DIGITALIZING INFOR-SECURITY POSTURE: AN ANALYSIS OF INFOR-SECURITY ARCHITECTURE AND INFOR-PROTECTION LAW OF COMMERCIAL BANKS IN RIVERS STATE, NIGERIA.

Julian Nwaonumah Julian ,Oke
Department of Office technology and Management Education
Federal College Of Educaion (TECH) Omoku, Rivers State, Nigeria.
nwaajulie@gmail.com;
07032472901

Dr. Erien-naikachep Maurice ,Ikuru
Department of Office and Information Management
Ignatius Ajuru University of Education, Rumuolumeni Port Harcourt, Nigeria.
mauriceikuru95@gmail.com;
08064345396
&
Kora Francis ,Atandikiari
Doctoral Student, Department of Office and Information Management
Ignatius Ajuru University of Education, Rumuolumeni, Port Harcourt, Nigeria.
atandikiarikora@gmail.com;
08033261361

ABSTRACT

This study on Digitalizing Infor-Security Posture: An Analysis of Information Security Architecture, and Information Protection Law of Commercial Banks in Rivers State, Nigeria investigate and analyze information security architecture, information protection law of Commercial Banks in Rivers State. Generally, the objective of the study was to empirically examine how information security architecture and information protection law of Commercial Banks in Rivers State aligned with the digitalization of information security posture drawing its indicies such as, incedent reponse and management, cyptography and scalability on one side while personal data protection, data breach and cross border data trasnsfer on the other side. The study adopted explanatory survey research design. The population of the study consisted of two hundred and thirty (230) top managers from twenty-three (23) Commercial Banks operating in Rivers State, Nigeria, as top 10 managers were chosen from each bank. By census study, the entire population was employed as the sample size of the study. The reliability of the instrument was ascertained using Crombach Alpha with the least coefficient up to 0.743. Out of 230 copies of the questionnaire distributed, 220 copies of the questionnaires were retrieved. The data obtained from the field were analyzed using Spearman's Rank Order Correlation Coefficient and t-test with the aid of SPSS Version 22.0. Three hypotheses were tested using Spearman Rank Order Correlation. The study found that infor-security architecture with its selected indicies: incidences response & management, cryptography and scalability. On the other hand infor- proctection law with the selected incidicies such as: personal data protection, data breach notification and cross border data transfer has significant positive relationship with operational efficiency and competitive advantage of Commercial Banks in Rivers State. The study concludes that the digitalization of information security in commercial banks not only fortifies their defenses against cyber threats but also drives operational efficiencies and fosters a competitive edge. The study recommended amongst other things that banks should develop and regularly update incident response plans that detail specific steps for identifying, mitigating, and recovering from security incidents.

Keywords: *Information Security Architecture, incident response & management, Cryptography, scalability Information Protection Law, personal data protection, Data breach notification and cross border data transfer*

INTRODUCTION

In the rapidly evolving digital landscape, the importance of robust information security measures cannot be overstated. Commercial banks, as custodians of sensitive financial data, are particularly vulnerable to cyber threats and data breaches. This vulnerability necessitates a comprehensive approach to information security that encompasses both legislative frameworks and technical architectures. Information protection laws serve as the legal backbone for securing sensitive data against unauthorized access, misuse, and breaches. In Nigeria, the legal framework for data protection, including the Nigeria Data Protection Regulation (NDPR) and other relevant laws, plays a crucial role in safeguarding sensitive information held by organizations, particularly

commercial banks (Anifalaje, 2024). These regulations emphasize the responsibilities of entities in securing personal data, upholding privacy rights, and implementing robust security measures to prevent unauthorized access and breaches. Compliance with these laws is paramount for commercial banks in Rivers State to avoid severe legal consequences, financial penalties, and reputational harm that may arise from non-compliance, highlighting the significance of stringent data protection practices within the banking sector. The enforcement of information protection laws is essential not only for regulatory adherence but also for maintaining trust with customers and protecting against potential data vulnerabilities that could lead to exploitation for corrupt purposes (Gulyamov&Raimberdiyev, 2023).

The NDPR, introduced in 2019, provides a comprehensive framework for data protection in Nigeria. It outlines the rights of data subjects, the obligations of data controllers and processors, and the penalties for data breaches. Commercial banks must adhere to the Nigerian Data Protection Regulation (NDPR) by implementing measures like data encryption, secure data storage, access controls, and regular security audits to safeguard sensitive information. Furthermore, the Cybercrimes (Prohibition, Prevention, Etc.) Act of 2015 is crucial in protecting information systems and critical infrastructure from cyber threats, emphasizing the importance of cyber resilience in the financial sector (Crisanto&Prenio, 2021). Studies highlight the significance of cybersecurity in banking, with a focus on governance strategies, human resources, and risk management to ensure a robust cybersecurity framework. Cognitive models have been developed to assess the level of protection of computer networks and critical infrastructure, aiding in predicting cybersecurity states and implementing necessary preventive mechanisms. Efforts to mitigate cybercrimes in banks involve public awareness, budget allocation, management support, and skilled personnel to enhance cybersecurity measures (Mwita&Mhina, 2023).This legislation criminalizes various cyber offenses, thereby providing a legal deterrent against cybercrimes targeting financial institutions. While legal frameworks establish the foundation for information protection, the implementation of a robust information security architecture is essential for translating these laws into practice. This study measured information protection law with personal data protection, data breach notification and cross border data transfer.

In the contemporary digital era, the protection of personal data has become a critical concern for organizations, particularly in the financial sector. Personal data protection refers to the practices and policies implemented to safeguard individuals' personal information from unauthorized access, use, or disclosure. This includes data encryption, secure storage, and access controls designed to ensure the confidentiality, integrity, and availability of personal data. A data breach, defined as any unauthorized access to, or disclosure of, personal data, poses significant risks, including financial loss, reputational damage, and regulatory penalties.

Data breach notification is a regulatory requirement mandating organizations to inform affected individuals and relevant authorities about a data breach within a specified timeframe. This practice is essential for mitigating the impact of breaches by enabling individuals to take protective measures and allowing regulatory bodies to enforce compliance and penalties where necessary. Timely notification fosters transparency and accountability, which are crucial in maintaining trust between organizations and their customers.

Cross-border data transfer involves the movement of personal data across national boundaries. This process is particularly relevant in the globalized financial sector, where banks often operate in multiple jurisdictions. Such transfers must comply with international data protection standards and the regulatory requirements of both the originating and receiving countries to ensure that personal data remains secure

and privacy rights are upheld. Regulatory frameworks like the General Data Protection Regulation (GDPR) in the European Union set stringent guidelines for cross-border data transfers, including adequacy decisions, standard contractual clauses, and binding corporate rules.

In Rivers State, the legal landscape concerning personal data protection, data breach notification, and cross-border data transfer is primarily shaped by the Nigeria Data Protection Regulation (NDPR) and the Cybercrimes (Prohibition, Prevention, Etc.) Act of 2015. These regulations mandate commercial banks to implement robust data protection measures, promptly notify stakeholders of any data breaches, and

ensure compliance with international data transfer standards (Ikram, 2024). Adhering to these laws is crucial for upholding the integrity and security of personal data, thereby safeguarding customers' privacy and fostering trust in the banking sector. Commercial banks in Rivers State must navigate these regulatory requirements while implementing comprehensive information security architectures. By integrating stringent data protection measures, effective breach notification protocols, and secure cross-border data transfer practices, banks can not only mitigate legal risks but also enhance their overall security posture, ensuring regulatory compliance and maintaining customer trust in the digital age.

