ISSN: 6654 – 6750
Volume 10, Number 2, 2025
The Canada Journal of Entrepreneurship and Management

SECURITY AWARENESS AND INNOVATIVENESS IN COMMERCIAL BANKS IN RIVERS STATE

Eke, Josephine Onyeri (Ph.D)
Department of Office and Information Management, Faculty of Administration and Management, Ignatius Ajuru University of Education, Rumuolumeni, Port Harcourt. Rivers State, Nigeria

ABSTRACT

The study examined the relationship between security awareness and innovativeness in Commercial Banks in Rivers State. The study was anchored on information security Theory. The study adopted a cross-sectional survey research design. The accessible population of the study consisted of Three Hundred and Forty-Eight (348) office managers of Twenty-Four (24) commercial bank's headquarters operating in Rivers State. The sample size of the study was One Hundred and Eighty-Six (186) respondents of twenty-four (24) commercial banks in Rivers State. The above sample size was obtained using the Tao Yamene Sampling Formula. In order to address the differences in the distribution of the population across the firms, Bowley's 1960 Population Proportionate Allocation Formula was applied. Thus, the study adopted the random sampling techniques. A structured questionnaire was used as instrument for data collection after ascertaining its reliability through the employment of Test-retest Method. In line with the sample size, a total of One Hundred and Eighty-Six (186) copies of the validated questionnaire were distributed to the targeted audience through the help of two research assistants. The researchers were able to retrieve One Hundred and Fifty (150) copies of the entire validated questionnaire distributed. Arithmetic mean and standard deviation were used for the research question analyses, while the test of hypotheses was done using Spearman Rank Order Correlation with the aid of SPSS Version 25.0. Findings revealed that there is a significant positive relationship between security awareness and innovativeness in Commercial Banks in Rivers State. The study concluded that security correlates with innovativeness in Commercial Banks in Rivers State. When information assets are safeguarded, office managers are better positioned to coordinate resources, maintain accuracy in records, and supervise staff without the distraction of security breaches or data loss. The study recommended amongst others that management of Commercial banks should ensure robust **access control mechanisms** such as multi-factor authentication, role-based access permissions, and audit trails should be implemented to improve the accuracy, security, and reliability of records management.

Keywords: Security, Office Manager Performance, Access Control, Data Protection

INTRODUCTION

The final information security dimension is security awareness and training, which relates to the human factor in information protection. Human error remains one of the most common causes of security incidents in banks, often through phishing, weak passwords, or mishandling of confidential documents. Information managers are expected to support the development and implementation of structured training programs that improve employee understanding of security policies and responsible information practices. Studies reveal that targeted awareness programs significantly reduce the likelihood of breaches and improve compliance with security frameworks (Chanda, 2025; Afolabi & Okafor, 2023). In Nigerian banks, regular training, simulated phishing exercises, and role-based security instructions have been shown to foster a culture of accountability and vigilance among staff (Ibrahim & Mohammed, 2023). In Rivers State, information managers' performance is thus reflected in their ability to coordinate training schedules, monitor participation, and measure behavioral improvements such as reporting suspicious emails or reducing policy violations.

Research Hypothesis

Ho_1: There is no significant relationship between security awareness/training and innovativeness in Commercial Banks in Rivers State.

Security Awareness and Training

Security awareness and training encompass programs that educate bank staff about cybersecurity threats, secure practices, and organizational policies. In the banking sector, where human error remains a primary breach vector, such training is a core defense layer. Udo and Grace (2022) reveal that workshops combining phishing simulations and hands-on policy reviews significantly reduce phishing click-through rates among bank tellers. Eze, *et al.* (2023) conducted ethnographic research in northern Nigeria and found that regular security dialogues weekly briefs, scenario-based case studies, and manager-led discussions foster a security-conscious culture. Staff became more proactive in reporting suspicious activity, strengthening organizational resilience.

Security awareness and training refers to as the systematic programs and initiatives designed to educate and equip bank employees with the knowledge, skills, and attitudes required to recognize, prevent, and respond to information security threats. Ugwoke *et al.* (2024) noted that generic, annual training modules are quickly forgotten. In contrast, micro-learning platforms daily 5–7 minute quizzes or short videos-maintained engagement and awareness retention across bank branches. They argue that frequent, bite-sized refreshers are more suited to busy banking environments. Institutionalizing these programs falls to information or office managers, whose performance is measured by training coverage, frequency, and behavioral change rather than mere attendance. They must blend content with simulation, measure outcomes, and ensure learning translates into improved security behavior without overburdening staff.

