electronic marketplace where buyers and sellers come together to compare offerings. And the electronic strategic networking effect: Information technology enables the design and deliberate strategic deployment of linkages and networks among cooperating firms intended to achieve joint strategic goals to gain competitive advantage.

2.12 Performance

Hansen and Wernefelt, (2007) identified two models of firm's performance as Economic model and organizational model. The Economic model emphasizes on the importance of external market factors in determining firm success. Whereas the organizational model builds on the behavioural and sociological paradigm, and sees organizational factors and there fit with the environment as the major determinants of success.

They further decomposed the Economic model to include:

- Industry variables (characteristic of the industry in which the firm competes)
- Variable relating the firm to its competitors
- Firm variables (the quality and quantity of the firm's resources)

The organizational model in broad term suggests that managers can influence the behavior of their employees (and thus the performance of the organization) by taking into account factors such as the formal and informal structure, the planning, reward, control and information systems, their skills and personalities, and the relation of these to the environment. That is, managers influence organizational outcomes by establishing context, and the context is the result of a complex set of psychological, sociological and physical interaction.

Hansen and Wernefelt, (2007) later integrated the two models of firm performance and their result confirmed the importance and independence of both sets of factors in explaining performances.

2.13 The Nigerian Banking Industry

"The free and monoculture banking era between (1892-1954) was the origin of banking in Nigeria. It dates back to 1892 when the African Banking Corporation (ABC) commenced the activities of banking in Lagos" (Oluduro, 2015). Also, "the British Bank of West Africa (BBWA) by Sir Alfred Jones started operating in Nigeria as a trust fund in 1893. The BBWA absorbed ABC operations in 1894 and in 1957, BBWA was changed to the Bank of West Africa and then to the Standard Bank of Nigeria in 1965, before finally becoming the renowned First Bank of Nigeria (FBN) in 1979. The Post Office Savings Bank was established under the savings bank ordinance in 1936, and between 1949 and 1952 over ten banks sprang up but did not survive for long with reasons like; inadequate capital base, lack of banking regulation and acceptable prudential guidelines, unskilled or poor management, illiquidity, inexperienced staffing, fraudulent operators, reckless and rapid expansion of branches, and inability to meet the demands of new government regulations" (Nwabuike, et al., 2020).

"The era of classical liberalism (1952-19d85) saw the establishment of many banks with laid down regulations like the 1952 Banking ordinance, and the banking Amendment Act. It marked the beginning of banking regulation in Nigeria. Specialised banks like; Development banks and Merchant banks which include the Nigerian Industrial Development Bank (NIDB), the Nigerian Bank of Commerce and Industry (NBCI), and the Nigerian Agricultural and Credit Bank (NACB) were established. In 1970, there were a total of 14 commercial banks in Nigeria which increased to 29 in 1980. Then the period of (1986 to date), there has been massive expansion and structural changes in the banking sector. By 1991, there were over 120 commercial banks and merchant banks in Nigeria, arising from the deregulation of the economy by the federal government which brought enhanced free-market enterprise and the liberalisation of the banking licensing scheme. The deregulation and proliferation of banks since 1986 also came with consequences among which are distresses in the sector owing to mismanagement in the form of grants, bad loans and advances, and then ownership structure. Also, inappropriate corporate governance, inadequate regulatory and supervisory capacity and more played a role in distressing the banks. Between 1994 and 2003, twenty seven banks were extinct because of distress. From 2004 to present, there have been mixed feelings in the sector in line with CBN's directive of twenty five billion naira capital base (paid-up) for commercial banks. The result is that by 2006, only 25 banks remained in existence resulting from reorganisations, mergers, and acquisitions. Banks in Nigeria have tried to improve their capital base, profitability and reach through expanding to various regions in the country. Some of them have also moved internationally, thereby bring the concept of internalization of banks in Nigeria to the fore. Nigerian banks expanded into other African countries following the 2004 consolidation that increased minimum capital requirements more than tenfold. Most banks expanded their operations domestically and internationally by increasing branch networks in the domestic market and opening subsidiaries abroad" (Alade, 2016).

2.14 Theoretical Framework

A Machine learning percpective of cybercrime and performance of Nigerian banks will be anchored on two theories; The New growth theory and Contingency Theory.

2.14.1 New growth theory

(Endogenous growth theory). Romer is credited with stimulating new growth theory. The theory states that Economic growth results from the increasing returns associated with new knowledge or technology (Romer, 1994). New growth theory makes shift from resources-based to a knowledge-based economy. It underscores the point that economic processes which create and diffuse new knowledge are critical to shaping the growth of business firms. The essential point of new growth theory is that knowledge drives growth. The major assumptions of new growth theory are:-

a. It views technological progress as a product of economic activity whereas previous theories treated technology as a product of non-market forces.

b. It holds that unlike physical objects, knowledge and technology are characterized by increasing returns, and these increasing returns drive the process of growth.

Based on New growth theory, technological advancements like machine learning, cybersecured systems will definitely boost performance of business firms.

2.14.2 The contingency theory

Fred Edward Fiedler in his article 'A contingency model of leadership effectiveness' states that there is no one best way of organizing/leading, that an organizing style effective in some situations may not be successful in others (Fiedler, 1964). Optimal organization style is contingent upon various internal and external constraints. These constraints may include size of organization, how organization adapts to its environment, strategies, technologies used, differences among resources and operations activities, managerial assumptions and more.