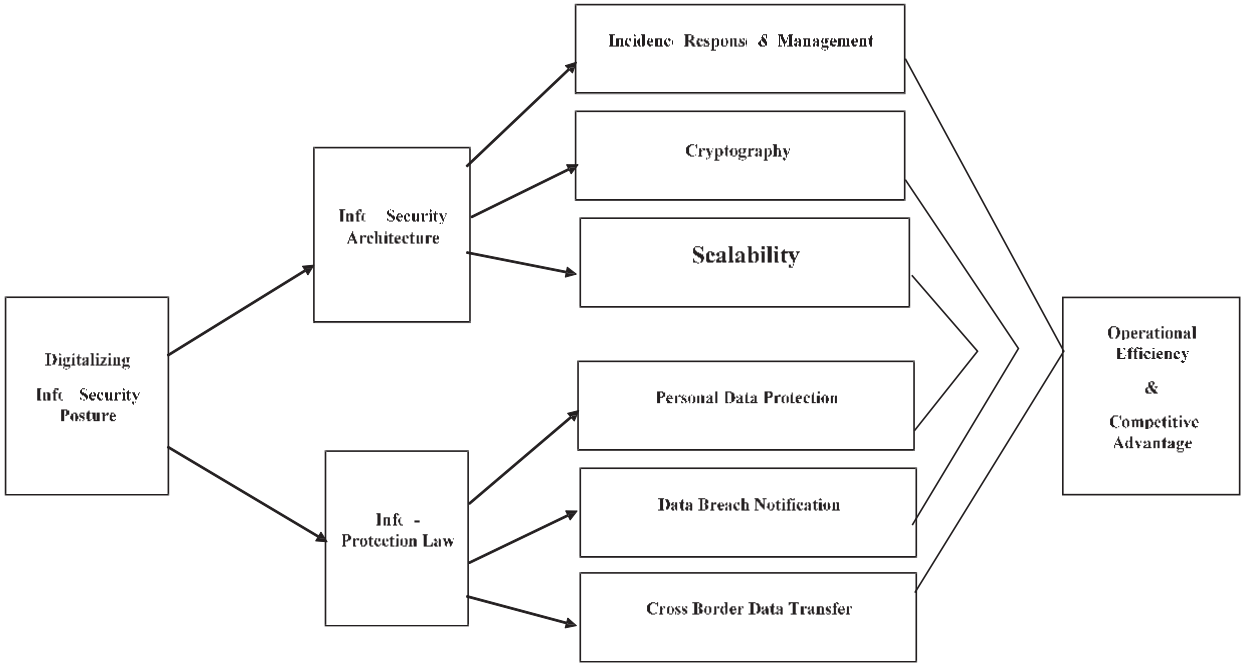
Information security architecture encompasses the structural design and deployment of security controls to protect information assets from threats. It involves a multi-layered approach that includes network security, application security, data security, and endpoint security. In commercial banks, information security architecture plays a crucial role in safeguarding against various cyber threats such as malware attacks, phishing, insider threats, and data breaches. Key components of this architecture, as highlighted across the provided research papers, include the integration of Artificial Intelligence (AI) for proactive threat detection and analysis, the implementation of firewalls and intrusion detection systems to counter advanced cyber threats, the emphasis on identity and access management, data encryption, and secure authentication to mitigate insider threats, the utilization of information protection systems to enhance financial security and combat cybercrime, and the focus on user identification, authentication, and authorization to prevent unauthorized access and ensure data integrity (Soesanto et al., 2023). By incorporating these components into their security frameworks, commercial banks can bolster their defenses and protect sensitive financial data from evolving cyber risks. These components work in concert to create a resilient security posture that can detect, respond to, and mitigate security incidents effectively. Moreover, the adoption of international standards such as ISO/IEC 27001, which provides a systematic approach to managing sensitive information, helps banks in Rivers State align their security practices with global best practices. This alignment not only enhances the security of their information systems but also boosts customer confidence and trust. As such, the study dimentionalize Information security architecture with, incident response and management, Cryptography and scalability.

In the contemporary digital realm, commercial banks encounter a myriad of cybersecurity challenges that demand resilient incident response and management, robust cryptography solutions, and scalable strategies within their information security framework (Oyewole et al., 2024). Incident response and management refer to the systematic approach organizations use to address and manage the aftermath of a security breach or cyberattack. This involves identifying, containing, eradicating, and recovering from security incidents while minimizing damage and reducing recovery time and costs. Effective incident response plans play a crucial role in maintaining operational continuity and safeguarding sensitive financial data. Incident response is pivotal in managing security breaches, ensuring business continuity, and protecting valuable personal and financial information in fintech organizations (Jangampeta, 2022). Cryptography, the practice of securing information by transforming it into an unreadable format using algorithms, is a cornerstone of information security. It ensures that sensitive data remains confidential and secure during transmission and storage. Techniques such as encryption, digital signatures, and hashing are employed to protect data integrity and authenticity. In the banking sector, cryptography is crucial for safeguarding customer information, transaction data, and proprietary banking systems against unauthorized access and cyber threats.

Scalability in information security architecture refers to the capability of a system to handle increasing amounts of data or users without compromising performance or security. As commercial banks in Rivers State continue to grow and adopt new technologies, their security systems must be scalable to accommodate expanding operations and evolving cybersecurity threats. Scalable security architectures ensure that banks can maintain robust security measures even as they scale their services and infrastructure to meet market demands.In the context of commercial banks in Rivers State, integrating incident response and management, cryptography, and scalability into their information security architecture is crucial (Farayola, 2024). By implementing incident response plans, banks can effectively address security breaches, reducing potential damage and regulatory penalties. Utilizing cryptographic

measures ensures the confidentiality and integrity of financial data, enhancing customer trust and compliance with data protection laws. Moreover, scalability allows banks to expand their digital services and infrastructure while maintaining robust security measures, especially as they adopt cloud services and mobile banking innovations. Implementing scalable security solutions, such as modular frameworks and automated threat detection systems, enables banks to adapt to evolving security requirements and technological advancements, ultimately enhancing their cybersecurity posture, aligning with regulatory mandates, and supporting sustainable growth in the digital era (Anifalaje, 2024).

Conceptualizing framework showing Digitalizing Infor-Security Posture: An Analysis of Infor-Security Architecture and Infor-Protection Law of Commercial Banks In Rivers State Nigeria.



Aim and Objectives of the Study

The aim of the study was to examine the relationship between Infor-Security Architecture and Infor-Protection Law of Commercial Banks in Rivers State. The specific objectives of the study include the following:

1. To ascertain the relationship between infor-security architecture and operational efficiency of Banks in Rivers State.
2. To determine the relationship between infor-security architecture and competitive advantage of Commercial Banks in Rivers State.
3. To examine the relationship between infor-protection law and operational efficiency of Commercial Banks in Rivers State.
4. To determine the relationship between infor-protection law and competitive advantage of Commercial Banks in Rivers State.

Concept of Digitalizing Infor-Security Posture

In today's digital age, the significance of information security has escalated, especially within financial institutions such as commercial banks. The integration of digital technologies into banking operations necessitates a robust information security posture to safeguard sensitive data and maintain trust with clients. This transformation is particularly pertinent in regions like Rivers State, where the banking sector plays a crucial role in the local economy. Digitalizing an information security posture involves implementing advanced digital tools and strategies to protect information systems from cyber threats (Igwenagu et al., 2024).

Information security architecture refers to the structural design of an organization's security framework, encompassing policies, procedures, and technical measures to prevent unauthorized access, data breaches, and cyber-attacks. Information protection laws, on the other hand, are legal frameworks designed to ensure the

confidentiality, integrity, and availability of data by setting standards and regulations for handling sensitive information.

The financial sector, including commercial banks in Rivers State, faces unique challenges in information security due to the high value of the data they handle and the increasingly sophisticated nature of cyber threats. These banks must navigate a complex landscape of regulatory requirements and technological advancements to maintain their information security posture. Digitalizing this posture involves adopting cutting-edge technologies such as artificial intelligence, machine learning, and blockchain to enhance security measures (Farayola, 2024). For instance, AI and machine learning can detect and respond to threats in real-time, while blockchain provides a tamper-proof ledger for secure transactions. In Rivers State, commercial banks have made strides in digitalizing their information security architecture by investing in secure infrastructure, training personnel, and complying with both local and international information protection laws. These efforts are crucial for maintaining the integrity of financial transactions and protecting customer data from breaches. However, the rapid pace of technological change requires continuous adaptation and vigilance. Banks must regularly update their security protocols and invest in ongoing staff training to keep pace with evolving threats (Farayola, 2024).
Moreover, the role of government and regulatory bodies in shaping the information security landscape cannot be overstated. In Rivers State, initiatives to strengthen information protection laws and enforce compliance among financial institutions are essential. Collaboration between banks, government agencies, and cybersecurity experts can foster a more resilient banking sector capable of withstanding cyber threats. The digitalization of information security posture in commercial banks is not just a technological upgrade; it represents a strategic shift towards proactive risk management and robust regulatory compliance. By leveraging advanced technologies and adhering to stringent legal frameworks, commercial banks in Rivers State can enhance their security posture, thereby protecting their assets and customers' trust. This transformation is pivotal in ensuring the long-term sustainability and competitiveness of the banking sector in an increasingly digital world (Adeyemo&Obafemi, 2024).

