NATIONAL INNOVATION AND RESEARCH ACADEMIA
International Journal of Computing, Engineering and Information
ISSN: 2713-4677. Volume 8, Issue 7. Pages 1-17. March, 2025
OTL: 6472-03062-871-5
Double Blind Peer Reviewed International Research Journal
https://arcnjournals.org
journals@arcnjournals.org

ARTIFICIAL INTELLIGENCE AND INFORMATION SECURITY MANAGEMENT OF COMMERCIAL BANKS IN EMERGING ECONOMIES IN RIVERS STATE

Happiness Nwanyi ELEKWACHI, PhD[1]
&
Josephine Onyeri EKE, PhD[2]
[1&2]Department of Office and Information Management, Faculty of Management Sciences, Ignatius Ajuru University of Education, Port Harcourt

Abstract: *This study investigated the relationship between Artificial Intelligence and information security management of commercial banks in Rivers State. Four research questions and hypotheses were stated for the study. The variables of the study were chatboth, automated control and automated fraud detection as dimensions of artificial intelligence and information security planning and information security control as measures of Information security management. A sample size of 150 was selected from a population of 400 comprising senior employees of commercial banks in Rivers State. A descriptive survey research design was employed for the study. The research instrument used for the study was a researcher-developed questionnaire. The data generated was analyzed using mean, standard deviation and coefficient of variance. The findings of the study revealed that artificial intelligence has a significant relationship with information security management in commercial banks. It recommends that artificial intelligence should be systematically implemented by banks not just as a form of competition but as an overall business strategy to ensure information security and banks should integrate Artificial intelligence such as chatboth, automated control and automated fraud detection for enhanced operational efficiency and information security of the banking industry.*

Keywords: *Artificial Intelligence, Information Security Management, Commercial Banks, Rivers State, Nigeria.*

Introduction

Information is vital for managers, scientists, and practitioners in the banking sector to make decisions, to prepare plans, to control activities, to outcast competitors to provide services, manage inflow of outflow of cash and meet customers' needs. Information, formal or informal, is however to be managed. Information is now seen as a valuable resource within the banking industry. It is an organizational resource, a self-regenerative resource and a key economic element in bank management. It can be accessed by anyone from anywhere, any number of times, yet remains undiminished and unchanged. This requires intensive use of information technologies. It is a resource that, if it is properly

managed and used, can stimulate innovation, speed product development, raise levels of productivity, ensure consistent standards of quality and through all these means raises the relative level of competitiveness (Dirican, 2015; Lucky, 2018). The proliferation of online and mobile banking platforms has caused customers to adjust their expectations, calling for banking experiences that are both more customized and convenient. Considering this, financial institutions are under intense pressure to implement cutting-edge technical solutions to maintain their market relevance (Dumasia, 2021).

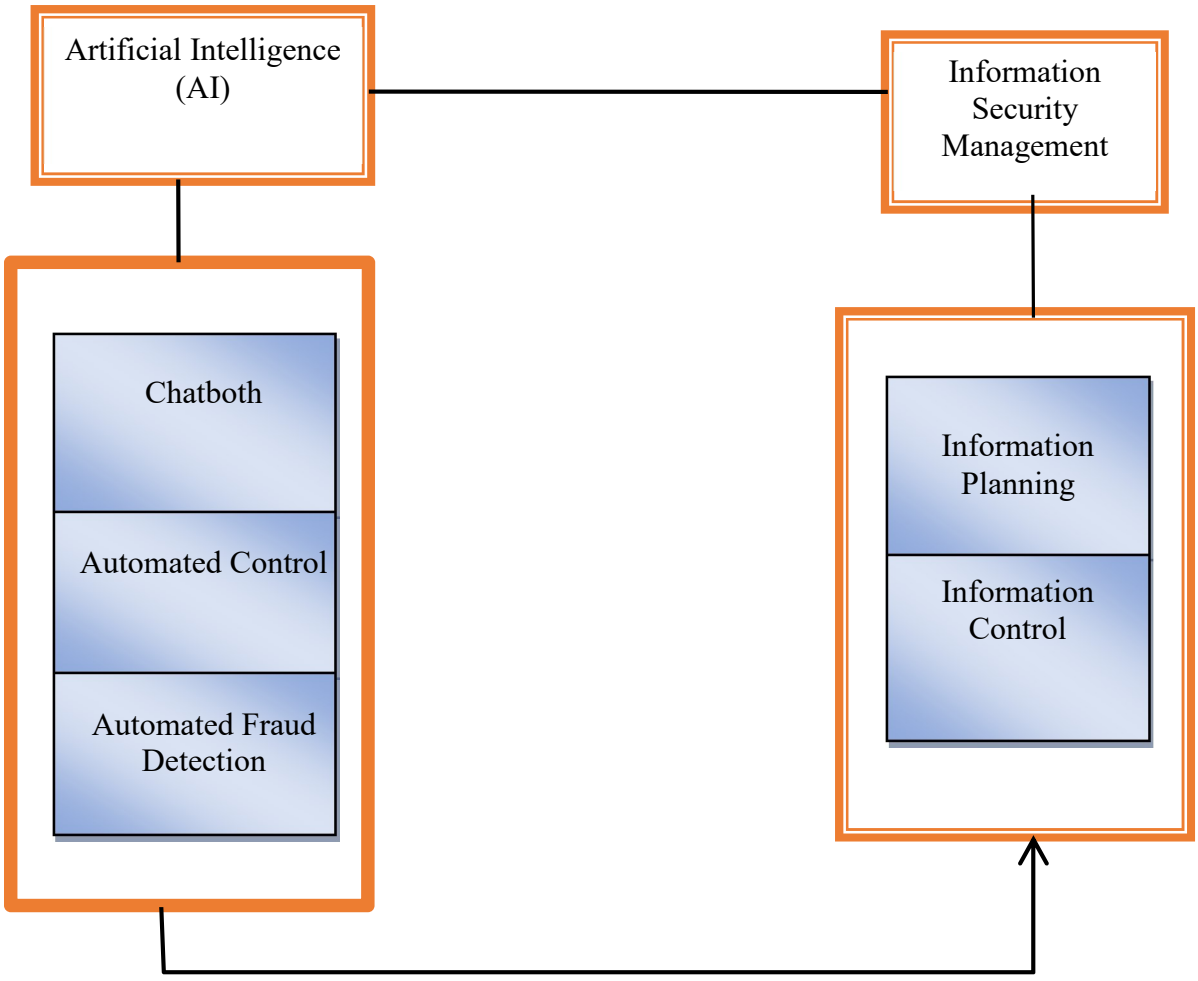
The use of technologies that utilize artificial intelligence has the potential to usher in a period of profound change within the banking sector. The term artificial intelligence refers to a wide range of applications, some of which include machine learning algorithms, natural language processing, robotic process automation, and chatbots (Fernando, 2018). Artificial intelligence as perceived by Ikegwuru, Jack and Amadi (2023) "is scientific mechanisms utilized to make a replica of humans' cognitive aptitudes to accomplish objectives independently". According to Brown et al. (2019), the use of these technologies may result in a broad variety of positive outcomes, including increased customer experience, greater operational efficiency, more efficient risk management, and sophisticated data analytics. In addition, artificial intelligence may aid financial institutions in offering tailored suggestions, automating mundane processes, identifying fraudulent activity, and enhancing cyber security measures (Eryk, 2020). However, the incorporation of artificial intelligence into banking operations is accompanied by a series of problems, some of which include issues over data privacy, ethical conundrums, the need to comply with regulatory requirements, and the possibility of job displacement (Holtel, 2016). The thoughtful examination of these difficulties and the development of suitable methods to address them are required to carry out the adoption of artificial intelligence solutions in a manner that is both effective and responsible.