Four basic assumptions of the contingency theory are;

There is no universal or one best way to manage. The design of an organization and its subsystems must fit with the environment.

Effective organizations do not only have a proper fit with the environment but also between its subsystems.

The needs of an organization are better satisfied when it is properly designed and the management style is appropriate both to the tasks undertaken and the nature of the work group.

Based on contingency theory, external environmental constraints like cybercrime must be contingently managed for optimal performance.

2.15 Emprical Review

A research on the Nature, causes and consequences of cyber crime in tertiary institutions in Zaria Kaduna State, Nigeria (Okeshola and Adeta, 2013). The key objectives of the study were (a) to determine the socio-economic attributes of those involved in cyber crime, (b) to determine the various cyber techniques used by cyber criminals to perpetrate the act and to determine the negative impacts the menace poses. They used questionnaires distributed to three institutions in Zaria Kaduna State Nigeria and operators of cyber cafe within Zaria. They used both probability and non-probability sampling techniques to select the respondents. Namely simple random sampling and purposive/snow ball sampling respectively. They equally interviewed a cyber criminal that participated in the research through the assistance of a cyber cafe operator. The study adopted the use of triangulation method in the analysis and interpretation of data (that is the combination of both quantitative and qualitative method in findings interpretation). In all a total of 400 questionnaires were administered and 12 key informants were interviewed. The study analysed the primary data collected using statistical frequency and mean and concluded that cyber criminals have a flamboyant life style, that unemployment is a caused factor of cyber crime and importantly that cyber crime hinders profitable transactions (Okeshola and Adeta, 2013).

“A study on the impact of cyber crime: issues and challenges” (NEFF, 2014). “The study was carried out in India, some of the specific objectives of the study were to determine the impact of cyber crime over socio-eco-political riders, to ascertain the impact of cyber crime over private industry and the impact of cyber crime over business. The study used secondary data sourced from various industry sectors published by Ponemon Institute, and analysed the data obtained with multiple bar charts for the industries, Benchmark study of US companies based on the representative sample of 50 larger-sized organizations in various industry sectors. The report shows that the median annualized lost of cyber crime for 50 organizations is USD 5.9 million per year. The key findings of this study are: A positive correlation between the growth in incidences of crime and the population of a country and a correlation of crime with the socio-economical and political factors, that industries fall victim to cyber crime, but to different degrees and with different economic impact and that cyber crime can result to less revenue in the long-term if customers decide not to do business with a company vulnerable to attack” (NEFF, 2014).

3. METHODOLOGY

This study a machine learning percpective of cyber crime and performance of the Nigerian Banking Industry is basically interested in finding out the relationship between cyber crime and business performance. The study took an ex-post facto experimental design approach. Ex- post facto design was used because of the time serial nature of the research. This study seeks new insights into the relationship of cyber crime and business performance. (Creswell & Plano, 2011)

The data for this study are mainly secondary data obtained from the Nigerian commercial banks annual report and The Nigeria Electronic Fraud Forum (NEFF) annual report (Nigeria Electronic Fraud Forum, 2014, Nigeria Electronic Fraud Forum, 2016).

3.1 Model Specifications

The dependent variables that made up performance in the banking industry namely; PAT, EPS and PBT were mapped and learnt using machine learning algorithm (Artificial intelligence) to fit a linear regression model with the independent variable of cybercrime which are; ATM card crime, POS crime and e-commerce crime. A simple linear regression model equation is given as;

$$Y = a + bX \qquad \text{equ. 3}$$

Y = dependent variables in this case refers to performance

X = independent variables in this case refers to cybercrime

a =constant also known as parameter theta degree zero

b = constant also known as parameter theta degree one

equation 3 above can also be written as; $Y = \theta_0 + \theta_1 X$ equ 4

$\theta_0 = a$
$\theta_1 = b$

Important note should be taken that these parameters were learnt by machine learning algorithm (Pandas with Python programming language) thus enabling a near perfect linear regression model most befitting to the variables.

4. RESULTS AND DISCUSSION

Table 1. shows commercial banks performance report for 2013, with total PAT of 421,963,744 Naira, total EPS of 1703.39 naira and total PBT of 513,682,120 naira (Zenith Bank PLC, 2013–2020, WEMA Bank PLC, 2013–2020, United Bank of Africa (UBA), 2013–2020, Union Bank PLC, 2013–2020, Stanbic IBTC, 2013–2020, Sterling Bank PLC, 2013–2020, First Bank PLC, 2013–2020, Ecobank Transnational Incorporated. 2013–2020, Fidelity Bank PLC, 2013–2020, Guaranty Trust Holding Company, 2013–2020, Access bank PLC, 2013 to 2020.

Table 2. shows commercial banks performance report for 2014, with total PAT of 544,208,047 Naira, total EPS of 2272.47 naira and total PBT of 647,807,260 naira.

Table 3. shows commercial banks performance report for 2015, with total PAT of 424,241,868 naira, total EPS of 1616 naira and total PBT of 516,142,497 naira.

Table 4. shows commercial banks performance report for 2016, with total PAT of 589,011,290naira, total EPS of 2323.75 naira and total PBT of 692,572,006 naira.

