DIGITAL SECURITY ARCHITECTURE AND INFORMATION PURITANISM OF COMMERCIAL BANKS IN RIVERS STATE, NIGERIA.

Dr. Erien-naikachep Maurice Ikuru
Department of Office and Information Management
Ignatius Ajuru University of Education, Rumuolumeni Port Harcourt, Nigeria.
mauriceikuru95@gmail.com;
08064345396

ABSTRACT

This study investigated the relationship between digital security architecture and information puritanism of Commercial Banks in Rivers State. Generally, the objective of the study was to empirically examine how digital security architecture relate with information puritanism in terms of objectivity and traceability of Commercial Banks in Rivers State. The study adopted explanatory survey research design. The population of the study consisted of two hundred and thirty four (234) top managers from twenty-three (23) Commercial Banks operating in Rivers State, Nigeria, as top five 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 234 copies of the questionnaire distributed, 226 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. Four hypotheses were tested using Spearman Rank Order Correlation. The study found that: data loss prevention has a moderate positive relationship with objectivity of Commercial Banks in Rivers State; data loss prevention has a weak relationship with traceability of Commercial Banks in Rivers State; security file transfer protocol mechanism has a very strong positive relationship with objectivity of Commercial Banks in Rivers State, and; security file transfer protocol culture has a moderate relationship with traceability of Commercial Banks in Rivers State. The study concluded that advancement in data security architecture such as data loss prevention and security file transfer protocol emanate to equivalent enhancement of puritanism of informationin Commercial banks. The study recommended amongst other things that management of commercial banks and other financial organizations should bring to fore the suggested dimensions of digital security architecture to remain current on best practices and innovations, ultimately improving their firms' information credibility.

Keywords: *Digital Security architecture, Data Loss Prevention, Security File Transfer Protocol, Information Puritanism, Objectivity, Traceability.*

INTRODUCTION

Information as a veritable resource of an organization especially in the Commercial bank is often describe as a lifeblood of an organization. Information puritanism is a practice that is aims to promote a culture of integrity, accuracy, and reliability in information sharing, it seeks to combat the spread of misinformation and disinformation, foster informed decision-making, and uphold the principles of transparency and objectivity in the pursuit of reliable knowledge by implementing security controls and maintaining compliance with regulatory requirements, the architecture ensures that personal data is protected, privacy is maintained, and information is handled in accordance with legal and ethical standards.The current era is called information and communication era as many studies are conducted regarding the collection, processing and transferring information (Bahman, 1991). This study measured information puritanism with objectivity, traceability, and credibility.

Objectivity allows others to assess the credibility and reliability of the information, and, the information should be free from undue influence, conflicts of interest, or external pressures that could compromise it.

Traceability outline that the methods and procedures used to collect the data, this helps establish the validity of the information by enabling others to replicate or validate the findings.

Credibility is produced by reputable sources that have a track record of reliability and accuracy and, credible information is consistent with other reliable sources and established knowledge within the field.The management information systems increased the managers' information and even the experts of various levels of the organization and by raising new concepts not only extended their knowledge scope about what they can do and what is their decision and helped them in doing their activities and responsibilities (Jams & Kent, 2003).

Digital security architecture ensures that data remains confidential, even if it is intercepted or accessed by unauthorized parties, incident response that involves the processes and procedures in place to detect, respond to, and mitigate security incidents or breaches. It includes incident detection, analysis, containment, eradication, and recovery activities. It is important to state that proficiency in operation of this framework is vital therefore, Digital security architecture begins with the establishment of security policies and standards that outline the organization's approach to security, define roles and responsibilities, and set guidelines for secure practices. As such, the study dimentionalize digital security with, data loss prevention, secure file transfer protocol and multi-factor authentication.