Understanding the effects that artificial intelligence on the banking industry is very necessary if one is to consider the importance of the sector as well as the disruptive potential of AI (Kumar, 2021). Conceptually, the term artificial intelligence (AI) refers to a kind of technology that has been more popular and widespread in recent years. Artificial intelligence has the potential to completely transform many different types of businesses and sectors. The financial services business is one that stands to benefit significantly from the use of AI. Banks are already employing AI to improve their services for all consumers, from the identification of fraudulent activity to customer care. This helps the banks simplify their processes, which in turn lowers their expenses. On the other hand, this is just the beginning, and the use of AI in banking will likely lead to far more fascinating opportunities in the future. There are many studies on the effect of artificial intelligence, some of the studies focused artificial intelligence and corporate performance. Eno (2022) investigated the integration of artificial intelligence applications for financial process innovation by commercial banks in Nigeria while Elegunde and Osagie (2022) examined Artificial Intelligence and Employee Performance in the Nigerian Banking Industry. This study focused on Artificial Intelligence and information management of commercial banks in Rivers State, Nigeria. The study provides answers to the following research questions:

i. to what extent does chatbot relate to information security planning of commercial banks in Rivers State?
ii. how does automated control relate to information control of commercial banks in Rivers State?

iii. to what extent does automated fraud control relate to information planning of commercial banks in Rivers State?
iv. to what extent does automated fraud detection relate to information planning of commercial banks in Rivers State?

Conceptual Framework



Source: Conceptualized by the Researcher (2024) with dimension of artificial intelligence sourced from the work of Andreas Svoboda, (2023) and measures of information security management sourced from the work of Odozi (2023).

Literature Review

Artificial Intelligence

Artificial Intelligence connotes the ability to adapt effectively to environmental changes either by making changes to oneself or changing the environment through machine

(Britannica, 2001). It entails the study of how to make computers do things in which now humans are better (Nordlander, 2001). Due to the broadness of the concept of AI, it has been subdivided into Weak AI and Strong AI (Nordlander, 2001). Weak AI advocates argue that it involves adding some types of thinking features to computers to make them more useful for humans, while Strong AI proponents maintain that computers can be made to mimic the thinking process of the human brains, such as robotics (Russell & Norvig, 2001; Goodwins, 2001). Maney (2001) reported that AI helps manage workload by understanding what humans are doing, evaluating work, making decisions about what information and messages should be delivered at a given time.