Infor-Security Architecture

In the modern digital landscape, information security architecture has become crucial for organizations, especially in the financial sector, where sensitive data is highly targeted by cyber threats. Information security architecture refers to the structural design and deployment of security controls and measures to protect information assets from various threats. It involves a multi-layered approach that includes network security, application security, data security, and endpoint security. The objective is to create a resilient security posture capable of effectively detecting, responding to, and mitigating security incidents. Information security architecture is essential for any organization's overall information security strategy. It involves implementing security policies, processes, and technologies to protect information assets against unauthorized access, use, disclosure, disruption, modification, or destruction. A well-designed architecture plays a crucial role in aligning with organizational goals and regulatory requirements, ensuring comprehensive coverage of all information security aspects. This alignment is essential to address the increasing risks associated with the integration of advanced technologies like unmanned vehicles. Security architecture should not only aim to make systems robust and resilient but also strive to improve defenses in the face of hostile actions, making them antifragile (Koien, 2020).
In commercial banks, robust information security architecture is critical. Banks handle vast amounts of sensitive data, including personal information, financial transactions, and proprietary information, making them prime targets for cybercriminals. Implementing a comprehensive information security architecture is essential to safeguard this data and maintain trust with customers and stakeholders. Information security architecture plays a crucial role in safeguarding critical systems like those in the banking sector. Network security, as discussed by Lu et al (2023), involves deploying firewalls, intrusion detection and prevention systems, and secure network protocols to defend against cyber threats like malware and denial-of-service attacks. Application security, focuses on ensuring that software applications are devoid of vulnerabilities by implementing secure coding practices, conducting regular security testing, and utilizing application firewalls. Additionally, having a well-defined security architecture aligned with the business strategy, as emphasized by Madsen (2022), is essential for

effectively addressing cyber threats and building a robust foundation for cybersecurity measures. Integrating these components into comprehensive security architecture is vital for enhancing the overall security posture of banking systems and protecting sensitive data from potential breaches and attacks.

Data security involves protecting data at rest, in transit, and in use through encryption, access controls, and data masking. Endpoint security protects devices such as computers, smartphones, and tablets that connect to the bank's network with antivirus software, endpoint detection and response systems, and mobile device management solutions. Identity and access management (IAM) systems ensure that only authorized users can access sensitive information and perform specific actions.In the context of digitalizing the information security posture of commercial banks in Rivers State, integrating these components is vital. These banks operate in a highly regulated environment, where compliance with the Nigeria Data Protection Regulation (NDPR) and the Cybercrimes (Prohibition, Prevention, Etc.) Act of 2015 is mandatory. In the digital age, a comprehensive information security architecture plays a pivotal role in enhancing cybersecurity posture, aligning with regulatory requirements, and adhering to industry best practices (Mpekoa, 2024). By prioritizing incident response and management, organizations, especially in the banking sector, can effectively protect sensitive data, ensure regulatory compliance, and support sustainable growth. Implementing advanced cryptographic techniques and ensuring scalability are crucial components of a robust security architecture, enabling banks to combat evolving cyber threats and maintain the integrity, confidentiality, and availability of financial information (Ewuga, 2023).

Incidences Response & Management

In the contemporary digital landscape, incident response and management play a vital role in the information security architecture of commercial banks, especially in Rivers State. These processes involve a systematic approach to preparing for, detecting, containing, eradicating, and recovering from cybersecurity incidents, as highlighted in the works of Guerra et al., (2023); Serrano et al., (2024). By implementing incident response strategies, organizations can minimize the impact of security breaches, ensure operational continuity, and safeguard sensitive financial data. Effective incident response and management begin with preparation, which involves developing and regularly updating incident response plans, training staff, and conducting simulated cyberattack drills. These preparatory steps ensure that the bank's personnel are well-equipped to handle potential security breaches efficiently. Detection is the next critical phase, where advanced monitoring tools and techniques are employed to identify and analyze security threats in real-time. Prompt detection allows for quicker responses, reducing the window of opportunity for attackers to inflict damage. Once a security incident is detected, containment strategies are implemented to isolate the affected systems and prevent the threat from spreading further within the network. This phase is vital for limiting the scope and impact of the incident. Following containment, the eradication process involves removing the threat from the system, whether it be through malware removal, patching vulnerabilities, or other remediation efforts. Finally, the recovery phase focuses on restoring affected systems and data to normal operations while ensuring that all security measures are re-evaluated and strengthened to prevent future occurrences.

The integration of incident response and management into the information security architecture of commercial banks in Rivers State is crucial due to the significant amounts of sensitive data they handle, making them prime targets for cybercriminals (Anifalaje, 2024). Implementing robust incident response strategies within their security frameworks can enhance resilience against cyber threats, mitigating immediate risks and aligning with regulatory requirements like the Nigeria Data Protection Regulation (NDPR) and the Cybercrimes (Prohibition, Prevention, Etc.) Act of 2015, which mandate stringent data protection and breach notification measures. Incident response and management not only help in regulatory compliance but are also vital for maintaining customer trust and confidence, especially in the face of increasing cyber-attacks and data breaches (Ajufo&Qutieshat, 2023). By embedding these

strategies, banks can effectively safeguard their operations and customer data while demonstrating a commitment to cybersecurity best practices and regulatory standards. In the event of a security breach, how a bank responds can significantly influence public perception. Prompt and effective incident management demonstrates a bank's commitment to protecting customer data and upholding the highest security standards. This, in turn, can enhance the bank's reputation and competitive edge in the market. Incident response and management are indispensable to the information security architecture of commercial banks in Rivers State. By incorporating these practices, banks can effectively manage and mitigate the impact of security incidents, comply with regulatory requirements, maintain customer trust, and ensure the continuity and integrity of their operations.

Cryptography

Cryptography plays a pivotal role in the information security architecture of commercial banks in Rivers State, ensuring the confidentiality, integrity, and authenticity of sensitive data. In the contemporary banking environment, where digital transactions are the norm, the necessity for robust cryptographic mechanisms cannot be overstated. Cryptography plays a crucial role in safeguarding sensitive information in commercial banks by utilizing sophisticated algorithms to encrypt data, ensuring its security from unauthorized access and cyber threats (Sari et al., 2024). Techniques like symmetric and asymmetric encryption are employed to protect customer information, financial transactions, and other critical data both during transmission and while stored in databases (Alemami et al., 2019). The RSA algorithm, for instance, utilizes prime numbers to generate secure keys for encryption and decryption processes, enhancing data protection in banking systems. Cryptography not only ensures confidentiality but also addresses integrity, authentication, and non-repudiation concerns, making it an indispensable tool for maintaining trust and security in the digital realm. For instance, during online banking transactions, Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols encrypt the data exchanged between the bank's servers and the customer's device. This encryption safeguards against interception and tampering by malicious actors, ensuring that the data remains private and intact throughout the communication process. Additionally, cryptographic hashing is used to verify the integrity of data, ensuring that any alterations can be detected immediately, thus maintaining data accuracy and reliability. Moreover, cryptography underpins the implementation of digital signatures and certificates within the banks' information security framework. Digital signatures provide a means of authenticating the identity of the sender and ensuring that the message has not been altered since it was signed. This is particularly crucial in the context of financial transactions and communications, where verifying the authenticity of the parties involved is essential to prevent fraud and unauthorized activities. Certificates issued by trusted Certificate Authorities (CAs) further bolster this system by linking public keys to the identities of individuals and entities, thereby establishing a trusted environment for secure communications.

In the realm of data storage, cryptographic methods such as Advanced Encryption Standard (AES) are utilized to encrypt sensitive information stored in databases. This encryption ensures that even if the physical storage media are compromised, the data remains inaccessible without the appropriate decryption keys. Access to these keys is tightly controlled, often involving multi-factor authentication mechanisms, to prevent unauthorized access and ensure that only authorized personnel can decrypt and access the information.Commercial banks in Rivers State can enhance data protection and regulatory compliance by leveraging cryptographic solutions, as mandated by regulations like the Nigerian Data Protection Regulation (NDPR) (Anifalaje, 2024). By integrating encryption practices into their information security frameworks, banks can ensure the safeguarding of personal data, thereby building trust with customers and assuring them of the highest security standards. Cryptographic solutions, such as RSA and ECC integration, can strengthen data integrity, authentication, and confidentiality within the banking sector, offering reliable protection for client account information. Additionally, technological innovations like blockchain can further fortify the defense mechanisms of banks against fraudulent activities, contributing to a more secure, efficient, and resilient banking system (Adeyemo&Obafemi, 2024).Integration of cryptography into the information security architecture of commercial banks in Rivers State is indispensable for safeguarding sensitive data, maintaining regulatory compliance,

and ensuring the overall security of banking operations. The implementation of robust cryptographic mechanisms provides a comprehensive defense against a myriad of cyber threats, thereby enhancing the banks' ability to protect their assets and maintain the trust of their customers.

Scalability

Scalability plays a pivotal role in the information security architecture of commercial banks in Rivers State, ensuring that security measures can effectively expand alongside rising transaction volumes, data storage requirements, and technological advancements (Tøndel&Brataas, 2022). The ability to scale is crucial for maintaining robust security protocols as banks grow their services and customer base in a rapidly evolving digital landscape. In the context of commercial banks, scalability involves enhancing security infrastructure to accommodate higher loads without compromising performance or security. This entails implementing scalable encryption methods that can handle increasing data volumes. For example, modern cryptographic algorithms like Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) are designed to provide strong encryption while being efficient enough to scale with the growing data demands. Banks utilize these algorithms to ensure that their encryption processes remain effective and efficient, regardless of the amount of data being processed.