Data loss prevention DLP safeguards valuable intellectual property, trade secrets, or proprietary information from being compromised or stolen, it helps prevent unauthorized disclosure or misuse of critical business assets. DLP mitigates the risk of reputational damage that can occur as a result of data breaches or unauthorized disclosures. Security file transfer protocol SFTP includes mechanisms to verify the integrity of transferred files, it uses cryptographic hashes or checksums to ensure that files have not been tampered with during transit. Also, SFTP is platform-independent and can be used on various operating systems, making it flexible for different environments, such as, remote file management allows users to perform various file management operations, including uploading, downloading, renaming, deleting, and changing file permissions on remote servers. A relevant insider threat is inadvertent disclosure of an organization sensitive data by an employee due to non-compliance of security guidelines if any or due to an employee nonchalant or careless behaviour (Wuchner & Pretschner, 2012). It is important to state that many Commercial Banks are still experiencing uncertainty in the reliability of their information system despite several research effort in the area such the works of Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Gross, et al (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes, However, none of these studies specifically mentioned digital security architecture with data loss prevention, security file transfer protocol interact with information puritanism of Commercial Banks. This gives credence to this study.

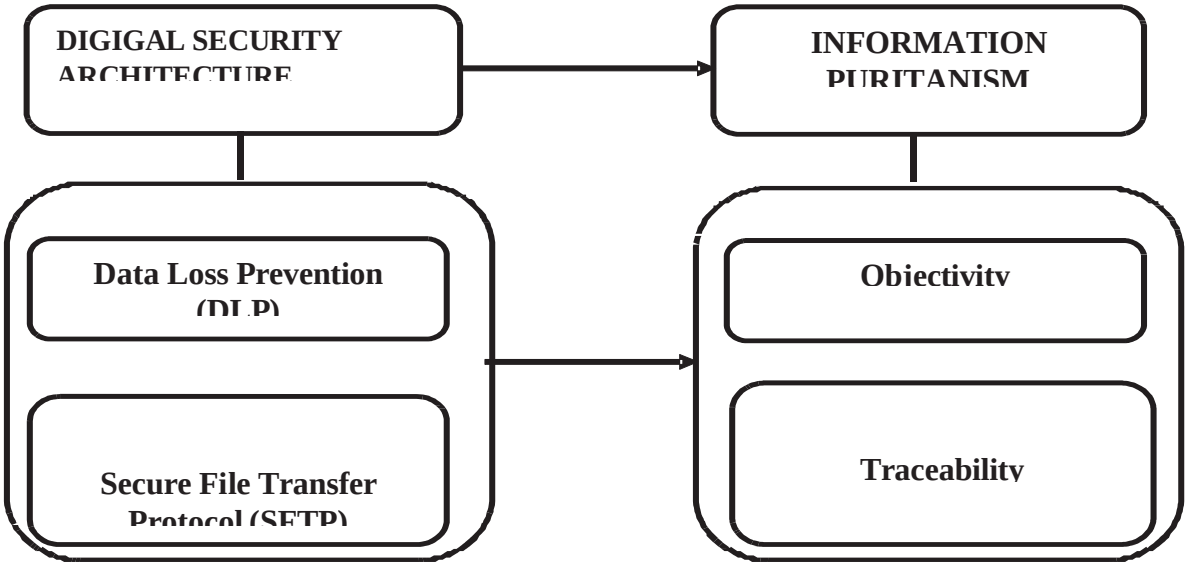

Fig. 1.1: Conceptual framework showing relationship between digital security architecture and information Puritanism of commercial banks In Rivers State.

Aim and Objectives of the Study

The aim of the study was to examine the relationship between digital security architecture and information puritanism of Commercial Banks in Rivers State. The specific objectives of the study include the following:

1. To ascertain the relationship between data loss prevention and objectivity of Banks in Rivers State.
2. To determine the relationship between data loss prevention and traceability of Commercial Banks in Rivers State.
3. To examine the relationship between security file transfer and objectivity of Commercial Banks in Rivers State.
4. To ascertain the relationship between security file transfer and traceability of Commercial Banks in Rivers State.