Artificial Intelligence as the simulation of human intelligence processes by machines, particularly computer systems The processes include learning (the acquisition of information and rules for using it), reasoning (the use of rules to reach approximate or definite conclusions), and self-correction Artificial Intelligence systems can perform tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making and language translation Russell and Norvig, P (206)

Artificial Intelligence is the ability of a computer programme or a machine to think and learn. It is also a field of study which tries to make computers smart. They work on their own without being encoded with commands. The first mention of AI was in 1955 by John McCarthy. Kaplan and Haenlein (2018) classified AI into three (3) types of AI systems, vis, Analytical AI which has characteristics consistent with cognitive representation of the world and using learning based on past experience to inform future decisions; Human-inspired AI which has elements from cognitive as well as emotional intelligence, understanding, as well as human emotions that are considered in their decision making process; and Humanized AI which shows characteristics of all types of competencies (cognitive, emotional and social intelligence) and are able to be self-conscious and self-aware in interactions with others. This can be achieved by observing AI through the lens of evolutionary stage (artificial narrow, artificial general intelligence, and artificial super intelligence) or by focusing on different types of AI systems (analytical AI, human-inspired AI, and humanized AI).

The 21st century has since experienced resurgence in AI techniques following concurrent advances in computer power, large amounts of data, and has become an essential part of the technology industry, helping to solve many challenging problems in computer science, software engineering and operational research (Dudhe & Rane, 2017). AI is not some magic wielding computerized character, it involves a wide range of algorithms (that are fast and can analyze millions of information in seconds) and machine learning tools that can rapidly inject data, identify patterns, optimize and predict trends (Ahmed, 2018). The system can understand speech, identify photos using pattern matching to pick up signals that are necessary. Statistically, AI systems can predict and learn by plotting curves of possible outcomes and then optimizing decisions based on many criteria.

Chatbot

Chabot technology is one of the most innovative and interesting forms of artificial intelligence (AI) software. It engages clients using preprogrammed questions to provide polite, effective communication and immediate issue resolution. Chabot technology is one of the most fascinating and distinctive forms of AI technology. According to Eno (2022) chatbot technology in banks not only answers customers' questions without the need for

human contact, but it also gathers data on customers' questions, which may then be utilized to handle unforeseen issues in the future (Svoboda, 2023).

Automatic Control

The application of Artificial Intelligence technology in the banking industry without the assistance of human beings can also be witnessed when digital computers count the cash in a precise (accurate) and speedy manner. This automation technology assistance results in a rise in the daily business volume of the banks, which concurrently lowers the amount of work-related stress and mathematical count mistake associated with cash-counting. The implementation of automation systems in the banking industry has produced a productive atmosphere that is receptive to the introduction of this technology in almost all the operational facets of financial institutions in the not-too-distant future.

Automation (mechanization or computerization) has been achieved by various means including mechanical, hydraulic, pneumatic, electrical, electronic devices, and computers, usually in combination (Walter,2017). Complicated systems, such as modern factories, aero planes, and ships typically use all these combined techniques. The benefits of automation includes labor savings, reducing waste, savings in electricity costs, savings in material costs, and improvements to quality, accuracy, and precision.

Detection of Frauds

Due to the high number of corporate financial transactions and the complexity of the job duties, financial institutions are more often exposed to the danger of fraud than other types of businesses. As was said previously, artificial intelligence makes use of mathematical calculation and intricate algorithms to assist monitor the behavior of both customers and employees by using unsupervised learning programs (Holtel, 2016). Consequently, the use of AI technology may make the prevention of fraud an easier task (Kaplan & Haenlein, 2018).AI is solely based on the machine learning programming method, and its primary goal within the banking industry is to take over jobs formerly performed by humans to protect business function performance from possible risks.

Information Security Management

Baskerville and Siponen (2002) defines information security management (ISM) as the controls that an organization needs to implement to ensure that it is sensibly managing risks that relate to protection of information and information infrastructure assets. The emerging trends (learning or movement) in information technology (IT) have resulted in organizations using different approaches to effectively manage information security. These approaches include risk-based approach and business aligned security approach (Odozi, 2023). The growing adoption of information security management practices (ISM) has been driven by the requirement for the information technology (IT) industry to better manage the quality and reliability of IT in business and respond to a growing number of regulatory and contractual regulatory and contractual requirements.

Information security management practices include COBIT, ITIL, and ISO/IEC 27000. These practices underpin different areas and requirements within the organization to enable it effectively to attain its goals both organization and business. Control Objectives for Information and related Technology (COBIT)'s focus is on development of clear policies and good practices for security and control in IT. It provides managers with a set of generally accepted measures, indicators, processes and best practices to assist them

in maximizing the benefits derived with IT and developing appropriate IT governance and control in an organization. COBIT ensures ISM and business alignment, ISM-enabled business processes, resource optimization and management of risks (Odozi, 2023). ISO/IEC is a standard for the information security industry that includes a comprehensive set of controls and best practices. This standard is intended to serve as a single reference point for identifying a range of controls needed for situations where information systems are used in industry and commerce (Larsen et al, 2006).

Many organizations are currently managing information technology security in applications 'slightly targeting security implementations that are not consistent or integrated across the enterprise. This approach often involves the use of "point security" for specific problems but does not provide a holistic approach for centralized security management. It may provide short-term benefits to a particular department or business unit, but this is often at the expense of future IT efficiency and effectiveness at the enterprise level (Blaunt, 2007; Odozi, 2023). A solution to such a problem is the approach of aligning all necessary information security actions seamlessly with the business management and business processes and how to consider the realities and requirements of the modern business environments.

