

DATA PROTECTION AND PRODUCTIVITY 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 data protection and productivity 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 Taro Yamene Sampling Formula. A structured questionnaire was used as instrument for data collection. The test of hypothesis 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 data protection and productivity in Commercial Banks in Rivers State. The study concluded that data protection and productivity in Commercial Banks in Rivers State. 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: *Data Protection, Protection, Access Control*

INTRODUCTION

The banking industry operates under strict regulatory frameworks that require accurate documentation and traceability of all financial transactions. Records form the foundation for audit readiness, dispute resolution, credit assessments, and compliance with supervisory authorities. Poorly managed records expose banks to litigation risks, regulatory penalties, and erosion of customer trust. Conversely, effective records management practices ensure transparency, enhance institutional memory, and safeguard the integrity of customer and organizational information. In recent years, Nigerian banks have increasingly adopted electronic records management systems to replace traditional paper-based filing, with studies showing that such digital approaches reduce operational delays and improve accountability (Onunwor, 2022; RSIS International, 2025). Motlhasedi (2024) further emphasizes that digital records systems contribute significantly to performance by improving retrieval accuracy, reducing storage costs, and facilitating compliance with retention schedules. For banks in Rivers State, where branch operations and electronic service delivery coexist, the performance of information managers is clearly observable in the way they coordinate records systems that balance accessibility with compliance and security.

Innovativeness reflects the ability of information managers to facilitate new ways of using information to enhance banking operations. In an era where Nigerian banks face intense competition from fintech firms and the growing expectations of digitally savvy customers, innovation has become a critical survival strategy. Information managers contribute to this by ensuring that data is not only preserved and protected but also harnessed as a tool for generating insights, supporting product development, and enabling process automation. Scholars note that banks that effectively leverage information assets for innovative purposes tend to perform better in terms of service delivery and competitive positioning (Adebayo & Omilusi, 2022; S&P Global Ratings, 2025). In Rivers State, this implies that information managers must go beyond routine information handling to actively support

digital transformation initiatives, ranging from mobile banking innovations to artificial intelligence-driven customer analytics. Their innovativeness, therefore, lies in enabling banks to transform information into actionable intelligence while ensuring that such practices remain aligned with ethical and regulatory standards.

Research Hypothesis

H₀₁: There is no significant relationship between data protection and productivity in Commercial Banks in Rivers State.

Data Protection

Data protection in commercial banking embodies the safeguards both technical and procedural that guard customer and institutional information from unauthorized disclosure, alteration, or loss. In contemporary digital banking, especially within Rivers State, the volume and sensitivity of stored information have surged, making structured data protection mechanisms indispensable. Uche and Ebere (2021) argue that when banks implement end-to-end encryption and strong data lifecycle management, they foster customer trust and reduce risk exposure. In many Nigerian commercial banks, including those in Rivers State, data protection practices now integrate privacy-by-design principles within core banking systems. Onyeka and Nwosu (2022) demonstrate how encrypted storage and anonymization protocols, when embedded within transaction processing systems, reduce breach consequences and improve regulatory compliance. Their study highlights that embedding encryption at the data-at-rest and data-in-transit stages strengthens resilience against interception and leakage.

Operationally, data protection is the legal, technical, and organizational measures put in place to ensure that customer and institutional data collected, processed, stored, and transmitted by banks are safeguarded against unauthorized access. Asoegwu and Nnadi (2023) examined several Nigerian banks' customer retention rates, finding that institutions with robust data protection standards enjoy higher loyalty metrics. Their qualitative interviews reveal that customers associate encryption, secure portals, and limited data retention with professionalism and reliability. The repercussions of weak data protection are tangible. Ekemini *et al.* (2024) recount an incident in a regional Nigerian bank where a poorly secured backup server led to a partial data leak. Apart from regulatory scrutiny, the episode triggered a loss of correspondent banking relationships and public trust, underscoring the real-world stakes of data handling lapses. In Rivers State's commercial banking landscape, where digital adoption is accelerating but oversight mechanisms vary across branches, data protection must be both standardized and enforced. Beyond safeguarding customer data, its significance extends to enabling smooth operations; data leaks disrupt productivity and compromise records integrity and innovation cycles.