In Rivers State's increasingly digital banking operations, awareness programs must adapt. As mobile banking and remote services proliferate, training must cover mobile phishing, app permissions, and secure customer interactions. Okafor and Ibe (2021) show that staff trained on secure chat and remote verification protocols reported fewer fraud incidents linked to new service offerings. Ultimately, embedding security awareness and training supports all facets of performance. It protects productivity by reducing disruptions caused by breaches, ensures accurate records by reducing accidental leaks, and enables innovation by equipping staff to safely adopt new technologies.

Innovativeness

Innovativeness within commercial banks refers to the adoption and adaptation of new processes, technologies, and products that differentiate service delivery and organizational agility. In Nigeria's banking sector, process innovation has been directly linked to organizational agility, as shown by Ekweli (2020), who found that banks which innovate their process systems enjoy greater decision speed and responsiveness pivotal capabilities for competing in dynamic markets. Adeyemo and Fatoki (2024) surveyed Nigerian Deposit Money Banks and reported that technologies such as real-time data analytics, machine learning, and blockchain significantly enhanced early fraud detection and prevention, indicating that innovativeness is not just about new products it must also serve institutional safety.

It refers to the ability and willingness of office manager in the banking institutions to develop, adopt, and implement new ideas, technologies, products, and processes that improve service delivery, operational efficiency, customer experience, and competitive advantage. Innovation also creates new managerial challenges and opportunities. In the Rivers State banking environment, information managers must not only support mobile banking, API services, and digital onboarding but also ensure these innovations are safe, compliant, and well-integrated. For instance, when First Bank of Nigeria deployed AI-powered chatbots and blockchain tools, it demonstrated how innovation can streamline customer service and risk management but success depended on managerial oversight

to embed these tools effectively (First Bank technology initiatives, 2023). Moreover, innovativeness directly contributes to customer-centric service. With Nigeria's progressing open banking framework, innovation enables banks to offer personalized experiences and seamless integrations. However, without strong governance, these new services could expose vulnerabilities. Thus, information managers' ability to foster innovation while overseeing its security implications becomes a key performance variable. In Rivers State, the nexus of innovativeness, productivity, and records management reflects how information managers orchestrate technical change to deliver value. Their role is to enable creativity in service design while ensuring that innovation does not erode trust, compliance, or operational coherence.

Empirical Review

Worlu and Adebayo (2025) studied identity and access management and the quality of work of information managers in Rivers State Banks. The design was correlational, and data were collected from 192 respondents in 11 commercial banks. Reliability tests showed alpha values above 0.85. Data were analyzed using regression analysis and structural modeling. Findings showed that stricter IAM practices reduced audit exceptions and improved the accuracy of access reviews. Privileged session recording and quarterly recertifications were the most significant contributors to improved performance. The study concluded that IAM rigor enhances the quality dimension of job performance and recommended that banks implement automated user provisioning, periodic recertifications, and comprehensive privileged access monitoring.

Okonkwo and Otobo (2024) examined security awareness, training intensity, and information managers' efficiency in Rivers State Commercial Banks. The purpose of this study was to investigate how security awareness programs and training intensity influence the efficiency and work quality of information managers in commercial banks in Rivers State. The study adopted a descriptive survey design. The population was drawn from information security and IT operations units in 12 banks, and 238 respondents were sampled proportionally. Validity was ensured by expert review and confirmatory factor analysis, while reliability was confirmed with Cronbach alpha scores above 0.88. Data were analyzed with regression analysis and structural modeling. Results indicated that training significantly improved awareness, and awareness in turn positively affected efficiency and quality of work. Banks that implemented phishing simulations and role-specific training achieved quicker incident responses and cleaner system records. The study concluded that continuous training drives awareness and enhances performance. It recommended that banks implement quarterly role-specific training, adopt micro-learning techniques, and monitor the relationship between training and performance outcomes.