Information security management systems have emerged as a contentious topic not only in information security but also in information management (Benson, McAlaney, & Frumkin, 2018; Bulgurcu, Cavusoglu & Benbasat, 2010); Odozi, 2023). Contemporary financial, and services-providing institutions are integrating intrinsically diverse workforce, physical assets, and process management with governance strategies and objectives for providing a competitive advantage for their business, as well as investing significant resources in developing and operating information systems to support the preceding operation. Firms increase overall productivity by sharing information through such information, but there are adverse effects that occur simultaneously, such as provoking a new criminal activity consisting of information being retrogressed from initially planned objectives or implications (Chen, Ramamurthy, & Wen, 2018; Odozi, 2023). Firms often created technical information security mechanisms in the early stages to address the negative impacts of digitization, but their focus is increasingly shifting to management security considering the features of contemporary information breaches. They are constructing information assurance systems comprised of five information protection organizational activities, notably, policy and organizational formation, controlling risks, implementation of programs, and follow-up control, to provide an organization with adequate in-depth information protection systems (Eloof & Von, 2000; Odozi, 2023).

Control Objectives for Information and related Technology

The Control Objectives for Information and related Technology (COBIT) is a certification created by ISACA and IT Governance Institute (ITGI) in 1996. COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues, business risks, and security issues. It entails a set of 34 high level control objectives for each of the IT processes that are grouped into four domains namely: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor. COBIT has five governance areas of concentration which include strategic alignment, value delivery, resource management, risk management and performance measurement. Strategic alignment focuses on ensuring the linkage of business and IT

plans (Odozi, 2023). Value delivery is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing cost, and proving the intrinsic value of IT. Resource management is about the optimal investment and the management of critical IT resources. Risk management is a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, and transparency into the organization. Performance measurement racks and monitors strategy implementation, resource usage, project completion, process performance and service delivery.

The adoption and integration of information communications technology (ICT) into the business process is indeed spreading rapidly and firms seek to improve their efficiency through increased integration of ICT. Information security has too often been viewed in isolation the perception being that security is someone else's responsibility and there is no collaborative effort to link the security program to business goals (ISACA, 2009). It is emerging that information security has struggled as a function in most organizations due to changing risk profiles, lack of funding, cultural issues and internal and external threats. In addition, Information security management problems are characterized by complexity and interdependence. This point to the need for an aligned approach to ISM, which not only involves technical measures but also policies, procedures and education to ensure that data is treated in an appropriately secure way at all times (Johnston & Warkentin, 2010; Odozi, 2023). The reason why the alignment of ISM has often not taken place effectively could be the fact that a company's own leadership system has not yet taken shape to a sufficient degree, resulting in the lack of points to grasp onto. It might also be the case that information security issues are delegated too much and to experts only, who will then create their own position.

Information Security Planning

Information security planning is the framework and core functions of identify, protect, detect, respond and recover work to access cyber security risks. The various functions are broken down into categories to determine the needs of the organizational programming. The subcategories are an additional subdivision below categories that help narrow down the specific technical and managerial resources that are needed to combat threats. The purpose of the identify function is to obtain an understanding of the organization's ability to detect threats and protect against their negative effects (Odozi, 2023). The protection aspect involves introducing new security protocols that will handle the needs of the organization. The detection element requires the security protocols to find threats and adapt the system to protect against similar attacks. The purpose of the response function is to develop security systems that will carry out solutions that fight against threats. The system must also be able to recover lost information and capabilities that were affected by cyber security breaches.

Information Security Controls

Information security control are measures that help to reduce risks such as breaches, data, theft and unauthorized Technical control, eg Firewalls, Antivirus software, Authentication solutions and usernames and passwords(researcher view)

In a business context, control can help in maintaining behaviours that can assist in improving the performance of a company (Kee, 2001). It is a challenge for management to implement change and controls in any organization (Jensen, 2017). Management must exercise control over people, processes, and technology through a risk awareness

program to positively affect the company. Several drivers such as internal and external threats, and business and regulatory requirements are necessary to analyze to create a proper control system for an effective information management system (Mahmoudzade & Radrajabi, 2007). Mantha, García de Soto (2021) stated that senior management at the board level and their support for organizational level information security initiatives will help to bring security awareness across the company with minimal resistance from employees for a change to adopt new processes and procedures to implement new security controls.

The alignment of people, processes, and technology at every level of the organization towards risk management helps in reducing internal and external threats from cyber-attacks (Chen, Ramamurthy, and Wen, 2018; Kour and Karim, 2020). Organizations that integrate and align people, processes, and technology into the overall business process lower the costs of data breaches (Kovacich, 1998; Prentice, Dominique Lopes, & Wang, 2020; Sabillon, Serra-Ruiz, Cavaller & Cano, 2019). Companies that have an alignment gap between organizational resources are found to have an increased amount of security risks. This literature review includes the effect of managerial capabilities on creating organizational readiness for handling information security risks. The leadership competencies of a manager play a large part in how the organization prevents and responds to threats.

Theoretical Review

Information Security Theory

This study is anchored on information security theory by Hong et al. (2003). The theory was a conceptual basis for exploring strategies that chief information security officer could use to provide tailored information security strategies to prevent cyber exploitation of financial institutions in Nigeria. The theory includes five individual theories: contingency theory, risk management theory, information security policy theory, control, and audit theory, and management system theory (Hong et al., 2003). Though there is no consistent security policy theory, one of the fundamental theories of the IST (Hong et al., 2003), there is a consensus that one of the key and fundamental means of achieving information security is by the establishment, operationalization, and maintenance of information security policy (Farrell & Gallagher, 2015).