Productivity

Productivity in the context of commercial banks embraces how effectively information and processes are organized to deliver timely, cost-effective banking services. In Rivers State, such productivity is often tied to the adoption of information and communication technologies (ICT) that automate routine tasks and reduce turnaround time. For example, Suleiman, Asimiyu *et al.* (2021) found that the implementation of integrated banking applications significantly improved staff efficiency and customer service speed across Nigerian banks, demonstrating the critical link between ICT and productivity in banking operations.

Moreover, productivity gains in banking extend beyond technology to the behavior of knowledge workers such as information managers whose lived experiences shape service outcomes. Olekanma (2022) used qualitative interviews with Nigerian bank executives to reveal how managerial indifference and micromanagement undermine productivity; productive information managers are those who motivate staff and reduce unnecessary oversight, enabling faster and more reliable service delivery. Ekpudu *et al.* (2020) studied the role of enterprise resource planning (ERP) in

Nigerian banks, noting that ERP implementations enhanced productivity by integrating human resource planning and quality control into banking processes, thereby enabling smoother coordination between branches, human resources, and operations management.

In Rivers State, productivity also depends on how office managers manage records and information flow. When records systems are reliable and accessible, managers can make decisions faster and resolve customer inquiries promptly. The absence of such systems such as outdated filing or fragmented communication introduces delays that degrade productivity and frustrate customers. Thus, for Rivers State commercial banks, productivity is multidimensional: it derives from technology (ICT, ERP), from human motivation (management style), and from integrated information systems (records accessibility), all of which information managers mediate through their daily decisions and oversight.

Theoretical Review

The study was anchored on Information Security Theory. Information Security Theory was founded by von Solms 1998. It emphasizes that information security is not only a technical issue but a **management responsibility** that must be systematically integrated into organizational processes. It argues that information security should follow a continuous cycle of **risk assessment, policy implementation, monitoring, and improvement**, where both technology and people play critical roles.

The study was built on the following core assumptions:

- i. Information security is not purely a technical issue but an organizational management process that requires clear structures, policies, and governance.
- ii. Security is guided by the principles of Confidentiality, Integrity, and Availability (CIA), which together ensure that information is protected against unauthorized access, modification, and disruption.
- iii. Effective information security is achieved through a systematic cycle of risk assessment, policy implementation, training, monitoring, and continuous improvement.
- iv. Responsibility for security is shared across the organization, with information managers playing a central coordinating role.
- v. Without a well-structured information security management system, organizations are vulnerable not only to technological risks but also to human errors, fraud, and regulatory non-compliance.

This theory is relevant to the study of information security and office managers' job performance in commercial banks in Rivers State because it directly links managerial responsibilities to the effectiveness of security outcomes. Information managers in banks are not only tasked with routine functions such as productivity, records management, and innovativeness, but also with ensuring that these functions are performed within the secure boundaries of data protection and regulatory compliance.

For example, in managing productivity, office managers must ensure that workflows are not disrupted by cyberattacks or unauthorized access. In records management, they are expected to maintain the integrity and confidentiality of customer data in line with ISO standards and banking regulations. For innovativeness, managers are challenged to integrate new technologies, such as digital banking platforms, while embedding security measures from the design stage. The ISMT provides a strong lens to examine these issues because it emphasizes that information security must be institutionalized rather than treated as an add-on. In the banking sector in Rivers State where cybercrime, insider threats, and compliance with the Central Bank of Nigeria's ICT/security regulations are critical adopting ISMT highlights that office managers' job performance cannot be evaluated without considering their ability to implement and sustain robust information security practices such as data protection, access control, and staff security training.

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 Hypotheses

Ho₁: There is no significant relationship between data protection and productivity in Commercial Banks in Rivers State.

Table 1Correlations between Data Protection and Productivity

		Data Protection	Productivity
Spearman's rho	Data Protection	Correlation Coefficient	1.000
		Sig. (2-tailed)	.610**
		N	.000
	Productivity	Correlation Coefficient	150
		Sig. (2-tailed)	.610**
		N	.000
		150	1.000
			.000
			150
			150

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

Source: Survey Data, 2025.