Adeyemi and Briggs (2024) studied information security policy governance and information managers' job performance in Commercial Banks in Rivers State. The aim was to determine how policy clarity, executive sponsorship, and enforcement mechanisms affect efficiency, quality of work, and compliance delivery among managers. The research adopted a cross-sectional survey design with a population consisting of information managers, IT security leads, and compliance officers from licensed commercial banks operating in Rivers State. A sample of 210 respondents was drawn from 14 banks using stratified random sampling. Data were collected with a structured questionnaire. Content validity was ensured through expert review, while construct validity was established using factor analysis. Reliability coefficients were all above 0.85. Data analysis was carried out using structural equation modeling and regression analysis. Findings showed that effective policy governance had a significant positive impact on the efficiency and quality of work of information managers. Banks that had board-approved policies and consistent enforcement experienced better audit outcomes and quicker task delivery. The study concluded that policy governance strengthens job performance and recommended that banks regularly review their security policies, link enforcement to performance evaluations, and ensure management sponsorship of information security.

Research Design
The cross sectional explanatory survey research design was adopted for the study. This research design was deemed suitable and most appropriate for the study because of two reasons: (i) the study was conducted across different Commercial Banks in Rivers State at the same time which makes it a survey study; (ii) it involves the test of hypotheses which is explanatory in nature.

Research Population
The accessible population of the study consisted of Three Hundred and Forty-Eight (348) office managers (customer service officer and system officers) of Twenty-Four (24) commercial bank's headquarters operating in Rivers State. The information was obtained from Human Resource Department of the Twenty-Four (24) commercial bank's headquarter situated in Port Harcourt understudy.

Sample and Sampling Technique
The sample size of the study was One Hundred and Eighty-Six (186) respondents of twenty-four (24) commercial banks in Rivers State. The above sample size was obtained using the Taro Yamene Sampling Formula.

Instrumentation and Measurement
Structured questionnaire was used as instrument for data collection. The structured questionnaire was developed by the researcher. The research instrument was called "Information Security and Office Manager's Job Performance Index" (ISOMJPI). The instrument was made up of two sections. Section A was designed to elicit demographic data concerning the respondents. Section B contained the main questionnaire items designed to measure the variables under investigation. The instrument was designed in a modified four (4) point likert scale with the following response options: Strongly Agreed (SA) =4; Agreed (A) = 3; Disagreed (D) = 2; and Strongly Disagreed (SD) = 1.

Administration of the Instrument
In line with the sample size, a total of One Hundred and Eighty-Six (186) copies of the validated questionnaire were distributed to the targeted audience through the help of two research assistants. The researchers were able to retrieve One Hundred and Fifty (150) copies of the entire validated questionnaire distributed.

Method of Data Analysis
Arithmetic mean and standard deviation were used for the research question analyses, while the test of hypotheses was done using Spearman Rank Order Correlation with the aid of SPSS Version 25.0. Spearman Rank Order Correlation Coefficient was computed.

Test of Hypothesis
Ho_1: There is no significant relationship between security awareness/training and innovativeness in Commercial Banks in Rivers State.

Table 1: Correlations between Security Awareness/Training and Innovativeness

			Security Awareness and Training	Innovativeness
Spearman's rho	Security Awareness and Training	Correlation Coefficient	1.000	.650**
		Sig. (2-tailed)	.	.000
		N	150	150
	Innovativeness	Correlation Coefficient	.650**	1.000
		Sig. (2-tailed)	.000	.
		N	150	150

**. Correlation is significant at the 0.05 level (2-tailed).

Source: Survey Data, 2025.

Table 1 above showed r value of 0.650 at significance value of 0.00 which is less than the chosen alpha level of 0.05 for the hypothesis relating security awareness/training and innovativeness. Since the significant value is less than the alpha level of 0.05, the null hypothesis (Ho_3) which states that there is no significant relationship between security awareness/training and innovativeness in Commercial Banks in Rivers State was rejected and the alternative hypothesis (Ha_1) was accepted. This implies that there is a moderate positive relationship between security awareness/training and innovativeness in Commercial Banks in Rivers State.