The information policy theory advocates the identification of information security requirements in an organization, drafting, and implementing policies to meet those security requirements. The policy states there must be an explicit and formal declaration of what is allowed and what is not allowed in terms of using information assets within the allowance of the information security objectives in an organization (Benson, McAlaney & Frumkin, 2018). The information policies of an organization must also be current and relevant (Ogalo, 2012). The information security policy must be regularly maintained and updated to be relevant for information security in the context of the organization to be protected. Information security policies address the human element of information security in organizations (Nica, Potcovaru & Hurdubei, 2019). The postulates of the theory will, therefore, help to achieve the security that pertains to the human element. The risk management theory component of the IST suggests that through an analysis of the risks

existing in an organization, information security threats and vulnerabilities can be identified, estimated, and assessed.

Technology Acceptance Model (TAM) Theory

The Technology Acceptance Model theory postulated by Davis (1989), states that perceived usefulness and perceived ease of use are the main drivers of technology, and these determine an individual's intention to adopt a technology. This theory as adapted from the Theory of Reasoned Action (TRA) by Ajzen and Fishbein (1980) and Theory of Planned Behaviour (TPB), developed by Ajzen (1985), which is tailored to the context of technology acceptance and usage supports how cash handling practices influence financial performance. According to Bátiz-Lazo (2018), the intention to use serves as mediator of the actual adoption of technology. To the words of Bátiz-Lazo (2018), the decision to adopt a technology follows the four stages as explained below: Stage one is where the external variables such as individual user beliefs or differences with Information Technology. Their evaluation is reflected in Perceived Usefulness (PU) and Perceived Ease of Use (PeU).

Whereas perceived usefulness is a user perception that using the new system would increase his/her performance in the organization and perceived ease of use is the extent to which using the new system would require minimal effort on a user's behalf (Tilakaratna,x 2016). Stage two is attitude which is a consequence of the user's beliefs of using a technology drives the user's attitude towards accepting/rejecting the technology. Stage three is intention where the attitude predicts the desirability of the user using the system and the extent of them using it. Stage four is actual use which is the user's intention to determine how well they would use the system. The adoption of technology depends on personal behaviour and external environment. People perceive that by using technology, they will obtain more benefits without doing much physical and mental effort (Tilakaratna, 2016).

Empirical Review

Eno (2022) investigated the Integration of Artificial Intelligence (AI) applications for financial process innovation by commercial banks in Nigeria. Three specific objectives and three research questions and hypotheses were stated for the study. The variables of the study were AIs for credit risk management, personalized banking experience and the challenge of implementing AI in commercial banks in Nigeria. A sample size of 143 selected from a population of 174 comprising accounting lecturers in public universities in Akwa Ibom State and bank managers, operational staff and key personnel in commercial banks operating in Uyo, Akwa Ibom State were used for the study. Descriptive survey research design was employed for the study. The research instrument used for the study was a researcher- developed questionnaire tagged "Artificial Intelligence Applications for Financial Process Innovation Questionnaire" (AIAFPIQ). The instrument developed by the researcher was face validated by three experts in the Faculty of Social Sciences, Akwa Ibom State University. The instrument was administered to 20 persons who were not part of the sample but part of the study population. The result was then coded for testing using cronbach alpha technique. The reliability index yielded 0.89.

The data generated was analyzed using mean, standard deviation and t-test Analysis. Findings of the study revealed that AI can be applied for credit risk management and personalized banking experience. Furthermore, Experts (Bankers and Accounting Lecturers) do not differ significantly on their responses on application artificial intelligence (AI) in credit risk management and personalized banking experience in promoting financial process innovation by commercial banks in Nigeria. It was recommended among others that AIs should be systematically implemented by banks, not just as a form of competition but as an overall business strategy; and that the international financial community should actively cooperate to share new scientific and technological achievements, to establish and improve the financial market of AI, so that the welfare of the society brought by financial AI will ultimately shine on mankind.

Elegunde and Osagie (2022) examined Artificial Intelligence and Employee Performance in the Nigerian Banking Industry, Lagos Nigeria as a study to generalize results. The objective of this study was to examine the complement ability of AI to work processes and to know if it eases employee operations in banks in Nigeria. Cross-sectional descriptive research design was adopted by the researcher. Primary data was to elicit information for this study. The population of the study was the entire employees of six (6) selected banks operating in Lagos State, Nigeria, which totaled 127 staff. The study adopted Taro Yamane (1967) sample size determinant to arrive at a sample size of 98 elements. 98 copies of questionnaires were administered to respondents of six banks in Lagos State, Nigeria, which was divided using simple proportion and ratio among the six banks, 98 respondents were used for data analysis. Content validity was adopted for this study. Reliability test was conducted using Cronbach Alpha and it returned 0.773 showing internal consistency of research instrument. Descriptive statistics such as mean, simple percentage was used to analyze the demography of respondents while regression and Pearson correlation coefficients were used to analyze data. The findings revealed that Artificial Intelligence complements work process in banks in Nigeria and that machine-aided tasks ease operations in banks in Nigeria. The study recommended the adoption of AI by not only banks but all other firms in the service industry; the need for all employees and people to be educated on the importance of embracing AI; the upgrading of school curriculum at all levels in developing and third world economies to incorporate AI and its accompanying gadgets.