A scalable security architecture also requires the implementation of dynamic access control systems. As banks expand and more users access their systems, the complexity of managing user permissions and access rights increases. Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) systems offer scalable solutions by allowing permissions to be assigned based on roles or attributes, rather than to individual users. This flexibility ensures that access control remains manageable and secure, even as the number of users grows. Network security is another critical area where scalability is essential. Banks must prioritize robust network security infrastructure to manage increased traffic without compromising performance or security (Butcovan& Ivan, 2023). Strategies such as passwords, antivirus software, firewalls, encryption, intrusion detection systems, and intrusion prevention systems are crucial in mitigating cyber threats in the banking sector (Sarumi&Omotosho, 2021). Scalable network security solutions include the deployment of advanced firewalls, intrusion detection and prevention systems (IDPS), and distributed denial-of-service (DDoS) mitigation tools. These systems are designed to expand and adapt in response to increased network demands, providing continuous protection against evolving cyber threats. Cloud computing offers significant advantages in terms of scalability for information security architecture. By leveraging cloud-based security services, banks can dynamically adjust their security resources to meet fluctuating demands. Cloud platforms provide scalable solutions for data encryption, identity management, and threat detection, allowing banks to enhance their security posture without the need for extensive on-premises infrastructure. This not only ensures scalability but also provides cost efficiency and flexibility in managing security operations.

Regulatory compliance in the banking sector is a critical aspect that evolves alongside the industry's growth. Implementing scalable compliance management systems is essential to align security measures with changing regulatory standards like the Nigerian Data Protection Regulation (NDPR) (Abrahams et al., 2024). These systems leverage advanced technologies such as artificial intelligence and blockchain to automate complex compliance tasks, ensuring continuous monitoring and adaptation of security practices to meet evolving requirements. Additionally, the human aspect of information security scalability is crucial, emphasizing the need for effective monitoring systems and continuous education to ensure adherence to regulatory demands. By embracing scalable compliance management systems, banks can enhance operational efficiency, reduce costs, and maintain regulatory compliance in a dynamic and evolving regulatory landscape (Olawale et al., 2024). As banks grow, the need for skilled cybersecurity professionals increases. Implementing scalable training and development programs ensures that staff are equipped with the latest knowledge and skills to manage security effectively. Continuous education and certification programs help maintain a workforce capable of addressing complex security challenges, regardless of the bank's size.

Infor- Protection Law

In the digital age, the protection of information has become a paramount concern for organizations worldwide, particularly in the financial sector. Information protection laws provide the legal framework to ensure that sensitive data is safeguarded against unauthorized access, misuse, and breaches. These laws define the responsibilities of organizations in protecting personal and financial information, ensuring privacy, and implementing adequate security measures. The objective is to create a secure environment where data integrity, confidentiality, and availability are maintained.Information protection laws play a crucial role in establishing trust and accountability within societies. These laws aim to safeguard personal information, prevent misuse, and ensure transparency in governance. The implementation of such laws, like the Freedom of Information Act in the US and the Right to Information Act in India, has been instrumental in providing citizens with access to timely and appropriate information, thereby enhancing transparency and holding institutions accountable for their actions (Bellver et al., 2008). They mandate that organizations implement specific security practices and controls to protect data from cyber threats and breaches. These laws typically include provisions for data encryption, secure storage, access controls, and regular security audits. They also stipulate the procedures for reporting data breaches and the penalties for non-compliance. Such regulations are critical for maintaining the integrity of financial systems and protecting the interests of customers and stakeholders. In Nigeria, the Nigeria Data Protection Regulation (NDPR) and the Cybercrimes (Prohibition, Prevention, Etc.) Act of 2015 are the primary legislative instruments governing data protection. The NDPR, introduced in 2019, provides a comprehensive framework for data protection, outlining the rights of data subjects and the obligations of data controllers and processors. Adherence to the Nigeria Data Protection Regulations (NDPR) in commercial banks in Rivers State is crucial for implementing robust data protection measures, ensuring privacy, and maintaining compliance with regulatory requirements. However, the legal framework is further strengthened by the Cybercrimes Act, which criminalizes various cyber offenses and provides a legal deterrent against cybercrimes targeting financial institutions (Abdulkadir&Sambo, 2022). The NDPR emphasizes the need for data protection impact assessments to identify and minimize risks in data processing operations, particularly in intensive operations like online profiling, which involves significant personal data usage (Izuogu, 2021). Information protection laws underscores their role in enhancing cybersecurity posture. These laws compel organizations to adopt best practices in data protection, thereby reducing the risk of data breaches and cyberattacks. Compliance with these laws not only mitigates legal risks but also enhances the overall security environment, fostering trust among customers and stakeholders. In the context of digitalizing the information security posture of commercial banks in Rivers State, information protection laws play a pivotal role. As banks increasingly adopt digital technologies, the volume and sensitivity of data they handle grow, making robust data protection measures more critical than ever (Swanzy et al., 2024). Compliance with information protection laws ensures that banks implement the necessary security controls to protect customer data and maintain regulatory compliance. This alignment between legal requirements and technical security measures is essential for safeguarding data integrity and fostering a secure banking environment.Integrating information protection laws such as the Nigerian Data Protection Regulation (NDPR) and the Cybercrimes Act into the digital transformation of commercial banks in Rivers State can significantly enhance their cybersecurity posture. By adhering to these regulations, banks can protect sensitive information, reduce the risk of cyber threats, and maintain the trust of their customers (Oyewole et al., 2024). This legal and regulatory framework supports the sustainable growth of digital banking services, ensuring that banks can securely manage and protect their information assets in an increasingly digital world.

Personal Data Protection

The increasing digitalization of financial services has made personal data protection a critical concern for commercial banks, especially in Rivers State. Personal data protection refers to the practices and policies implemented to ensure the confidentiality, integrity, and availability of individuals' data. This involves safeguarding sensitive information such as personal identification details, financial records, and transaction histories from unauthorized access, misuse, or breaches.

Personal data protection in the banking sector is a critical aspect that combines technical requirements with legal obligations. Various research papers emphasize the importance of robust data protection measures in banking relationships, highlighting the need for explicit customer consent, strict security standards, and legislative improvements to safeguard personal data (Khuan, 2024; Haliwela, 2023). The legal frameworks governing personal data protection in the financial sector, such as the Electronic Information and

Transactions Law and the Omnibus Law on Job Creation, play a crucial role in ensuring transparency, data security, and fair data usage practices. Additionally, the Information Protection Law stipulates the appointment of a Data Protection Officer (DPO) in each bank to oversee compliance with data protection regulations. The DPO is responsible for ensuring that all data handling practices meet the legal requirements and for managing any data protection issues that arise. The law also emphasizes transparency, requiring banks to provide clear and accessible privacy policies and conduct regular training for employees on data protection principles. Compliance with the Information Protection Law is enforced through regular audits and inspections by regulatory bodies. Non-compliance with digital banking regulations can indeed lead to severe consequences such as fines and the suspension of banking licenses, underscoring the critical importance of adherence to these regulatory frameworks (Ofodile et al., 2024). By implementing and strictly following these measures, commercial banks in Rivers State can effectively safeguard customer data, establish trust with their clients, and uphold their reputations in a fiercely competitive digital environment.

Data Breach Notification

In today's digital age, data breaches have become a significant concern for organizations, particularly commercial banks, due to the sensitive nature of the data they handle. A data breach occurs when protected or confidential data is accessed, disclosed, or used without authorization, potentially compromising customer information. Data breach notification is the process by which affected individuals and regulatory authorities are informed about such incidents. This process is crucial for mitigating potential harm and ensuring transparency and accountability. The Information Protection Law of commercial banks in Rivers State underscores the significance of data breach notification within the realm of information governance, aligning with the broader discourse on cybersecurity and fraud prevention (Adeyemo&Obafemi, 2024; Ashraf & Sunder, 2023). This law mandates that banks promptly inform affected customers and relevant authorities upon breach discovery, outlining breach specifics, compromised data, potential risks to individuals, and remedial actions taken to mitigate the breach and prevent future incidents. The emphasis on timely and transparent notification not only aligns with best practices in data security but also serves to enhance customer trust, regulatory compliance, and overall cybersecurity resilience within the banking sector, reflecting a proactive approach to safeguarding sensitive information and maintaining stakeholder confidence. Timely and transparent communication is essential in maintaining customer trust and regulatory compliance. The Information Protection Law's strict timelines for breach notification, mandating banks to inform affected parties within 72 hours of breach discovery, play a crucial role in empowering customers to safeguard themselves against fraud and identity theft. Research indicates that consumers often fail to take necessary protective actions even after receiving breach notifications, highlighting the importance of timely alerts (Zou et al., 2019). The law also requires banks to have a comprehensive incident response plan in place. This plan should include procedures for detecting, reporting, and responding to data breaches. Having such a plan ensures that banks can act quickly to contain breaches and minimize damage. Regular security assessments and employee training are also mandated to reduce the risk of breaches and improve the bank's ability to respond effectively when they occur.