Table 1. Banks performance report 2013

Bank	PAT (000)	EPS (Kobo)	PBT (000)
WEMA	1,596,531	80	1,947,308
Access	36,298,000	159	44,996,000
ETI	24,890,938	95.39	35,374,959
FBN	70,631,000	216	91,337,000
FCMB	16,000,155	81	18,184,399
Fidelity	7,721,000	27	9,028,000
GTB	90,023,256	317	107,091,256
Stanbic IBTC	20,773,000	186	24,617,000
Sterling	8,274,864	52	9,310,198
Union	3,836,000	37	5,141,000
UBA	46,601,000	152	56,058,000
Zenith	95,318,000	301	110,597,000
Mean	35,163,645	141.9492	42,806,843
Total	421,963,744	1703.39	513,682,120

Source: Banks annual report 2013

Table 2. Banks performance report 2014

Bank	PAT (000)	EPS (Kobo)	PBT (000)
WEMA	2,372,445	60	3,093,940
Access	42,976,000	188	55,022,000
ETI	66,139,453	304.47	86,441,599
FBN	82,839,000	255	92,884,000
FCMB	22,133,257	112	23,942,893
Fidelity	13, 796,000	48	15,515,000
GTB	98,694,919	347	116,385,843
Stanbic IBTC	32,065,000	293	40,070,000
Sterling	9,004,973	42	10,747,985
Union	26,825,000	151	27,708,000
UBA	47,907,000	156	56,200,000
Zenith	99,455,000	316	119,796,000
Mean	45,350,671	189.3725	53,983,938
Total	544,208,047	2272.47	647,807,260

Source: Banks annual report 2014

Table 3. Banks performance report 2015

Bank	PAT (000)	EPS (Kobo)	PBT (000)
WEMA	2,327,275	67	3,045,528
Access	58,924,744	237	65,177,913
ETI	21,252,606	56	40,589,019
FBN	15,148,000	44	21,512,000
FCMB	4,760,666	24	7,768,664
Fidelity	13,904,000	48	14,024,000
GTB	99,437,000	351	120,695,000
Stanbic IBTC	18,891,000	155	23,651,000
Sterling	10,292,577	36	11,061,301
Union	13,987,000	83	14,548,000
UBA	59,654,000	179	68,454,000
Zenith	105,663,000	336	125,616,000
Mean	35,353,489	134.6667	43,011,875
Total	424,241,868	1616	516,142,497

Source: Banks annual report 2015

Table 4. Banks performance report 2016

Bank	PAT (000)	EPS (Kobo)	PBT (000)
WEMA	2,591,799	67	3,276,364
Access	64,026,135	221	80,579, 576
ETI	52,600,893	259	33,707,558
FBN	17,141,000	53	22,948,000
FCMB	14,338,882	72	16,251,397
Fidelity	9,734,000	34	11,061,000
GTB	132,280,655	467	165,136,461
Stanbic IBTC	28,520,000	246	37,209,000
Sterling	5,162,365	18	5,999,880
Union	15,391,000	92	15,738,000
UBA	72,264,000	204	90,642,000
Zenith	129,652,000	412	156,748,000
Mean	45,308,561	178.75	53,274,770
Total	589,011,290	2323.75	692,572,006

Source: Banks annual report 2016

Table 5. Cyber Crime types and loss values in naira for 2014

Crime Type	Loss Value(Naira)
ATM card crime	2,688,669,292
Internet banking crime	2,120,881,512
Mobile banking crime	13,328,957
POS crime	157,610,831
E-commerce crime	58,994,920

Source: NEFF cyber crime report 2014

Table 6. Cyber crime types and loss values in naira for 2013

Crime Type	Loss Value
ATM card crime	54,999,829
Internet banking crime	271,762,696
Mobile banking crime	6,787,544
POS crime	5,851,443
E-commerce crime	13,948,390

Source: NEFF cyber crime report 2013

Table 5. above shows different cyber crime types and loss values in naira for 2014, ATM crime has a total loss value of 2,688,669,292 naira, Internet banking crime has 2,120,881,512 naira, Mobile banking crime has 13,328,957 naira, POS crime has 157,610,831 naira and E-commerce crime has 58,994,920 naira.

Table 6. above shows different cyber crime types and loss values in naira for 2013, ATM crime has a total loss value of 54,999,829 naira, Internet banking crime has 271,762,696 naira, Mobile banking crime has 6,787,544 naira, POS crime has 5,851,443 naira and E-commerce crime has 13,948,390naira.

4.1 Data Mining

Owing to the limited data availability from NEFF, where cyber crime loses were only captured for 2013, 2014, 2015 and 2016. data was mined from these past data available by fitting a regression model between cyber crime and E-business performance. (Amsreas & Huido, 2016) A classifier will be learnt by the machine using supervised learning (linear regression). (Andrew, 2008)

The code used for learning is giving below;

On a Jupyter notebook

```
import numpy as np # linear algebra
import pandas as pd # data processing csv file I/O
import os

for dirname, -, filenames in os.walk ('/kaggle/input'):
                    for name in filenames:
                    print (os.path.join (dirname, filename))

import matplotlib.pyplot as plt
import seaborn as sns
from sklearn.pipeline import pipeline
from sklearn.preprocessing import standardscaler, polynomial features
from sklearn.linear_model import LinearRegression
% matplotlib inline

df = pd.read_csv('../input/foldername.csv')
# note that foldername is relative to data

df.head ()

X = df [['X_ axis']] # X axis is colum header of cybercrime
Y = df  [['Y_ axis']] # Y axis is colum header of performance
lm = LinearRegression ()

lm.fit (X,Y)
lm.score (X, Y)
Y = [[Y]] # Y is value of performance to be used for prediction
x_hat = ln.predict (Y) # x_hat is predicted cyberrime value
print (x_hat)
```