Relationship between Security Awareness/Training and Innovativeness

The test of hypothesis three revealed that there is a moderate positive relationship between security awareness/training and innovativeness in Commercial Banks in Rivers State. In commercial banks across Rivers State, security awareness and training have become more than just routine compliance activities they are quietly shaping how banks innovate. With the rise of mobile banking, agency networks, and digital transactions, cyber threats have become a daily reality. Employees who lack basic security awareness often hesitate to try new approaches, fearing mistakes that could expose the bank. When banks invest in continuous security training, however, staff gain confidence to experiment within safe boundaries, and this directly boosts innovativeness. Research shows that well-structured security awareness programmes significantly improve employee behaviour, reducing vulnerabilities such as phishing and social engineering attacks (Parsons *et al.,* 2017). In practice, this means fewer disruptions and more freedom for employees to focus on creative problem-solving and new product development.

The link between awareness and innovation is especially relevant in Rivers State. Studies on deposit money banks in Nigeria confirm that employee innovativeness strongly drives productivity and competitive performance (Okorie & Chinedu, 2022). By embedding security training into this process, banks create an environment where innovative ideas can move more smoothly from design to implementation without being derailed by compliance failures. A recent study on Nigerian banks also highlights that organisational support for security training not only reduces fraud incidents but also strengthens collaboration across departments, which is crucial for innovation (Adebayo & Omilusi, 2022). Customers also feel the difference. When frontline staff are well-trained in security practices, they communicate confidence to clients, encouraging greater adoption of digital services. This is important because trust is a major factor in whether customers embrace new innovations such as mobile transfers or agency banking platforms. Evidence from the Nigerian financial sector shows that improved cybersecurity readiness leads to stronger digital service adoption and better performance outcomes (Garcia & Vargas, 2021).

CONCLUSION

Based on the results and discussion of findings, the study concluded that information security correlate with office manager's job performance of Commercial Banks in Rivers State. When information assets are safeguarded, office managers are better positioned to coordinate resources, maintain accuracy in records, and supervise staff without the distraction of security breaches or data loss. Conversely, weak security practices expose office managers to risks that compromise efficiency, accountability, and service quality.

RECOMMENDATIONS

Based on the findings, the following recommendations were made:

1. Management of Commercial banks should strengthen data protection frameworks through encryption, secure backups, and NDPR compliance to safeguard information, reduce system downtimes, and enhance employee productivity.

2. Management of Commercial banks should ensure robust access control mechanisms such as multi-factor authentication, role-based access permissions, and audit trails should be implemented to improve the accuracy, security, and reliability of records management.
3. Management of Commercial banks should ensure continuous security awareness and training programs that institutionalized, using role-specific and scenario-based modules tailored to the threat environment in Rivers State.

REFERENCES

Adeyemi, T., & Briggs, F. (2024). Information security policy governance and information managers' job performance in commercial banks in Rivers State. *Journal of Information Security and Banking Studies*, *12*(3), 44–59.

Afolabi, J., & Okafor, C. (2023). Cybersecurity awareness and employee compliance in Nigerian financial institutions. *African Journal of Information Systems, 15*(1), 101–118.

Chanda, R. C. (2025). *Assessing cybersecurity awareness among bank employees in developing countries*. https://doi.org/10.1016/j.cose.2025.103458

Eze, C., Nnaji, P., & Akpan, I. (2023). Building a culture of information security in Nigerian banks: An ethnographic approach. *International Journal of Information Management, 69*, 102578.

Federal Republic of Nigeria. (2023). *Nigeria Data Protection Act 2023*. Government Printer.

Garcia, J., & Vargas, M. (2021). Cybersecurity readiness and digital innovation adoption in financial services: Evidence from emerging economies. *Journal of Financial Innovation, 7*(2), 85–104.

Ibrahim, S., & Mohammed, K. (2023). Security awareness and organizational resilience in Nigerian banks. *Journal of African Business, 24*(2), 231–248.

International Organization for Standardization. (2022). *Information security management systems — Requirements*. Geneva: International Organization for Standardization

Okafor, N., & Ibe, C. (2021). Security awareness for mobile banking staff: Evidence from selected banks in Nigeria. *Journal of African Business, 22*(4), 512–530.

Onunwor, A. A. (2022). Record management practice and organizational performance of Access Bank Plc, Rivers State. *International Journal of Academic Research in Business and Social Sciences, 12*(6), 101–115.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176.

RSIS International. (2025). Impact of artificial intelligence on effective document management in the banking sector in Nigeria. *International Journal of Research and Innovation in Social Science, 9*(2), 143–153.

S&P Global Ratings. (2025). *Nigerian banking outlook 2025*. S&P Global Market Intelligence Reports.