Transparency is indeed crucial in the realm of information protection, especially in the banking sector, as it fosters trust and accountability (Haryandu et al., 2023). Banks are mandated to offer clear and easily accessible details regarding any data breaches, specifying the compromised data and outlining the measures being implemented to mitigate the repercussions.

Continuous updates are essential to keep customers informed throughout the resolution process, ensuring transparency and maintaining customer confidence. Studies emphasize the significance of transparency in banking activities, highlighting how increased disclosure can aid in reducing the costs of banking crises and enhance market discipline to monitor risk-taking behaviors of banks (Manganaris et al., 2017). Therefore, a commitment to transparency not only aligns with legal requirements but also contributes to building a resilient and trustworthy banking environment. Non-compliance with data breach notification requirements can result in severe penalties, including substantial fines and reputational damage. Regulatory bodies conduct regular audits and inspections to ensure that banks adhere to these regulations. By complying with the data breach notification requirements, commercial banks in Rivers State demonstrate their commitment to protecting customer data and upholding their legal obligations. Adhering to these regulations not only helps protect customers but also enhances the bank's reputation for reliability and integrity. Prompt and transparent data breach notification reinforces the bank's commitment to safeguarding personal information, thus fostering trust and confidence among its customers. In the rapidly evolving digital landscape, where cyber threats loom large over the banking sector, effective data breach notification plays a pivotal role in upholding security and trust within financial institutions (Oyewole et al., 2024)

Cross Border Data Transfer

In an increasingly interconnected world, cross-border data transfer has become a critical issue for commercial banks operating in diverse regions, including Rivers State. Cross-border data transfer refers to the movement of data across national borders, often for processing, storage, or management purposes. This practice is essential for global financial institutions that require efficient data handling to provide seamless services to their customers. However, it also raises significant concerns about data protection and regulatory compliance. The Information Protection Law of commercial banks in Rivers State plays a vital role in addressing the complexities of cross-border data transfer (Anifalaje, 2024). This law imposes stringent requirements on banks to ensure that personal data transferred internationally is adequately protected, necessitating that the recipient country has robust data protection laws akin to those in Rivers State. Such measures are crucial for maintaining consistent levels of data security and privacy protection, regardless of where the data is processed or stored. The implementation of these regulations aligns with the global trend of enhancing personal data protection in the digital era, especially within the financial and banking sectors (Khuan, 2024); to comply with the Information Protection Law, banks must conduct thorough assessments of the data protection regulations in the destination country before transferring any personal data. This involves evaluating the legal framework, enforcement mechanisms, and data protection practices to ensure they meet the required standards. If the destination country does not offer adequate protection, banks must implement additional safeguards, such as binding corporate rules or standard contractual clauses, to protect the data during the transfer process. The law also mandates that banks obtain explicit consent from customers before transferring their personal data across borders. Customers must be informed about the transfer, the reasons for it, and the measures in place to protect their data. This transparency helps to build trust and ensures that customers are aware of how their information is being handled.

Additionally, the Information Protection Law requires banks to maintain detailed records of all cross-border data transfers. These records should include the nature of the data, the destination country, the purpose of the transfer, and the safeguards implemented to protect the data. Regular audits and inspections by regulatory bodies ensure that banks comply with these requirements and maintain high standards of data protection. Failure to comply with cross-border data transfer regulations can result in severe penalties, including fines and restrictions on data transfer capabilities. These penalties underscore the importance of adhering to the law and implementing robust data protection measures. By complying with the Information Protection Law, commercial banks in Rivers State can mitigate the risks associated with cross-border data transfers and ensure that customer data is protected at all times.

Effective management of cross-border data transfer is essential for maintaining the integrity and trustworthiness of the banking sector. Adhering to information protection laws is crucial for banks to securely transfer and safeguard personal data across geographical boundaries, enhancing customer trust and maintaining their reputation in the global financial landscape. Studies emphasize the significance of data security in fostering consumer trust in fintech services (Druga, 2024), highlighting the need for robust cybersecurity protocols, regulatory compliance, and transparent communication strategies to mitigate risks and build confidence.

Operational Efficiency & Competitive Advantage

The implementation of digitalizing information security posture within the information security architecture and information protection law in commercial banks in Rivers State is pivotal in achieving operational efficiency and competitive advantage. This transformation is driven by the increasing reliance on digital technologies and the corresponding rise in cyber threats, necessitating robust measures to safeguard sensitive financial information. The digitalization of information security posture in commercial banks can significantly enhance operational efficiency by integrating advanced security technologies like artificial intelligence (AI), machine learning, and blockchain (Farayola, 2024). AI empowers proactive threat detection through real-time analysis of data, while machine learning enables dynamic adaptation to emerging threats, automating routine security tasks and reducing human error. Blockchain technology ensures transactional data integrity and transparency, reducing fraud risks and unauthorized access, while also facilitating secure data sharing among stakeholders (Odeyemi et al., 2024). By combining these technologies, banks can streamline security processes, detect anomalies swiftly, prevent security breaches effectively, and automate the execution of secure transactions, ultimately bolstering the resilience and efficiency of their security operations in the dynamic landscape of digital banking. Another crucial aspect of operational efficiency is the optimization of resource allocation. Digitalizing the information security posture allows banks to adopt a proactive approach to risk management. Predictive analytics can forecast potential security breaches, enabling banks to allocate resources more effectively and prioritize areas that require immediate attention. This proactive stance not only mitigates risks but also reduces the costs associated with security incidents, such as data breaches and regulatory fines. Moreover, the integration of security measures into the overall information security architecture ensures a cohesive and unified approach to data protection, further enhancing operational efficiency.

Competitive advantage is also significantly bolstered through the implementation of a digitalized information security posture. In an industry where trust and reputation are paramount, demonstrating a commitment to robust security measures can differentiate a bank from its competitors (Farayola, 2024). Customers are increasingly aware of the importance of data security and are likely to choose banks that prioritize the protection of their personal and financial information. By investing in state-of-the-art security technologies and adhering to stringent information protection laws, commercial banks in Rivers State can build and maintain customer trust, fostering long-term loyalty and retention. Furthermore, compliance with information protection laws is essential in maintaining a competitive edge. Regulations such as the Nigeria Data Protection Regulation (NDPR) mandate strict data protection standards, and non-compliance can result in substantial penalties and reputational damage. Digitalizing information security in banks through innovative technologies like Artificial Intelligence (AI), Blockchain, and Business Intelligence (BI) can indeed enhance their compliance with regulations, thus avoiding fines and bolstering their reputation as secure and responsible institutions (Onyshchenko et al., 2023). These technologies enable real-time threat detection, proactive risk management, and secure transactional data storage, ensuring the integrity and confidentiality of financial information while meeting regulatory requirements (Dopamu et al., 2024). This compliance also opens up opportunities for collaboration with international partners who prioritize data security and regulatory adherence. In addition, the digitalization of information security posture fosters innovation and agility.

With secure and resilient IT infrastructures, banks can confidently explore new digital services and products, such as mobile banking, digital wallets, and personalized financial advisory services. This ability to innovate and quickly adapt to changing market demands is a key competitive advantage in the fast-paced financial sector. By leveraging cutting-edge security technologies, commercial banks in Rivers State can offer innovative solutions that meet the evolving needs of their customers, thereby attracting new clients and expanding their market share. The implementation of a digitalized information security posture within the information security architecture and information protection law framework significantly enhances both operational efficiency and competitive advantage for commercial banks in Rivers State. Through automation, resource optimization, and proactive risk management, banks can streamline their operations, reduce costs, and improve overall efficiency. Simultaneously, by prioritizing data security and regulatory compliance, banks can build trust, foster customer loyalty, and maintain a competitive edge in the dynamic financial landscape. The integration of advanced security technologies not only safeguards sensitive information but also empowers banks to innovate and adapt, ensuring sustained growth and success in the digital era (Adeyemo&Obafemi, 2024).

Theoritical Review

The Technology Acceptance Model (TAM), developed by Fred Davis in 1989, provides a robust theoretical framework for analyzing the digitalization of information security posture within the information security architecture and information protection law of commercial banks in Rivers State. The theory's relevance lies in its focus on the factors that influence the acceptance and usage of new technologies, making it an ideal lens through which to examine the adoption of digital security measures in the banking sector. The TAM posits that two primary factors, Perceived Usefulness (PU) and Perceived Ease of Use (PEOU), play a critical role in determining users' acceptance of technology. Perceived Usefulness refers to the degree to which an individual believes that using a particular system will enhance their job performance. In the context of commercial banks, if employees perceive that digital security measures, such as advanced encryption techniques and automated threat detection systems, will significantly improve the efficiency and effectiveness of their work, they are more likely to embrace these technologies. This perceived enhancement in job performance is crucial for fostering a positive attitude towards the adoption of digital security measures.