Table 7. ATM crime losses and PAT values in naira from 2013 to 2019

ATM Crime (Naira)	PAT(Naira)
54999829	421963744000
2688669292	544208047000
355892200	424241868000
466514680	589011290000
2676, 954, 720	756366375000
3214777910	835140545000
4122320670	968066995000

Source: researcher 2024

Table 8. POS crime losses and EPS values in naira from 2013 to 2019

POS Crime (Naira)	EPS (Naira)
5851443	1703.39
157610831	2272.47
63533467	1616
243321810	2323.75
353081820	2900.083
448930425	3275
564004380	3725.118

Source: researcher 2024

Table 7, above shows ATM crime losses against banks PAT from year 2013 to 2019.

Table 8 above shows POS crime losses against banks EPS from year 2013 to 2019.

Table 9 shows E-commerce crime losses against banks PBT from year 2013 to 2019.

Table 9. E-commerce crime losses and PBT values in naira from 2013 to 2019

E-Commerce (Naira)	PBT (Naira)
13948390	513682120000
58994920	647807260000
52161394	516142497000
132252110	692572006000
207924542	908832208000
246813396	994494260000
327861587	1173022391000

Source: researcher 2024

The following Algorithm was used to correlate the dependent and independent variables:

```
import pandas as pd
import matplotlib. pyplot as plt
import numpy as np
import seaborn as sns
From sklearn.p.pipeline import Pipeline
From sklearn.preprocessing import Standardscaler, Polynomialfeatures.
From sklearn.linear_model import LinearRegression
From scipy import stats
% matplotlib inline

df= pd. read_csv ('file path') # file path- data address
df.head ()
df. Corr ()
sns.regplot(x ="X", y ="Y", data = df) # X is independent variable, Y is dependent variable.
```

4.2 Hypotheses Testing

The hypotheses were tested in the following steps;

Step 1 = Statement of the Hypothesis.
Step 2 = Analysis of the data using pearson product moment correlation coefficient method on pandas df. [corr] and the P-value with sm.OLS.

Step 3 = Decision rule: If pearson product moment correlation co-efficient r is not zero ($-1 \leq r \leq 1$) and at 0.05 level of significance reject H_0 and Accept H_A if the P-value is less than or equal to significance level $\alpha = 0.05$. But if $r = 0$ and at 0.05 significance level α , do not reject H_0 and reject H_A.

Reject H_0 if P ≤ 0.05.

Do not reject H_0 if P > 0.05

Step 4 = Decision.
Step 5 = Interpretation.

4.2.1 Test of hypothesis 1

Step 1 = H_{A1}, There is a significant relationship between ATM card crime and PAT in the banking industry.

H_{01} There is no significant relationship between ATM card crime and PAT in the banking industry.

```
Step 2 = import pandas as pd
         import matplotlib. pyplot as plt
         import numpy as np
         Import seaborn as sns
         From sklearn.pipeline import Pipeline
         From sklearn.preprocessing import Standardscaler, Polynomial

Features

From sklearn.linear_model import LinearRegression
From Scipy import stats

import statsmodels.api as sm

% matplotlib inline

df = pd.read_csv ('file path') # file path = data address
df. head ()
df. corr ()

sns.regplot(x ="X", y ="Y", data = df) # X is independent variable, Y is dependent variable.

         ATM CRIME = df [['ATM CRIME']]
         PAT = df [['PAT']]
         lm1 = sm.OLS.from_formula("PAT ~ ATMCRIME",data= df)
         result = lm1.fit()
         result. summary
```

Table 10. Correlation test result for atm crime and PAT

	ATMCRIME	PAT
ATMCRIME	1.0	0.885669
PAT	0.885669	1.0

Source: Kaggle notebook 2024

Table 11. P-value test result for atm crime and PAT

	Coef	Std err.	T	p> t
Intercept	$4.525e^{+11}$	$6.6e^{+10}$	6.444	0.001
ATMCRIME	114.8912	26.937	4.265	0.008