Manju (2019) in a landmark study on artificial intelligence in finance, understanding how automation and machine learning is transforming the financial industry. The study examined the influence of artificial intelligence in modern world, especially in the field of finance. This research focuses on the application of artificial intelligence, its challenges, opportunities and its impact on jobs and functions. The research applied qualitative and quantitative research designs. This study found that many financial sectors have been benefiting greatly by implementing different artificial intelligence applications. The study found AI useful in fraud detection, credit scoring and personalized banking experiences in the form of rob advisers and chatbots among others.

Nekesa and Olweny (2018) investigated the effect of financial innovation on financial performance: a case study of deposit-taking savings and credit cooperative societies in Kajiado County. It was established that product, process and organizational innovations are the critical factors that influence the performance of the financial status of deposit-taking money banks. The challenges of implementing innovation are staff and institutional

adaptability, security and compliance. While the above studies are well established, they failed to capture the relationship between artificial intelligence and information security management of commercial banks in Rivers State, Nigeria.

Methodology

This study was conducted in Rivers State, Nigeria. The design of the study was quantitative, employing the descriptive survey research design for the study. The population is 400 respondents, comprising of employees of commercial Banks in Rivers State, Nigeria. The sample size is 150 determined through the Krecjie and Morgan Finite (set). The Sample comprised of senior staff of the 24 commercial banks operating in Rivers State. Simple random sampling was used. The research instrument used for the study is a researcher-developed questionnaire. All items in Section B were structured using a four-point rating scale of Strongly Agree (SA), Agreed (A), Disagree (D) and Strongly Disagreed (SD) with weighted options of 4,3,2 and 1 respectively. The instrument developed by the researcher was face-validated. All corrections and inputs were built into the final version of the instrument. The test-retest method was used to determine the reliability of the instrument. The instrument was administered to 30 persons who were not part of the sample but part of the study population. The result was then coded for testing using cronbach alpha technique. The reliability index yielded 0.78. Based on the high-reliability index, the instrument was deemed suitable to be used in conducting the study. The data generated was analyzed using mean, standard deviation and coefficient of variance.

Analysis and Discussion of Results

Table 1: To what extent does chatboth relate to information policy of commercial banks in Rivers State?

Chatboth	Mean	Std. Deviation	Coefficient of variation
Chatboth enhances information planning	2.68	.740	27.6
The objective of information planning can facilitated using chatboth	2.54	.654	25.7
Chatboth promote effective information planning	2.52	.597	.23.6

Source: Field Data (2024)

Table 1 shows the item analysis on relationship between chatboth and information planning of the commercial banks. The study identified 3 ways of applying chatboth for information planning in the banking experiences. Table 2 shows that all the items have mean responses above 4 and above, standard deviation of less than 1 and coefficient of variation of 2 and above indicating strongly agreed. Thus, all the items were taken as being ways and means of managing information planning in the commercial banks.

Table 2: How does automated control relate to information control of commercial banks in Rivers State?

Chatboth	Mean	Std. Deviation	Coefficient of variation
Chatboth enhances information control	4.52	.601	13.3
The objective of information control can facilitated using chatboth	4.66	.658	14.12
Chatboth promote effective information control	4.52	.599	13.25

Source: Field Data (2024)

Table 2 reveals the item analysis for how application of Chatboth relate to information control of the commercial banks in Rivers State. The study identified 3 ways of applying Chatboth for information control management. Table 2 showed that all the items have

mean responses above 4, indicating strongly agreed. Thus, all the items were taken as being ways and means of promoting information security control.

Table 3: To what extent does automated control relate to information planning of commercial banks in Rivers State?

Automated Control	Mean	Std. Deviation	Coefficient of variation
Automated control relate to information planning	4.71	.483	10.25
automated control has been used to manage information planning	4.57	.597	13.06
The need for adequate security planning is achieved by automated control	4.57	.597	13.06

Source: Field Data (2024)

Table 3 gives the summary of the mean and standard deviation of respondents on the relationship between automated control and information planning of commercial banks in Rivers State. The result shows that all the 3 items have mean responses above 4,0 and standard deviation less than 1.0 and coefficient of variation of above 10.0 indicating strongly agreed by all the experts on the relationship between automated control and information planning.

Table 4: How does automated control relate to information control of commercial banks in Rivers State?

Automated control	Mean	Std. Deviation	Coefficient of variation
Automated control relate to information control	4.51	.589	13.05
Automated control has been used to manage information control	4.31	.567	13.15
The need for adequate security control is achieved by automated control	4.42	.597	13.50

Source: Field Data (2024)

Table 4 shows the item analysis on relationship between automated control and information planning of the commercial banks. The study identified 3 ways of applying automated control for information planning in the banking experiences. Table 4 showed that all the items have mean responses above 4 and above, standard deviation of less than 1 and coefficient of variation of 13 and above indicating strongly agreed. Thus, all the items were taken as being ways and means of managing information planning in the commercial banks.

Table 5: To what extent does automated fraud detection relate to information planning of commercial banks in Rivers State?