Digital Security Architecture

Digital security architecture refers to the design and implementation of a comprehensive framework of security measures and practices to protect digital assets, data, and systems from unauthorized access, breaches, or attacks. It involves the integration of various security components, technologies, and processes to create a robust and layered defense system. It also involves access controls which ensure that only authorized individuals or entities can access resources, systems, or data. This includes authentication mechanisms (e.g., passwords, biometrics), authorization controls, and user management practices. Because most of the architecture revolves around network in designing security architecture it is pertinent to put Network security in to consideration which involves securing the organization's network infrastructure to protect against unauthorized access, data interception, or network attacks. This can include firewalls, intrusion detection and prevention systems, virtual private networks (VPNs), and network segmentation.Trust is essential in situations where uncertainty and interdependence exist (Mayer, 1995), and thedigital environment certainly encapsulates those factors. Today's digital economy relies on an intricate,hyper-connected information and communication technology (ICT) ecosystem based on the processing oflarge streams of data (“big data”) enabled by sophisticated data analytics and the widespread use of mobile connectivity. An effective security architectures should carry data encryption that involves the use of cryptographic techniques to protect sensitive information and prevent unauthorized access. Security awareness and training programs educate employees and users about security best practices, policies, and procedures, it helps to create a security-conscious culture and reduces the risk of human error or negligence.By implementing a well-designed digital security architecture, organizations can establish a strong defense against cybersecurity threats, protect sensitive data, and maintain the integrity and availability of digital systems and assets. Digital security architecture on information puritanism is significant, as the security measures and practices implemented through the architecture directly support the principles and goals of information puritanism.

Data Loss Prevention (DLP)

Data Loss Prevention (DLP) refers to a set of strategies, policies, and technologies implemented to prevent the unauthorized disclosure, leakage, or loss of sensitive or confidential data. DLP aims to protect sensitive information from being accessed, shared, or transferred inappropriately, whether intentional or accidental more critically, DLP focuses on safeguarding sensitive data from unauthorized access, disclosure, or loss. Getting hacked is not just about losing the confidential data but losing the relationship with customers in the market (Bendovschi, 2015). It helps prevent data breaches, data theft, or inadvertent exposure by implementing controls and monitoring mechanisms which emphasize on Compliance with Regulations: DLP helps organizations comply with industry-specific regulations, data privacy laws, and contractual obligations. It ensures that sensitive data is handled and protected according to legal requirements and industry standards.By protecting sensitive data, organizations maintain trust with customers, partners, and stakeholders.

More specifically, DLP typically involves a combination of policies, procedures, and technologies to monitor, detect, and prevent data breaches. Some common components of a DLP solution include, data classification, data discovery and data monitoring. Implementing monitoring mechanisms to track data usage, access, and transfers. This includes real-time monitoring, alerting, and blocking of unauthorized activities or policy violations.By implementing a comprehensive data loss prevention strategy, organizations can minimize the risk of data loss or exposure, protect sensitive information, meet compliance requirements, and preserve their reputation.

Secure File Transfer Protocol (SFTP)

Secure File Transfer Protocol (SFTP) is a network protocol that allows for secure file transfer over a secure shell (SSH) connection. It provides a secure and encrypted channel for transferring files between a client and a server.SFTP offers several key features to ensure the security and integrity of file transfers. Today an individual can receive and send any information may be video, or an email or only through the click of a button but did s/he ever ponder how safe this information transmitted to another individual strongly with no spillage of data? The proper response lies in cybersecurity. Today more than 61% of full industry exchanges are done on the internet, so this area prerequisite high quality of security for direct and best exchanges. Thus, cybersecurity has become a most recent issue (Dervojeda, et. al., 2014). Consequently,SFTP is also designed to work well with firewalls and network address translation (NAT) devices, making it easier to deploy in secure network environments.SFTP is often preferred over other file transfer protocols, such as FTP (File Transfer Protocol), because it provides enhanced security features and encryption capabilities. It is commonly used in scenarios where secure and reliable file transfers are required, such as in corporate environments, cloud storage, and server-to-server transfers.