Source: Kaggle Notebook 2024

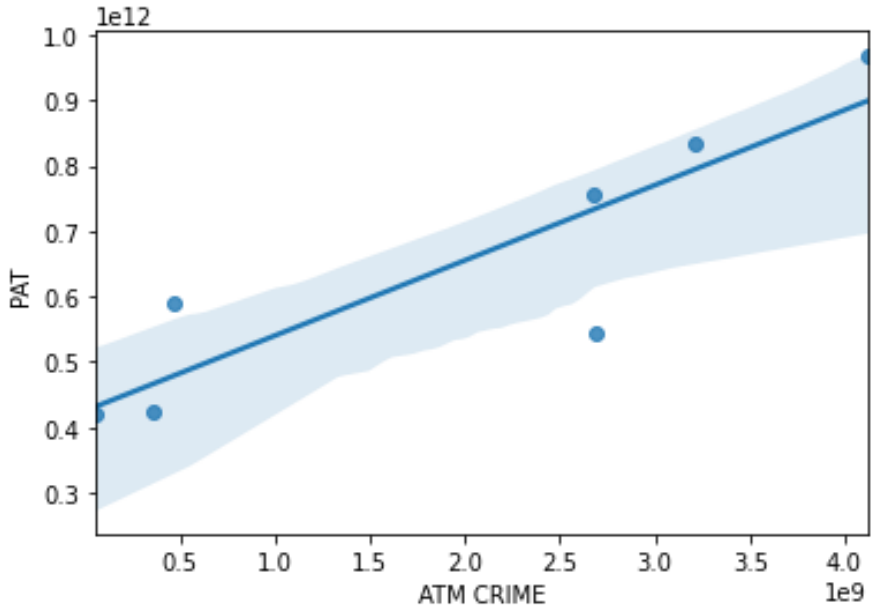

Fig. 1. Regplot of ATM Crime and PAT
Source: Kaggle notebook 2021

From the test results, r = 0.885669, P = 0.008

Step 3 = H_0 is rejected since (- 1 ≤ r ≤ 1) r= 0.885669 and at 0.05 level of significance α, P –value = 0.008. H_{A1} is accepted

Step 4 = There is a significant relationship between ATM card crime and PAT of the banking industry.

Step 5 = ATM card crime loses increases with increasing PAT of in the banking industry.

This finding confirms a relationship between ATM card crime loses and PAT, implying that ATM card crime loses increases with increasing PAT and thus likely to erode resources that could have been accounted as PAT.

4.2.2 Test of hypothesis 2

Step 1 = H_{A2} There is a significant relationship between POS crime and EPS in the banking industry.
H_{02} There is no significant relationship between POS crime and

EPS in the banking industry.

step 2 = import pandas as pd
import matplotlib. pyplot as plt
import numpy as np
Import seaborn as sns
From sklearn.pipeline import Pipeline
From sklearn.preprocessing import Standardscaler, Polynomial

Features

From sklearn.linear_model import LinearRegression

```
From Scipy import stats
import statsmodels.api as sm
% matplotlib inline

df = pd.read_csv ('file path') # file path = data address
df. head ()
df. corr ()
sns.regplot(x ="X", y ="Y", data = df) # X is independent variable, Y is dependent variable.
POSCRIME = df [['POS CRIME']]
EPS = df [['EPS']]
lm1 = sm.OLS.from_formula ("EPS ~ POSCRIME", data = df)
result = lm1.fit ()
result. Summary
```

Table 12. Correlation test result for POS crime and Eps

	POS CRIME	EPS
POS CRIME	1.0	0.988276
EPS	0.988276	1.0

Source: Kaggle Notebook 2024

Table 13. P-value test result for POS crime and Eps

	Coef	Std err.	T	p> t
Intercept	1542.9046	85.380	18.071	0.000
POSCRIME	$3.82e^{-06}$	$2.64e^{-07}$	14.474	0.000

Source: Kaggle Notebook 2024

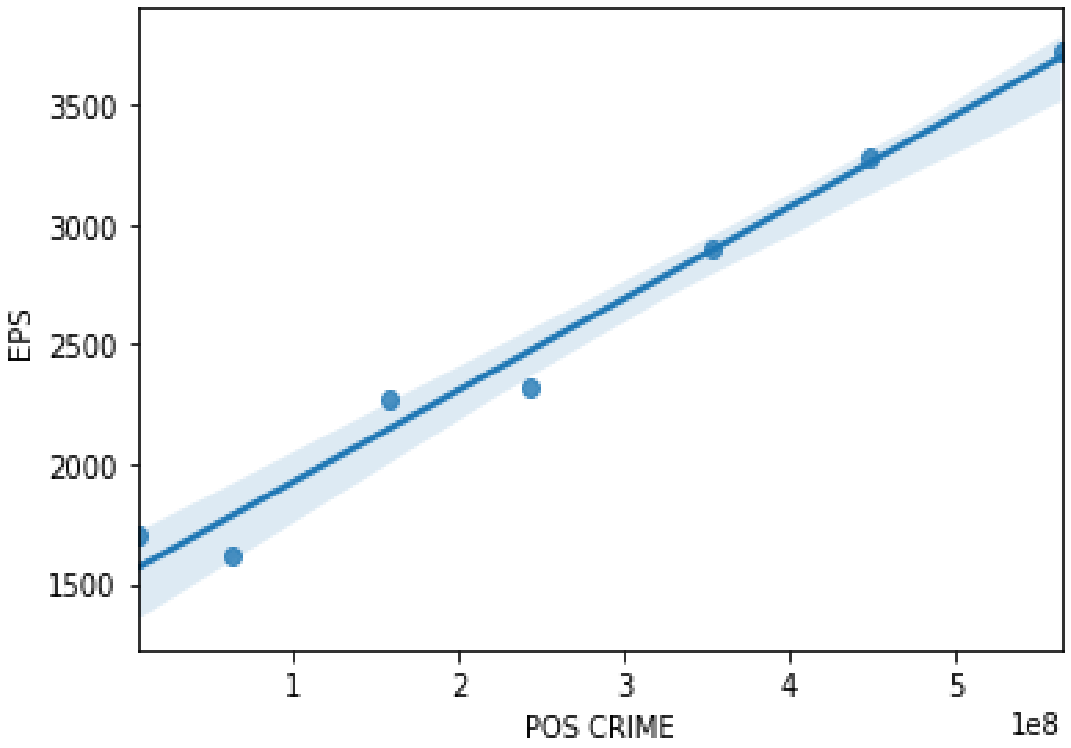

Fig. 2. Regplot Of POS crime AND EPS

Source: Kaggle Notebook 2024

From the results r = 0.988276, P = 0.000.