Automated Fraud Detection	Mean	Std. Deviation	Coefficient of variation
Automated fraud detection relate to information planning	4.33	.730	16.85
Banks have to adopt automated fraud detection to safeguard customers	4.47	.679	15.19
The use of automated fraud detection enhances management information planning	4.67	.657	14.06

Source: Field Data (2024)

Table 5 reveals the item analysis for how application of automated fraud detection relate to information planning of commercial banks in Rivers State. The study identified 3 ways of applying automated fraud detection for information planning management. Table 5

showed that all the items have mean responses above 4, indicating strongly agreed. Thus, all the items were taken as being ways and means of promoting planning security.

Table 6: To what extent does automated fraud detection relate to information control of commercial banks in Rivers State?

Automated Fraud Detection	Mean	Std. Deviation	Coefficient of variation
Automated fraud detection relate to information control	4.33	.658	15.19
Banks have to adopt automated fraud detection for effective control of information	4.42	.676	15.29
The use of automated fraud detection enhances management information control	4.52	.601	13.29

Source: Field Data (2024)

Table 6 gives the summary of the mean and standard deviation of respondents on the relationship between automated fraud detection and information control of commercial banks in Rivers State. The result shows that all the 3 items have mean responses above 4.0 and standard deviation less than 1.0 and coefficient of variation of above 10.0 indicating strongly agreed by all the experts on the relationship between automated fraud detection and information control.

Discussion of Findings

The findings of the study show that respondents strongly agreed on the relationship between artificial intelligence and information security management in the commercial banks in Rivers State. The study identified ways of artificial intelligence relate to security of information. Table 1-6 showed that all items have mean responses above 2.5 and 4.0 with standard deviation less than 1 and coefficient of variation above 10.0 indicating strongly agreed. Thus, all the items were taken as being ways and means of managing information in the banking industry. This finding is corroborated by Nekesa and Olweny (2018) who investigated effect of financial innovation on financial performance. They found artificial intelligence and other innovations as enriching the customer experience and making customer service more flexible while extending more services to the customers. This finding is also supported by Manju (2019) who investigated artificial intelligence in finance, understanding how automation and machine learning is transforming the financial industry. This study found out that many financial sectors have been benefiting greatly by implementing different artificial intelligence applications and the finding is supported by Manju (2019) who found that artificial intelligence is changing the financial service industry with positive effects, but also exposing the banks to systems that might soon be beyond their control while also introducing errors that would be costly to the banks in terms of dollars and cents

Conclusion

The integration of chatbots, automated control systems, and automated fraud detection significantly enhances information planning and control in commercial banks while promoting responsible consumption and production practices. These technologies not only improve operational efficiency and customer satisfaction but also support sustainable banking practices in emerging economies, ultimately contributing to a more secure and accountable financial environment.

The influence that artificial intelligence has had and will continue to have on the banking sector cannot be denied. Artificial intelligence has ushered in a new era of efficiency, greater consumer experiences, and improved risk management. However, securing the appropriate and successful integration of artificial intelligence in banking is dependent on tackling ethical issues, algorithmic bias, and workforce difficulties head-on. Banks will be able to fully grasp the promise of Artificial intelligence if they navigate these issues with care and continue to adapt despite the fast-changing environment of the financial industry. The potential gains in areas such as predictive analytics, regulatory compliance, and customized financial services suggest a bright future for the integration of artificial intelligence in the banking sector. It is imperative for the banking sector to persist in adopting artificial intelligence in a prudent manner, ensuring a harmonious equilibrium between groundbreaking advancements and the conscientious and ethical use of Artificial intelligences. From the findings, the study concludes significant relationship between artificial intelligence and information security management in commercial banks in Rivers State.

Recommendations

i. Artificial intelligence should be systematically implemented by banks not just as a form of competition but as an overall business strategy to ensure information security.
ii. Banks should integrate Artificial intelligence such as chatboth, automated control and automated fraud detection for enhanced operational efficiency of the banking industry
iii. Commercial banks can integrate Artificial intelligence for assisting in managing information and reduce information breach
iv. As the global financial world adopts Artificial intelligences for financial services, banks in Nigeria should follow the same lines for seamless transition into the digital age.

Refernces

Elegunde, F.A., & Osagie, R.A., (2022). Artificial intelligence adoption and employee performance in the Nigerian banking industry. *International Journal of Management and Administration*, 1(2), 90-110.

Ahmed, O. (2018). Artificial Intelligence in HR. *International Journal of Research and Analytical Reviews, 5(4), 971-978.*

Baskerville, R. & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management, 15 (5/6), 337-346.*

Benson, V., McAlaney, J., & Frumkin, L. A. (2018). Emerging threats for the human element and countermeasures in current cyber security landscape. In *Psychological and Behavioral Examinations in Cyber Security* (pp. 266-271). IGI Global.

Benson, V., McAlaney, J., & Frumkin, L. A. (2018). Emerging threats for the human element and countermeasures in current cyber security landscape. In *Psychological and Behavioral Examinations in Cyber Security* (pp. 266-271). IGI Global.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34 (3), 523-548*.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2018). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11-19.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2018). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11-19.

Dirican, C. (2015). The impacts of robotics, artificial intelligence on business and economics. Procedia Social and Behavioural Sciences, 195, 564-573.

Dumasia, J. (2021). 5 applications of artificial intelligence in banking. https://ibsintelligence.com/ibsi-news/5-applications-of-artificial-intelligence-in-banking/.