Information Puritanism

Information puritanism refers to a set of principles and practices that prioritize the integrity, accuracy, and reliability of information, it emphasizes the importance of presenting information in an unbiased, transparent, and evidence-based manner, free from personal opinions, biases, or distortions. The importance of information as an organizational resource has been identified by many studies (Abdul Kargbo, 2005; Akotia, 2003 ;) in order for the information to be useful and provide the needed knowledge, it has to be managed, there is enough evidence to explain that the degree of success enjoyed by an organization and its members depends largely on how well information is managed.The concept of information puritanism aims to counter the spread of misinformation, disinformation, and manipulation by promoting high standards of information quality and credibility. An information system is a collection of people, processes, data, and technology that work together to gather, store, and process, analyze, and disseminate information within an organization. It involves the use of technology and various components to manage and support the flow of information for decision-making and business operations. Information systems play a crucial role in organizations by facilitating efficient data management, supporting decision-making processes, enhancing communication and collaboration, and enabling strategic planning and analysis, they are integral to the functioning and success of modern businesses across industries. More specifically, factual accuracy, transparency and ethical responsibility Information puritanism places a strong emphasis on ensuring that information is based on verified facts. It promotes the use of reliable sources, fact-checking, and rigorous validation processes to ensure accuracy and minimize errors or inaccuracies. Consequently, information puritanism emphasizes the need for transparency in the sources, methods, and processes used to gather and analyze information. It promotes clear documentation of data sources, methodologies, assumptions, and limitations to enable users to evaluate the reliability and validity of the information, and ethical responsibility of individuals and organizations to provide accurate and reliable information, it discourages the intentional spread of misinformation, disinformation, or propaganda and promotes ethical practices in information dissemination.

Objectivity

Objectivity, in the context of information puritanism, refers to the principle of presenting information in an unbiased and impartial manner, free from personal opinions, prejudices, or subjective influences, it involves providing information that is factual, accurate, and based on evidence, without distorting or skewing it to favor a particular perspective or agenda, the focus is on maintaining the highest standards of objectivity in the dissemination and presentation ofinformation, this approach aims to ensure that information is reliable, trustworthy, and devoid of personal biases or subjective interpretations, objectivity maintain that information should be factual accuracy this means that it is based on verifiable facts and supported by evidence. In this respect, Wang (2011) argued that organizations need to treat information and its management as an imperative organizational activity that should be linked to the mission, strategy and goals of organizations. This is because information objectivity is notion for information to be free from inaccuracies, exaggerations, or distortions also, transparency and independency, the sources and methods used to gather information should be transparent and open to scrutiny. It should be produced and disseminated without bias. Adhering to these principles of objectivity, information puritanism aims to promote a high standard of integrity and trustworthiness in the information that is shared with the public. It seeks to create a foundation of reliable information for informed decision-making and discourse, free from manipulation or distortion.

Traceability

In the context of information puritanism, traceability refers to the ability to track the sources, origins, and verifiability of information, it involves providing clear and transparent documentation of the information's provenance, including the data sources, methodologies, and processes used to gather and analyze the information. Robertson (2005) explains that information management is a systematic process of collecting data from one or more sources, organizing, processing it into information, storing, and distributing the information to one or more users to help accomplish the organizational goals. The concept of traceability emphasizes the principle of source identification clearly identify the sources from which it is derived. This includes citing the authors, organizations, publications, or databases that provide the original data or information it emphases on data collection methods, data quality assurance and methodological transparency. Information should demonstrate efforts to ensure data quality, such as data validation, data cleaning, and verification processes, this helps to maintain the integrity and accuracy of the information.Information should provide a clear description of the analytical methods and techniques used to process and analyze the data. This enables others to assess the validity and robustness of the information.By emphasizing traceability, information puritanism aims to promote accountability, credibility, and trustworthiness in the information that is shared. It enables users to assess the reliability and validity of the information, make informed judgments, and engage in critical thinking. Traceability ensures that information is not just presented as isolated facts but is accompanied by the necessary context and documentation to enable users to evaluate its credibility and verifiability.