Step 3 =H_{02} is rejected since (- 1 ≤ r ≤ 1) r = 0.988276, and at 0.05 level of significance α, P-value = 0.000 H_{A2} is accepted.

Step 4 =There is a significant relationship between POS Crime and EPS in the banking industry

Step 5 = POS Crime losses increase with increase in EPS in the banking industry having a positive correlation between both variables.

The finding above depicts that there is a significant relationship between PoS crime loses and EPS of Nigerian banking industry. Which suggests that increasing PoS crime loses is associated with increasing EPS.

4.2.3 Test of hypothesis 3

Step 1 =H_{A3} There is a significant relationship between E-commerce crime and PBT in the banking industry

H_{03} There is no significant relationship between E-Commerce crime and PBT in the banking industry

Step 2 = import pandas as pd
import matplotlib. pyplot as plt
import numpy as np
Import seaborn as sns
From sklearn.pipeline import Pipeline
From sklearn.preprocessing import Standardscaler, Polynomial

Features

```
From sklearn.linear_model import LinearRegression
From Scipy import stats
import statsmodels.api as sm
% matplotlib inline
df = pd.read_csv ('file path') # file path = data address
df. head ()
df. corr ()
sns.regplot(x ="X", y ="Y", data = df) # X is independent variable, Y is dependent variable.
ECOMMERCE = df [['E-COMMERCE']]
PBT = df [['PBT']]
lm1 = sm. OLS.from_formula ("PBT w E-COMMERCE", data = df)
result = lm1. Fit ()
result. Summary
```

Table 14. Correlation test result for e-commerce crime and PBT

	E-Commerce Crime	PBT
E-commerce crime	1.0	0.986632
PBT	0.986632	1.0

Source: Kaggle Notebook 2024

Table 15. P-value test result for e-commerce crime And PBT

	Coef	Std err.	T	p> t
Intercept	$4.595e^{+11}$	$2.91e^{+10}$	15.816	0.000
E-Commerce	2144.2410	158.390	13.538	0.000

Source: Kaggle Notebook 2024

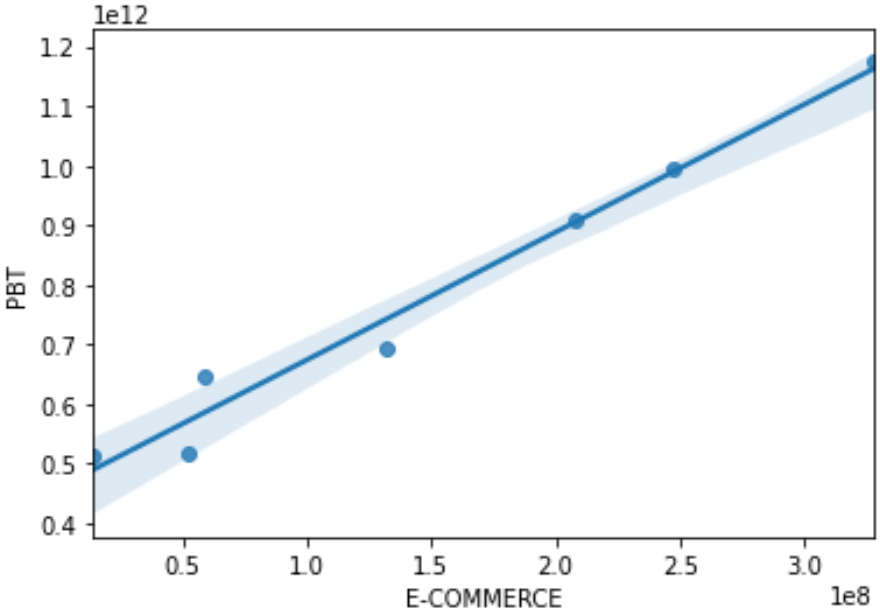

Fig. 3. Regplot of E-commerce crime and PBT
Source: Kaggle Notebook 2024

From the results r = 0.986632, P = 0.00.

Step 3 = H_{03} is rejected since (- 1 ≤ r ≤ 1) r = 0.986632 and at 0.05 level of significant δ, P-value = 0.000 H_{A3} is accepted.

Step 4 =There is a significant relationship between E-commerce crime and PBT in the banking industry.

Step 5 = E-Commerce crime losses increase with increase in PBT since both variable have positive correlation.

This finding proves a significant relationship between E-commerce crime loses and PBT of Nigerian banking industry. Which also suggests a simultaneous increase for E-commerce crime loses and PBT.

5. CONCLUSION

There is a significant relationship between ATM card crime and PAT in the banking industry. From Tables 10 and 11, the correlation coefficient between ATM card crime and PAT is 0.885669 with a p-value of 0.008 upholding that there is a significant relationship between both variables.

Moreover, Fig. 1 shows the regplot between ATM card crime and PAT, indicating that increasing ATM card crime loses is accompanied with increasing PAT in the banking industry, this implies that ATM card crime has tendency to erode resources that could have been accounted as PAT. This further supports the work factors affecting online transaction in the developing countries: A case of E-commerce business in Nairobi county Kenya (Kyalo and Kanyaru, 2015). where they concluded that increased sophistication of fraudsters attacks are specifically a challenge in online transaction (Kyalo and Kanyaru, 2015).