Perceived Ease of Use is the degree to which an individual believes that using a particular system will be free of effort. For commercial banks, the implementation of user-friendly digital security solutions is essential. If the new security systems are intuitive and easy to navigate, employees will experience less resistance and frustration, leading to higher acceptance rates. Ease of use not only encourages initial adoption but also ensures sustained usage of the security measures, thereby strengthening the overall information security posture of the bank.

The TAM further asserts that Behavioral Intention to Use (BI) is influenced by both PU and PEOU. When employees find digital security technologies both useful and easy to use, their intention to utilize these systems increases. This behavioral intention is a strong predictor of actual system use. In the banking context, this means that when staff members recognize the benefits and user-friendliness of advanced security measures, they are more likely to integrate these tools into their daily operations, enhancing the bank's overall security framework. Actual System Use, the end result in the TAM, is determined by the users' behavioral intentions. For commercial banks in Rivers State, achieving high levels of actual system use is critical. It ensures that the digital security measures implemented are effectively utilized, providing robust protection against cyber threats and regulatory compliance. This alignment between behavioral intention and actual use underscores the importance of addressing both perceived usefulness and ease of use during the implementation phase.

The justification for applying the TAM to this analysis lies in its proven applicability across various technological contexts. The model's emphasis on user perceptions aligns well with the practical considerations of implementing digital security measures in commercial banks. By understanding and addressing the factors that influence technology acceptance, banks can design and deploy security systems that not only meet technical requirements but also gain user acceptance, thereby maximizing their effectiveness.

Empirical Review

Grobler&Louwrens (2005) investigated the critical role of information security within organizational operations, highlighting how it has become an indispensable aspect of modern business practices. They examined the increasing implementation of security countermeasures, such as security policies, intrusion detection systems, access control mechanisms, and anti-virus products, which organizations deploy to protect their information and information assets from potential threats. The authors conducted an in-depth analysis of the challenges faced by organizations in managing information security. They found that many companies do not adopt an integrated, holistic management approach, making it difficult for security professionals and managers to fully understand their organization's security posture. This fragmented approach, combined with limited budgets and staff, hinders the ability of security professionals to adequately address the security demands of their organizations.

Grobler&Louwrens emphasized the necessity for managers to assess the security posture of their organizations accurately to determine the effectiveness and efficiency of the security measures in place. However, their research revealed that many organizations lack proper guidelines for conducting forensic investigations following security incidents. This deficiency often leads to unproductive conclusions in investigations, as organizations do not prioritize forensic investigations, a view supported by Sinangin (2002). To address these issues, Grobler&Louwrens proposed the development of a digital forensic management model (DFMM). This model, they argued, is essential for conducting successful investigations. The aim of their paper was to use elements of existing information security architectures to propose a new architecture. This new architecture would encompass various dimensions of information security and serve as a framework for managing, implementing, and assessing an organization's security posture. Additionally, they posed the question of whether the DFMM should be integrated into the broader information security architecture, suggesting that such integration could enhance the overall effectiveness of security management within organizations.

Molnár (2016) investigated the impact of the Information Security Law (2013. L. law) in Hungary, a legislative measure accepted by the Hungarian Parliament after two decades of effort. This law lays the groundwork for enhancing information security within Public Administration, accompanied by decrees and resolutions that regulate the categorization and management of information systems in compliance with the required security levels. Molnár examined the execution of this law and identified several issues and problems that have arisen. These issues need to be addressed by the guardians of information security and the owners of information systems within various sectors of the Hungarian Public Administration. One major challenge is the categorization of these systems and the realization of control objectives, particularly for legacy systems. This challenge necessitates a systematic and disciplined methodology to manage the complexity effectively. To address these challenges, Molnár proposed the adaptation of Enterprise Architecture, specifically a customized version for Information Security Architecture. This approach provides a structured framework for managing information security. Additionally, security guardians in Hungary are trained in this methodology through courses offered by the Public Administration University in Budapest, ensuring they possess the necessary knowledge to implement the law effectively.

Al-Zaben et al. (2018) investigated the growing concerns surrounding surveillance and breaches of user privacy, which have raised questions about the current procedures for third-party data collection. They examined how massive amounts of Personally Identifiable Information (PII) are being exploited due to malpractice, identity theft, spamming, phishing, and cyber-espionage. The study noted the extensive flow of data from users to enterprises for data-driven market analysis and prediction, which makes it challenging to track the flow and authenticity of PII. To address these issues, Al-Zaben et al. proposed the use of Blockchain technology, described as an 'immutable' distributed ledger capable of effectively tracking the exchange, storage, and distribution of PII. However, they also considered the ongoing EU General Data Protection Regulation (GDPR), which demands the 'right to be forgotten' and the ability for data to be erased. To reconcile these requirements with the characteristics of Blockchain, the authors proposed an off-chain Blockchain architecture that combines both local databases and distributed ledgers to ensure a trustworthy PII lifecycle.

The study involved modifying existing Blockchain architectures to align with key GDPR factors and creating a prototype using Multichain 2.0 to validate the proposed architecture. This architecture stores PII and non-PII in physically separated locations, allowing users to benefit from the privacy and security of Blockchain technology while complying with GDPR regulations. The validation process included comparing the proposed system with existing methodologies from a technical perspective, and the study also discussed future research opportunities in this area.

Summary of Empirical Review and Knowledge Gap

S/N	Researcher (s)	Study Focus	Variables	Findings	Remarks: Knowledge Gap and Action
1	Grobler&Louwrens (2005)	Information security within organizational operations	Security policies, intrusion detection systems, access control mechanisms, anti-virus products	- Lack of integrated management approach. Challenges due to limited budgets and staff. Need for guidelines in forensic investigations	The study of Grober&Louwrens. (2005) centered on Information security within organizational operations. While this study focuses on infor-security architecture and infor-protection law of Commercial Banks in Rivers State. The current study dimensionalizesinfor-security architecture incidence responses and management, cryptography, and scalability; the study also measures infor-protection law in terms of personal data protection, data breach notification, and cross border data transfer. The study shows its outcome in terms of operational efficiency, and competitive advantage.

2	Molnár (2016)	Impact of Information Security Law (2013. L. law) in Hungary	Categorization of information systems, compliance with security levels	- Issues in law execution within Public Administration. Challenges in categorizing and controlling legacy systems	The study of Molnar (2016) centered on impact of information security law (2013. L. law) in Hungary. While this study focuses on infor-security architecture and infor-protection law of Commercial Banks in Rivers State. The current study dimensionalizesinfor-security architecture incidence responses and management, cryptography, and scalability; the study also measures infor-protection law in terms of personal data protection, data breach notification, and cross border data transfer. The study shows its outcome in terms of operational efficiency, and competitive advantage.
3	Al-Zaben et al. (2018)	Surveillance, privacy breaches, Blockchain technology in data protection	Personally Identifiable Information (PII), Blockchain architecture, GDPR compliance	- Exploitation of PII due to malpractice. Proposal of off-chain Blockchain architecture for PII lifecycle management	The study Al-Zaben et al. (2018) centered on surveillance, privacy breaches, Blockchain technology in data protection. While this study focuses on infor-security architecture and infor-protection law of Commercial Banks in Rivers State. The current study dimensionalizesinfor-security architecture incidence responses and management, cryptography, and scalability; the study also measures infor-protection law in terms of personal data protection, data breach notification, and cross border data transfer. The study shows its outcome in terms of operational efficiency, and competitive advantage.

Methodology

The study adopted explanatory survey research design. The population of the study consisted of Two Hundred and Thirty (230) top managers from twenty-three (23) Commercial Banks operating in Rivers State, Nigeria. Top Ten (10) managers were chosen from each bank. Census was adopted for the study, the entire population was employed as the sample size of the study. To obtain primary data, a structured questionnaire entitled "Infor- Security Architecture and Infor-protection law(ISAIPL)" was designed in five point Likert scale with the following response options: Very High Extent (VHE) 4; High Extent (HE) 3; Moderate Extent (ME) 2; Low Extent (LE) 1. The instrument was validated by two experts in Management. The reliability of the instrument was ascertained using Crombach Alpha with the least coefficient up to 0.763. Out of 230 copies of the questionnaire distributed, 220 copies of the questionnaires were retrieved, representing 83%. The data obtained from the field were analyzed using Spearman's Rank Order Correlation Coefficient with the aid of SPSS 22.0 (Statistical Package for Social Sciences).