Eno, G. U. (2022). Integration of artificial intelligence applications for financial process innovation by commercial banks in Nigeria. *AKSU Journal of Administration and Corporate Governance, 2(1), 125-137*

Eryk, L. (2020). Artificial intelligence in finance: Opportunities and challenges. https://towardsdatascience.com/artificial-intelligence-in-finance-opportunities-andchallenges-cee94f2f3858

Farrell, M., & Gallagher, R. (2015). The valuation implications of enterprise risk management maturity. *Journal of Risk and Insurance, 82*(3), 625-657.

Fernando, J. (2018). Artificial Intelligence in 3. the Banking Industry. Retrieved from https://www.cio.com/article/3239296/artificial-intelligence-in-the-banking-industry.html

Goodwins, R. (2001). The machine that wanted to be a mind. ZDNet news portal. Available from: http://news.zdnet.co.uk/story/0,,s2083911,00.html. (Accessed 24 June, 2024).

Holtel, S. (2016). Artificial Intelligence creates a wicked problem for enterprise. *Procedia Computer Science, 99, 171-180.*

Hong, K.S., Chi, Y.P., Chao L.R. & Tang J.-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security, 11 (5), 243-248.*

Ikegwuru, M., Jack, O.T., & Amadi, N.E., (2023). Artificial intelligence implementation and organizational performance of mainstream oil and gas companies in Nigeria. *International Academy Journal of Business Administration Annals, 9*(5), 91-106

ISO/IEC (2005). ISO/IEC 27002 – Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization/International Electrotechnical Commission.

ISO/IEC (2009). ISO/IEC 27000 – Information technology – Security techniques – Information security management systems – Overview and vocabulary. International Organization for Standardization/International Electrotechnical Commission.

Johnston, A. C. & Warkentin, M. (2010). Fear appeals and information security behaviors: An Empirical Study. *MIS Quarterly, 34 (3), 549-566.*

Kaplan, A. & Haenlein, M. (2018). Siri, Siri in my hand, who's the fairest in the land? On the interpretations, illustration and implications of Artificial Intelligence. Business Horizon, 62(1). Jump up to a-b.

Kee, C. (2001). Security policy roadmap – process for creating security policies. SANS Institute.

Kour, R., & Karim, R., (2020). Cybersecurity workforce in railway: its maturity and awareness. *Journal of Quality in Maintenance Engineering*, *27*(3), 453–464.

Kovacich, G.L. (1998). The information systems security officer's guide: Establishing and managing an information protection program. butterworth-heineman, Woburn.

Lucky, A. L., (2018). Marketing of Financial Service: Evidence from Nigeria Financial Market. *International Journal of Marketing Research Innovation 2(1), 31-46.*

Mahmoudzade, E., & Radrajabi, M. (2007). Security management in information systems. *Iranian Journal of Management Sciences, 1(4), 78-112.*

Maney, K. (2001). Artificial Intelligence isn't just a movie. USA Today. Available from: http://www.usatoday.com/news/acovwed.htm. (Accessed 24 June, 2024).

Manju, K. (2019). Artificial intelligence in finance. Understanding how automation and machine learning is transforming the financial industry. Masters Degree Thesis, Centria University of Applied Sciences, India.

Mantha, B. R. K., García de Soto, B., (2021). Assessment of the cybersecurity vulnerability of construction networks. *Engineering, Construction and Architectural Management*, *28*(10), 3078–3105.

Nekesa, M. & Olweny, T. (2018). Effect of financial innovation on financial performance: a case study of deposit-taking savings and credit cooperative societies in in Nigerian Banking Sector through engineering and technology-based channels. *International Journal of Civil Engineering and Technology, 10(1), 2156-2169.*

Nica, E., Potcovaru, A.-M. & Hurdubei Ionescu, R. E., (2019). Resilient cyber-physical systems and big data architectures in industry 4.0: Smart digital factories, automated production systems, and innovative sustainable business models. *Economics, Management, and Financial Markets, 14(2), 46–51.*

Nordlander, T.E. (2001). AI surveying: Artificial Intelligence in business. A thesis submitted to department of Management Science and Statistics, De Montfort University.

Odozi, V. C. (2023). Information security management and organizational efficiency in Deposit Money Banks in Nigeria. A thesis submitted to the postgraduate school, Rivers State University Nkpolu-Oroworukwo, Port Harcourt, in partial fulfillment of the requirements for the award of a doctor of philosophy (PhD) degree in office and information management.

Ogalo, O.J. (2012). The impact of information system security policies and controls on firms operation enhancement for Kenyan SMEs. *Prime Journal of Business Administration and Management (BAM), 2 (3).573-581*

Prentice, C., Dominique Lopes, S., & Wang, X. (2020). The impact of artificial intelligence and employee service quality on customer satisfaction and loyalty. *Journal of Hospitality Marketing & Management*, 1-18.

Russell, S, & Norvig, P (2016) *Artificial Intelligence*: A Modern Approach 3rd Edition Pearson

Russell, S. & Norvig, P. (2001) FAQ's for AI (WWW). Available from: http://www.doi.ic.ac.uk/project/2001/firstyeartopics/g01t28/faqs.html (Accessed 24 June, 2019).

Sabillon, R., Serra-Ruiz, J., Cavaller, V. & Cano, J. J. M., (2019). An effective cyber security training model to support an organizational awareness program: The Cyber security Awareness Training Model (CATRAM). A case study in Canada. *Journal of Cases on Information Technology*, *21*(3), 26–39.

.