There is a significant relationship between PoS crime and EPS in the banking industry Tables 12 and 13 show a correlation co-efficient of 0.988276 and P-vale of 0.000 respectively. These imply that there is a positive correlation between PoS crime and EPS. Moreover, Fig. 2 shows an ascending positive relationship between PoS crime and EPS, meaning that both variables are increasing simultaneously. Association of these two variables upholds the work of a study on the impact of crime on

Business: A model for prevention, detection and Remedy at Houston, USA (Bressler, 2010). The study concluded that businesses must determine the best way to minimize loss form crime (Bressler, 2010).

There is a significant relationship between E-commerce crime and PBT. Tables 14 and 15 have correlation coefficient for E-commerence crime and PBT as 0.986632 and P-value as 0.000 respectively. These imply a strong positive relationship between both variables. Which also suggests that E-commerce crime increases with PBT by looking at Fig. 3 and is in line with the study E-business at risk: A look at the impact and control of E-business fraud (Behling and Lake, 2010). The study concluded that effects of E-business fraud include heavy financial loss to the tone of about 4 billion USD yearly (Behling and Lake, 2010). This study established a relationship between cyber crime and performance in the Nigerian banking industry after accepting the three hypotheses using a regression algorithm (machine learning). The Pearson's product moment correlation coefficient rs for the three accepted hypotheses were highly positive, greater than -1 but less than 1. This implies that cyber crime losses are progressing geometrically with arithmetic progression in Nigerian banks performance in the industry. This will undoubtedly erode investors return on investment if not checked and regulated. As stated by Fiedler's contingency theory, there is no universal or one best way to manage cyber crime, rather banking organization should find the best fit to mitigate cyber crime losses. This study concludes that mitigating cybercrime with robust cybersecurity system is a new economic knowledge that will shape the growth of the Nigerian banking industry positively.

6. LIMITATION

This study is limited to the available data from Nigeria Commercial Banks annual reports and The Nigerian Electronic Fraud Forum (NEFF) between the period of 2013 to 2019 and thus increases the chances of having the linear regression algorithm overfit the data set, which is a major disadvantage of using this technique with few data set. Furthermore, the data are location bound to Nigeria and may not be applicable to other locations.

7. SUGGESTION

Given that E-business activities are rapidly increasing in Africa in general and Nigeria in particular, it is very pertinent that adequate security measures are put in place to ensure, confidentiality, integrity of sensitive and important data. Based on these, the following recommendations are suggested:

a. Robust data security through encryption is necessary to ensure the authenticity of sensitive information in online activities. This could be achieved through prudent investment in Antivirus technology, efficient backup systems and effective encryption.

b. Total enterprise risk management for E-business platforms through identification and resolution of related threats to sensitive data protections.

c. Government should increase intensive training of law enforcement agencies on ICT so that they can track down cyber criminals no matter how sophisticated the crime may appear.

d. Innocent users should cultivate the habit of continuous update of their knowledge about the ever evolving nature of ICTs, this will make them more informed about the current trends in cyber crimes. Also, users should not provide personal or financial information to others unless there is a legitimate reason to do so.

e. E-business platforms should also consider the latest Biometric technology to data and information security against the regular password and code encryption.

DISCLAIMER (ARTIFICIAL INTELLIGENCE)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc) and text-to-image generators have been used during writing or editing of this manuscript.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

Access bank PLC audited annual reports 2013 to 2020

Adelowo, S. A., & Mohammed, E. A. (2010). Challenges of automated teller machine

(ATM) usage and fraud occurrences in Nigeria: A case of selected banks in Minna Metropolis. *Journal of Internet Banking and Commerce*, *15*(2).

Alade, S. O. (2016). Cross-border expansion of Nigerian banks: Has it improved the continent's regulatory and supervisory frameworks? *The Role of Central Banks in Macroeconomic and Financial Stability*, *76*(1), 83–96.

Amsreas, C. M., & Huido, S. (2016). *Introduction to machine learning with Python: A guide for data scientists* (1st ed.). O'Reilly Media.

Andrew, M. G. (2008). *Machine learning yearning: Technical strategy for AI engineers, in the era of deep learning* (Draft version). Deep Learning.

Arpana, M., & Chauhan, M. (2012). Preventing cyber crime: A study regarding awareness of cyber crime in Tricity. *International Journal of Enterprise Computing and Business Systems*, *2*(1), 2230–8849.

Badillo, S., Banfai, B., Birzele, F., Dauydov, I., Hutchinson, L., Kam-Thong, T., Siebourg-Polster, J., Steiert, B., & Zhang, J. D. (2020). An introduction to machine learning. *Clinical Pharmacology & Therapeutics*, *00*(0).

Balogun, V. F., & Obe, O. O. (2010). E-crime in Nigeria: Trends, tricks, and treatment. *The Pacific Journal of Science and Technology*, *11*(1), 343–355.

Behling, S., & Lake, P. (2010). E-business at risk: A look at the impact and control of e-business fraud. *Issues in Information Systems*, *11*(1), 280–285.

Brain, C. (2000). The measurement of white-collar crime using Uniform Crime Reporting (UCR) data. U.S. Department of Justice, Federal Bureau of Investigation.