Decision Rule: Using a level of significance of 0.05 (confidence interval of 95%), when a calculated significant value is less than 0.05 the null hypothesis is rejected, if otherwise, the null hypothesis is accepted.

Results/findings

Ho_1: Infor- Security Architecture does not have any significant relationship with Operational Efficiency of Commercial Banks in Rivers State.

Table 1. Correlations between Infor-security architecture and operational efficiency

		Infor-security architecture	Operational efficiency
Infor-security architecture	Pearson Correlation	1	.737**
	Sig. (2-tailed)		.000
	N	220	220
Operational efficiency	Pearson Correlation	.737**	1
	Sig. (2-tailed)	.000	
	N	220	220

**. Correlation is significant at the 0.01 level (2-tailed).

Source: SPSS Output from Field Data (2024)

Table 1 above indicates that the hypothesis relating to Infor-security architecture and operational efficiency has an r-value of 0.737 at a significance level of 0.00, which is less than the selected alpha level of 0.05. The alternative hypothesis is accepted while the null hypothesis (Ho1), which claims that Infor-security architecture does not have any significant relationship with operational efficiency of Commercial Banks in Rivers State, is rejected because the significance value is less than the alpha level of 0.05. The correlation coefficient of 0.737 suggests that infor-security architecture and operational efficiency of commercial banks in Rivers State has a significant positive relationship.

Ho_2: Infor- Security Architecture does not have any significant relationship with competitive Advantage of Commercial Banks in Rivers State.

Table 2. Correlations between Infor-security architecture and competitive advantage

			Infor-security architecture	Competitive advantage
Spearman's rho	Infor-security architecture	Correlation Coefficient	1.000	.609**
		Sig. (2-tailed)	.	.000
		N	220	220
	Competitive advantage	Correlation Coefficient	.609**	1.000
		Sig. (2-tailed)	.000	.
		N	220	220

**. Correlation is significant at the 0.01 level (2-tailed).

Source: SPSS Output from Field Data (2024)

Table 2 above indicates that the hypothesis relating to Infor-security architecture and competitive advantage has an r-value of 0.609 at a significance level of 0.00, which is less than the selected alpha level of 0.05. The alternative hypothesis is accepted while the null hypothesis (Ho2), which claims that infor-security architecturedoes not have any significant relationship with competitive advantage of Commercial Banks in Rivers State, is rejected because the significance value is less than the alpha level of 0.05. The correlation coefficient of 0.609 suggests that infor-security architecture and competitive advantage of commercial banks in Rivers Statehas a significant positive relationship.

Ho_3: Infor- Protection Law does not have any significant relationship with Operational Efficiencyof Commercial Banks in Rivers State.

Table3. Correlations between infor-protection law and operational efficiency

			Infor-protection law	Operational efficiency
Spearman's rho	Infor-protection law	Correlation Coefficient	1.000	.519**
		Sig. (2-tailed)	.	.000
		N	220	220
	Operational efficiency	Correlation Coefficient	.519**	1.000
		Sig. (2-tailed)	.000	.
		N	220	220

**. Correlation is significant at the 0.01 level (2-tailed).

Source: SPSS Output from Field Data (2024)

Table 3 above indicates that the hypothesis relating to infor-protection law and operational efficiency has an r-value of 0.519 at a significance level of 0.00, which is less than the selected alpha level of 0.05. The alternative hypothesis is accepted while the null hypothesis (Ho3), which claims that infor-protection law does not have any significant relationship with operational efficiency of Commercial Banks in Rivers State, is rejected because the significance value is less than the alpha level of 0.05. The correlation coefficient of 0.519 suggests that infor-protection law and operational efficiency of commercial banks in Rivers Statehas a moderate positive relationship.

Ho_4: Infor- Protection Law does not have any significant relationship with competitive advantage of Commercial Banks in Rivers State.

Table3. Correlations between infor -protection law and competitive advantage

			Infor-protection law	Competitive advantage
Spearman's rho	Infor-protection law	Correlation Coefficient	1.000	.408**
		Sig. (2-tailed)	.	.000
		N	220	220
	Competitive advantage	Correlation Coefficient	.408**	1.000
		Sig. (2-tailed)	.000	.
		N	220	220

**. Correlation is significant at the 0.01 level (2-tailed).

Source: SPSS Output from Field Data (2024)

Table 4 above indicates that the hypothesis relating to infor-protection law and competitive advantage has an r-value of 0.408 at a significance level of 0.00, which is less than the selected alpha level of 0.05. The alternative hypothesis is accepted while the null hypothesis (Ho4), which claims that infor-protection law does not have any significant relationship with competitive advantage of Commercial Banks in Rivers State, is rejected because the significance value is less than the alpha level of 0.05. The correlation coefficient of 0.408 suggests that infor-protection law and competitive advantage of commercial banks in Rivers Statehas a moderate positive relationship.

Discussion:

Ho_1: Infor- Security Architecture and Operational Efficiency

Result reveals that there is significant correlation between Infor-security architecture and operational efficiency of Commercial Banks. With a correlation value of 0.737, the result reveals that infor-securityarchitecture has a significant positive relationship with operational efficiency of Commercial Banks in Rivers State. Similarly, this finding was supported by **Grobler&Louwrens (2005) whose findings** emphasis on integrated security management and the need for holistic approaches to security align with the significant relationship between Infor- Security Architecture and Operational Efficiency.

Ho_2: Infor- Security Architecture and competitive Advantage

Result reveals that there is significant correlation between Infor- Security Architecture and competitive Advantageof Commercial Banks. With a correlation value of 0.609, the result reveals that Infor-security architecture has a significant positive relationship with competitive advantage of Commercial Banks in Rivers State. Similarly, this finding was supported by **Al-Zaben et al. (2018)** their focus on Blockchain technology for secure data management aligns with the findings on Infor- Security Architecture and competitive Advantage.

$H0_3$: Infor- Protection Law and Operational Efficiency

Result reveals that there is significant correlation between Infor- Protection Law and Operational Efficiencyof Commercial Banks. With a correlation value of 0.519, the result reveals that infor-protection law has a moderate positive relationship with operational efficiency of Commercial Banks in Rivers State. Similarly, this finding was supported by **Molnár (2016)** the findings pointed on the structured framework for managing information security aligns with the findings on Infor- Protection Law and Operational Efficiency.

$H0_4$: Infor-Protection Law and Competitive Advantage

Result reveals that there is significant correlation between Infor- Protection Law and competitive advantage of Commercial Banks. With a correlation value of 0.408, the result reveals that infor-protection law has a moderate positive relationship with competitive advantage of Commercial Banks in Rivers State. Similarly, this finding was supported by **Molnár (2016)** the findings pointed on the structured framework for managing information security aligns with the findings on Infor- Protection Law and competitive advantage.

Conclusion

The digitalization of the information security posture in commercial banks in Rivers State is essential for enhancing operational efficiency and gaining a competitive advantage. This study has comprehensively analyzed key components of information security architecture, including incident response and management, cryptography, and scalability. Additionally, it has examined crucial aspects of information protection law, such as personal data protection, data breach notification, and cross-border data transfer. The findings underscore the critical importance of a robust information security architecture in safeguarding sensitive data and ensuring the resilience of banking operations. Effective incident response and management protocols are vital for mitigating the impact of security breaches, while advanced cryptographic measures ensure the confidentiality and integrity of data.

Scalability within security systems allows banks to adapt to evolving threats and growing data volumes without compromising security.

Furthermore, adherence to information protection laws enhances customer trust and ensures compliance with regulatory requirements. Personal data protection measures safeguard customer information, data breach notifications ensure transparency, and regulations governing cross-border data transfers maintain data security in an increasingly globalized environment. Overall, the digitalization of information security in commercial banks not only fortifies their defenses against cyber threats but also drives operational efficiencies and fosters a competitive edge. By prioritizing information security, these banks can build a resilient infrastructure that supports sustainable growth, regulatory compliance, and enhanced customer confidence.

Recommendations

- Banks should develop and regularly update incident response plans that detail specific steps for identifying, mitigating, and recovering from security incidents.
- Banks should employ state-of-the-art encryption techniques to protect sensitive data both in transit and at rest.
- Banks should implement security systems that can scale with the growth of data and the evolving threat landscape without compromising performance.
- Banks should establish protocols for promptly notifying affected individuals and relevant authorities in the event of a data breach, as required by law.
- Banks should implement measures to ensure the security of data transferred across borders, in compliance with international data protection standards.

REFERENCE

Abdulkadir, A. B., &Sambo, A. O. (2022). Data privacy rights and bankers' business interests in Nigeria: Reflections on opportunities, challenges and legal reforms. *Malaysian Journal of Law & Society*, *30*.

Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., &Dawodu, S. O. (2024). Mastering compliance: A comprehensive review of regulatory frameworks in accounting and cybersecurity. *Computer Science & IT Research Journal*, *5*(1), 120-140.