Table 1 above showed r value of 0.610 at a significance level of 0.00 which is less than the chosen alpha level of 0.05 for the hypothesis relating data protection and productivity. Since the significance value is less than the alpha level of 0.05, the null hypothesis (H_{01}) which states that there is no significant relationship between data protection and productivity in Commercial Banks in Rivers State was rejected and the alternate hypothesis (H_{a1}) was accepted. This implies that there is a strong positive relationship between data protection and productivity in Commercial Banks in Rivers State.

Relationship between Data Protection and Productivity

The test of hypothesis one revealed that there is a strong positive relationship between data protection and productivity in Commercial Banks in Rivers State. Data protection, broadly defined as the practice of safeguarding sensitive information from unauthorized access, corruption, or loss (Uche & Ebere, 2021), goes beyond compliance to become a performance enabler in the banking sector. When data is secured through encryption, controlled access, and lifecycle management, managers and employees can work with greater confidence, thereby minimizing downtime associated with breaches or system failures. This creates an environment where productivity flourishes because workflows are not disrupted by avoidable data incidents. In Rivers State, where commercial banks operate in a highly competitive and digitalized environment, productivity is tightly linked to the integrity and availability of information. Onyeka and Nwosu (2022) argue that embedding privacy-by-design mechanisms into banking systems improves transaction efficiency because staff spend less time resolving customer complaints related to data errors or leaks. This efficiency is particularly critical in busy metropolitan areas such as Port Harcourt, where large volumes of transactions occur daily. When data protection systems are strong, operational bottlenecks are reduced, allowing managers to focus on service delivery rather than crisis management.

Asoegwu and Nnadi (2023) found that Nigerian banks that prioritize customer data confidentiality enjoy smoother operations because customers are more willing to adopt digital channels, reducing pressure on physical branches. In Rivers State, where internet and mobile banking are increasingly popular, effective data protection encourages customers to transact digitally, which not only increases throughput but also frees up employees for higher-value tasks. This shift in workload allocation translates into measurable productivity gains at the organizational level. According to Ekemini, *et al.* (2024), banks that invest in robust data protection frameworks avoid regulatory penalties and reputational damage that often divert resources away from core operations. By proactively aligning with legal standards, commercial banks in Rivers State save time and financial resources, enabling managers to channel their efforts toward innovation and customer engagement instead of crisis-driven responses. Nweke, *et al.* (2023) showed that implementing structured privilege management systems in Nigerian banks reduced internal misuse and created smoother information flows between departments. In the context of Rivers State, where employees handle high volumes of sensitive financial information daily, reduced risks of misuse and mismanagement ensure uninterrupted workflows, thereby maximizing job performance for office managers and staff.

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

- Adebayo, T., & Omilusi, M. (2022). Cybersecurity awareness and organisational collaboration in Nigerian banks: Implications for performance and innovation. *African Journal of Business Management*, 16(5), 134–145.
- Asoegwu, C., & Nnadi, I. (2023). Data protection practices and customer retention in Nigerian banking institutions. *Journal of African Business*, 24(3), 291–309.
- Ekemini, E., Udoh, J., & Nkereuwem, A. (2024). Data leakages and resilience strategies in Nigerian commercial banks. *Information and Computer Security*, 32(2), 198–214.
- Ekpudu, J. E., Omoera, C. I., & Ogunleye, O. J. (2020). Enterprise resource planning and organisational performance in the Nigerian banking industry. *Global Journal of Accounting*, 4(3), 37-39
- Nweke, G., Okpara, C., & Bello, S. (2023). Privilege management and insider misuse in Nigerian commercial banks. *Information Resources Management Journal*, 36(4), 55–72.
- 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.
- Onyeka, U., & Nwosu, J. (2022). Embedding privacy-by-design in Nigerian banking systems: A case of transaction security. *African Journal of Science, Technology, Innovation and Development*, 14(6), 1462–1472. <https://doi.org/10.1080/20421338.2021.1903409>
- Onyeka, U., & Nwosu, J. (2022). Embedding privacy-by-design in Nigerian banking systems: A case of transaction security. *African Journal of Science, Technology, Innovation and Development*, 14(6), 1462–1472.
- S&P Global Ratings. (2025). *Nigerian banking outlook 2025*. S&P Global Market Intelligence Reports.
- Uche, C., & Ebere, M. (2021). Encryption and data lifecycle management in Nigerian banks. *Journal of Information Privacy and Security*, 17(4), 231–247.