Theoritical Review

The study is anchored on Technology Acceptance Model (TAM) by Fred D. Davis (1989): this theory is an information system theory that models how users come to accept and use a technology. TAM model and provide insights into the factors that influence user acceptance and adoption of technology by understanding users' perceptions of usefulness and ease of use, as well as their attitudes and intentions, organizations can design and implement technologies that align with user preferences and drive successful adoption. The theory assumes that:

1. Perceived Usefulness (PU): Users are more likely to accept and use a technology when they perceive it to be useful in enhancing their job performance, productivity, or overall effectiveness.
2. Actual System Use (ASU): Users' actual usage of a technology is influenced by their behavioral intention and perceived usefulness and ease of use.
3. Perceived Ease of Use (PEOU): Users are more likely to accept and use a technology when they perceive it to be easy to use and require minimal effort or complexity.

Implication of this theory are users are more likely to accept and use data loss prevention measures when they perceive them to be easy to use, compatible with their needs, and effective in preventing data loss also users are more likely to accept and use secure file transfer mechanisms when they perceive them to be easy to use, reliable, and providing secure and encrypted transfer of files, consequently, users are more likely to accept and use multi-factor authentication when they perceive it to be easy to use, providing an additional layer of security, and not overly burdensome in their daily tasks, this in turn, leads to improved data protection, reduced risks of breaches and more secure digital environment.
Justification of incorporating TAM as the theoretical foundation is that, implementation of digital security architecture, organization can enhance user acceptance and adoption of the predictor's variable which are DLP, SFTP and MFA. This in turn, reinforce the principles of information puritanism by protecting objectivity, traceability and credibility of information.

Empirical Review

Piskovski et al. (2020) carried out a study to explore the problem of protecting information when attackers use indirect signs to gather valuable data. The study acknowledges that anonymization alone does not suffice in securing personal data. By leveraging information links, adversaries can re-identify depersonalized data and extract additional valuable information. The authors propose a distributed ledger architecture to register access to data containing indirect signs. This architecture allows for the identification of users attempting to recover information through indirect signs, thus enhancing information protection.

The key components of the proposed solution include a public resource for registering access facts and a mechanism for authorized users or commissions to obtain identifiers of organizations and individuals accessing the data. The distributed ledger ensures comprehensive and reliable information about data access, thereby deterring malicious activities. The study underscores the readiness of technical and theoretical bases for implementing such solutions.
Kumar & Singh (2013) conducted a study to investigate the effects of security risks on the architecture of information systems. The study qualitatively explores the relationship between security risks and architectural components, providing insights into designing secure and robust information systems. The findings suggest that addressing security risks at the architectural level is crucial for developing sound information systems. This complements Piskovski et al.'s (2020) emphasis on using advanced architectural solutions, such as distributed ledgers, to enhance information protection.

Park et al. (2000) carried out a study that review application-level security solutions designed for controlled dissemination of digital information. They identify eight security architectures based on virtual machines, control sets, and distribution styles. These architectures provide varying degrees of control and tracking capabilities for information dissemination and usage. The study highlights the need for comprehensive security architectures, which aligns with Piskovski et al.'s (2020) proposal of using distributed ledger technology for tracking data access and preventing information leakage.

DuraiPandian et al. (2006) conducted a study that discuss the importance of organization-specific security policies and internal controls to protect information against unauthorized access and misuse. They advocate for flexible, context-aware access control models that address the dynamic nature of organizational environments. This perspective supports Piskovski et al.'s (2020) approach of using a public resource and distributed ledger to register data access, thereby ensuring dynamic and context-aware information protection mechanisms.