Adeyemo, K., &Obafemi, F. J. (2024). A survey on the role of technological innovation in Nigerian deposit money bank fraud prevention. *South Asian Journal of Social Studies and Economics*, *21*(3), 133-150.

Ajufo, G., &Qutieshat, A. (2023). An examination of the human factors in cybersecurity: Future direction for Nigerian banks. *Indonesian Journal of Information Systems*, *6*(1), 1-16.

Alemami, Y., Mohamed, M. A., &Atiewi, S. (2019). Research on various cryptography techniques. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(2S3), 395-405.

Al-Zaben, N., Onik, M. M. H., Yang, J., Lee, N. Y., & Kim, C. S. (2018, August). General data protection regulation complied blockchain architecture for personally identifiable information management. In *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)* (pp. 77-82). IEEE.

Anifalaje, K. (2024). A legal approach to the protection of customers of banks and other financial institutions from identity theft in Nigeria. *Northern Ireland Legal Quarterly*, *75*(AD1), 1-28.

Ashraf, M., & Sunder, J. (2023). Can shareholders benefit from consumer protection disclosure mandates? Evidence from data breach disclosure laws. *The Accounting Review*, *98*(4), 1-32.

Bellver, A., Mendiburu, M., &Poli, M. (2008). Strengthening transparency and accountability through Access to Information.

Butcovan, M. A., & Ivan, R. (2023). Policies and strategies aimed at ensuring the security of banking institutions and their It Systems. *Agora International Journal of Economical Sciences*, *17*(2), 27-33.

Crisanto, J. C., &Prenio, J. (2021). Emerging prudential approaches to enhance banks' cyber resilience. *The Palgrave Handbook of FinTech and Blockchain*, 285-306.

Dopamu, O., Adesiyan, J., &Oke, F. (2024). Artificial intelligence and US financial institutions: Review of AI-assisted regulatory compliance for cybersecurity. *World Journal of Advanced Research and Reviews. Available at: https://wjarr. com/content/artificial-intelligence-and-us-financial-institutions-review-ai-assistedregulatory (Accessed: 28 May 2024)*.

Drugã, R. I. (2024). The effect of trust in banking institutions on behavioural intentions for e-services. *Three Seas Economic Journal*, *5*(1), 1-12.

Ewuga, S. K., Egieya, Z. E., Omotosho, A., &Adegbite, A. O. (2023). ISO 27001 in banking: An evaluation of its implementation and effectiveness in enhancing information security. *Finance & Accounting Research Journal*, *5*(12), 405-425.

Farayola, O. A. (2024). Revolutionizing banking security: integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity. *Finance & Accounting Research Journal*, *6*(4), 501-514.

Grobler, T., &Louwrens, B. (2005, June). New information security architecture. In *ISSA 2005 New Knowledge Today Conference. Information Security South Africa*.

Guerra, P. A. C., Barcelos, F. A., Nunes, R. C., De Freitas, E. P., & Silva, L. A. D. L. (2023, October). An artificial intelligence framework for the representation and reuse of cybersecurity incident resolution knowledge. In *proceedings of the 12th Latin-American symposium on dependable and secure computing* (pp. 136-145).

Gulyamov, S., &Raimberdiyev, S. (2023). Personal data protection as a tool to fight cyber corruption. *International Journal of Law and Policy*, *1*(7).

Haliwela, N. S. (2023). The essence of legal protection of personal data of customers in banking transactions. *SASI*, *29*(3), 548-556.

Haryandu, R., Azheri, B., & Rembrandt, R. (2023). Legal protection of customer data in implementing the financial information access law for tax purposes. *GemaWiralodra*, *14*(2), 912-920.

Igwenagu, U. T. I., Salami, A. A., Arigbabu, A. S., Mesode, C. E., Oladoyinbo, T. O., &Olaniyi, O. O. (2024). Securing the digital frontier: Strategies for cloud computing security, database protection, and comprehensive penetration testing. *Journal of Engineering Research and Reports*, *26*(6), 60-75.

Ikram, N. A. H. S. (2024). Data breaches exit strategy: a comparative analysis of data privacy laws. *Malaysian Journal of Syariah and Law*, *12*(1), 135-147.

Izuogu, C. E. (2021). Conducting data protection impact assessments for online profiling under the NDPR 2019. *Protecting digital consumers, assets, identity, privacy and data in a digital economy: The Nigerian experience*.

Jangampeta, S. (2022). Financial data security and SIEM: Protecting sensitive financial information in banking and fintech systems. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *13*(2), 1185-1188.

Khuan, H. (2024). The legal protection of personal data in fintech peer-to-peer (p2p) lending practices: Orientation and formulation. *Pena Justisia: Media KomunikasidanKajianHukum*, *22*(3), 433-466.

Køien, G. M. (2020). A philosophy of security architecture design. *Wireless personal communications*, *113*(3), 1615-1639. Køien, G. M. (2020). A philosophy of security architecture design. *Wireless Personal Communications*, *113*(3), 1615-1639.

Lu, X., Dong, R., Wang, Q., & Zhang, L. (2023). Information security architecture design for cyber-physical integration system of air traffic management. *Electronics*, *12*(7), 1665.

Madsen, T. (2022). *Security architecture–how & why*. River publishers.

Manganaris, P., Beccalli, E., &Dimitropoulos, P. (2017). Bank transparency and the crisis. *The British accounting review*, *49*(2), 121-137.

Molnár, B. (2016). IT security in Hungarian public administration, Models of information security architecture in practice. *AssociazioneItaliana per l'informaticaedilCalcoloAutomatico, AICA, IT Star, Milan, Italy*, 28-44.

Mpekoa, N. (2024, March). An analysis of cybersecurity architectures. In *international conference on cyber warfare and security* (Vol. 19, No. 1, pp. 200-207).

Mwita, P. S., &Mhina, J. R. A. (2023). Assessing the effectiveness of the implementation of cybercrimes mitigation strategies in selected commercial banks in Tanzania. *European Journal of Theoretical and Applied Sciences*, *1*(6), 571-583.

Odeyemi, O., Okoye, C. C., Ofodile, O. C., Adeoye, O. B., Addy, W. A., &Ajayi-Nifise, A. O. (2024). Integrating AI with blockchain for enhanced financial services security. *Finance & Accounting Research Journal*, *6*(3), 271-287.

Ofodile, O. C., Odeyemi, O., Okoye, C. C., Addy, W. A., Oyewole, A. T., Adeoye, O. B., &Ololade, Y. J. (2024). Digital banking regulations: a comparative review between Nigeria and the USA. *Finance & Accounting Research Journal*, *6*(3), 347-371.

Olawale, O., Ajayi, F. A., Udeh, C. A., &Odejide, O. A. (2024). RegTech innovations streamlining compliance, reducing costs in the financial sector. *GSC Advanced Research and Reviews*, *19*(1), 114-131.

Onyshchenko, S., Zhyvylo, Y., Cherviak, A., &Bilko, S. (2023). Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security. *Eastern-European Journal of Enterprise Technologies*, *125*(13).

Oyewole, A. T., Okoye, C. C., Ofodile, O. C., &Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio. *World Journal of Advanced Research and Reviews*, *21*(3), 625-643.

Sari, S. R., Resmawan, R., Yahya, N. I., &Yahya, L. (2024). Implementation of cryptography using the RSA (Rivest-Shamir-Adleman) algorithm in encoding text messages and documents. *JOSTECH Journal of Science and Technology*, *4*(1), 97-107.

Sarumi, J. A., &Omotosho, O. M. A (2022). Review of network security strategies employed by the Nigerian banking sector (Case Study of Access Bank PLC, Bariga, Lagos, Nigeria).

Serrano, Manuel A., Luis E. Sánchez, Antonio Santos-Olmo, David García-Rosado, Carlos Blanco, Vita Santa Barletta, DaniloCaivano, and Eduardo Fernández-Medina. "Minimizing incident response time in real-world scenarios using quantum computing." *Software Quality Journal* 32, no. 1 (2024): 163-192.

Soesanto, E., Ningsih, N. A., Khoerunisa, L., &Faturrahman, M. I. (2023). Information data security in the use of information technology at PT Bank Central Asia (BCA). Student Research Journal, 1(3), 227-238.

Swanzy, P. N., Abukari, A. M., &Ansong, E. D. (2024). Data security framework for protecting data in transit and data at rest in the cloud. *Current Journal of Applied Science and Technology*, *43*(6), 61-77.

Tøndel, I. A., &Brataas, G. (2022, June). SecureScale: Exploring synergies between security and scalability in software development and operation. In *Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference* (pp. 36-41).

Zou, Y., Danino, S., Sun, K., &Schaub, F. (2019, May). You might' be affected: An empirical analysis of readability and usability issues in data breach notifications. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-14).