Bressler, M. S. (2010). The impact of crime on business: A model for prevention, detection, and remedy. *Journal of Management and Marketing Research*, *1*(1), 1–13.

Creswell, J. W., & Plano Clark, V. L. (2011). *Designing and conducting mixed methods research* (2nd ed.). Sage.

Diebold, I. (2002). *ATM fraud and security: White paper*. New York.

Duah, F. A., & Kwabena, A. M. (2015). The impact of cyber crime on the development of electronic business in Ghana. *European Journal of Business and Social Sciences*, *4*(1), 22–34.

Ecobank Transnational Incorporated. (2013–2020). *Audited consolidated annual reports*.

Fidelity Bank PLC. (2013–2020). *Audited annual reports*.

Fiedler, E. F. (1964). A contingency model of leadership effectiveness. *Advances in Experimental Social Psychology*, *1*(1), 149–190.

First Bank PLC. (2013–2020). *Audited annual reports*.

Florida Tech Magazine. (2019, Winter).

Guaranty Trust Holding Company. (2013–2020).

Han, J., Pei, J., & Kamber, M. (2011). *Data mining: Concepts and techniques*. Elsevier.

Hansen, G. S., & Wernefelt, B. (2007). Determinants of firm performance: The relative importance of economic and organizational factors. *Strategic Management Journal*, *110*(5), 399–411.

Kaelbling, L. P., Littman, M. L., & Moore, A. W. (1996). Reinforcement learning: A survey. *Journal of Artificial Intelligence Research*, *4*.

Kleene, S. C. (1951). *Representation of events in nerve nets and finite automata* (RAND Project Air Force, Santa Monica, CA). https://apps.dtic.mil/docs/citations/ADA596 1387

Kyalo, J. K., & Kanyaru, P. M. (2015). Factors affecting the online transaction in developing countries: A case of e-commerce business in Nairobi County, Kenya. *Journal of Educational Policy and Entrepreneurial Research*, *2*(3), 1–7.

Lin, H., & Bergmann, N. W. (2016). IoT privacy and security challenges for smart home environments. *Information*, *7*(44).

McCallum, A. (2005). Information extraction: Distilling structured data from unstructured text. *Queue*, *3*(9).

Midhun, M., Sreelakshmi, V. R., Lavanya, K. M., Nabeela, M., Nandini, B., & Prabhu, M. (2017). Cloud-based POS with online purchase. *International Journal of Engineering and Management Research*, *7*(2), 33–47.

Mohammed, M., Khan, M. B., & Bashier, M. B. E. (2016). *Machine learning: Algorithms and applications*. CRC Press.

Nwabuike, C. C., Onodugo, V. A., Arachie, A., & Nkwunonwo, U. C. (2020). Blockchain technology for cyber security: Performance implications on emerging markets multinational corporations, overview of Nigerian internationalized banks.

International Journal of Scientific & Technology Research, *9*(8).

Okeshola, B. F., & Adeta, A. K. (2013). The nature, causes, and consequences of cyber crime in tertiary institutions in Zaria–Kaduna State, Nigeria. *American International Journal of Contemporary Research*, *3*(9), 98–114.

Olayemi, J. O. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, *6*(3), 116–125.

Oluduro, F. O. (2015). History and evolution of banking in Nigeria. *Academia Arena*, *7*(1), 1–6.

Olusola, M., Ogunlere, S., Ayinde, S., & Adekunle, Y. (2013). Impact of cyber crimes on Nigerian economy. *The International Journal of Engineering and Science*, *2*(4), 45–51.

PayPal Market Intelligence. (2013). *The future of POS: Point of sale evolution and its impacts*.

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., et al. (2011). Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research*, *12*.

Romer, P. M. (1994). Beyond classical and Keynesian macroeconomic policy. *Policy Options*, *1*(5), 15–21.

Sarker, I. H. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. *SN Computer Science*.

Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. *SN Computer Science*, *2*, 160.

Sarker, I. H., Hoque, M. M., Uddin, M. K., & Tawfeeq, A. (2020). Mobile data science and intelligent apps: Concepts, AI-based modeling and research directions. *Mobile Networks and Applications*.

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from a machine learning perspective. *Journal of Big Data*, *7*(1), 1–29.

Stanbic IBTC. (2013–2020). *Audited annual reports*.

Sterling Bank PLC. (2013–2020). *Audited annual reports*.

Steve, W. (2002). Automated teller machines. *CGAP Staff and Exchange, CGAP IT Innovation Series*, Los Angeles.

Sumanjit, D., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International Journal of Engineering Sciences and Emerging Technologies*, *6*(2), 142–153.

The Nigeria Electronic Fraud Forum. (2014). *Annual report*.

The Nigeria Electronic Fraud Forum. (2016). *Annual report*.

Union Bank PLC. (2013–2020). *Audited annual reports*.

United Bank of Africa. (2013–2020). *Audited annual reports*.

WEMA Bank PLC. (2013–2020). *Audited annual reports*.

Wigand, T. W. (1997). Electronic commerce: Definition, theory, and context. *The Information Society*, *13*(1), 1–16.

Witten, I. H., & Frank, E. (2005). *Data mining: Practical machine learning tools and techniques*. Morgan Kaufmann.

Zenith Bank PLC. (2013–2020). *Audited annual reports*.

Peer-review history:
The peer review history for this paper can be accessed here:
https://pr.sdiarticle5.com/review-history/134584