Summary of Empirical Review and Knowledge Gap

S/N	Researcher (s)	Study Focus	Variables	Findings	Remarks: Knowledge Gap and Action
1	Piskovski et al. (2020)	Protecting information from attackers using indirect signs to gather valuable data	Anonymization, Information links, Distributed ledger architecture	Anonymization alone is insufficient; information links can re-identify data; a distributed ledger can track data access	The study of Piskovski et al. (2020) centered on protecting information attackers using indirect signs to gather valuable data. While this study focuses on digital security architecture and information puritanism of Commercial Banks in Rivers State. The current study dimensionalizes digital security architecture through Data loss prevention, secure file transfer protocol, multi-factor authentication; the study also measures information puritanism in terms of objectivity, traceability, credibility.
2	Kumar & Singh (2013)	Investigating the effects of security risks on the architecture of information systems	Security risks, Architectural components	Security risks impact architectural components; addressing risks at the architectural level is crucial for secure systems	The study of Kumar & Singh (2013) centered on investigating the effects of security risks on the architecture of information system. While this study focuses on digital security architecture and information puritanism of Commercial Banks in Rivers State. The current study dimensionalizes digital security architecture through Data loss prevention, secure file transfer protocol, multi-factor authentication; the study also measures information puritanism in terms of objectivity, traceability, credibility.

3	Park et al. (2000)	Reviewing application-level security solutions for controlled dissemination of digital information	Security architectures, Virtual machines, Control sets, Distribution styles	Identified eight security architectures with varying control and tracking capabilities	The study of Park et al. (2000) centered on reviewing application-level security solutions for controlled dissemination of digital information. While this study focuses on digital security architecture and information puritanism of Commercial Banks in Rivers State. The current study dimensionalizes digital security architecture through Data loss prevention, secure file transfer protocol, multi-factor authentication; the study also measures information puritanism in terms of objectivity, traceability, credibility.
4	Duraipandian et al. (2006)	Discussing organization-specific security policies and internal controls to protect information against unauthorized access	Security policies, Internal controls, Context-aware access control models	Emphasize the need for flexible, context-aware access control models	The study of Duraipandian et al. (2020) centered on discussing organization-specific security policies and internal controls to protect information against unauthorized access. While this study focuses on digital security architecture and information puritanism of Commercial Banks in Rivers State. The current study dimensionalizes digital security architecture through Data loss prevention, secure file transfer protocol, multi-factor authentication; the study also measures information puritanism in terms of objectivity, traceability, credibility.

Methodology

The study adopted explanatory survey research design. The population of the study consisted of one hundred and fifteen (115) top managers from twenty-three (23) Commercial Banks operating in Rivers State, Nigeria. Top five (5) top managers such as General Manager, Operations Manager, Human Resource Manager, Customer Relations Manager, and Information Technology Manager 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 "Digital security Architecture and Information Puritanism (DSAIP)" 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 115 copies of the questionnaire distributed, 95 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: Data loss prevention does not have any significant relationship with objectivity of Commercial Banks in Rivers State.

Ho_2: Data loss prevention does not have any significant relationship with traceability of Commercial Banks in Rivers State

Table 1: Correlation between Data Loss Prevention and Information Puritanism

		Predictor	**Criterion**	
		Data loss prevention	Objectivity	Traceability
Data loss prevention	Rho	1.000	.315**	.222**
	Sig.	.	.000	.000
	N	95	95	95

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

Source: SPSS Output from Field Data (2024)

Column two of table 1 above shows a correlation value of 0.315 at a significance level of 0.000 which is less than the chosen alpha level of 0.05 for the hypothesis relating to data loss prevention and objectivity. Since the significance value is less than the alpha level of 0.05, the null hypothesis (Ho_1) which states that data loss prevention does not have any significant relationship with objectivity of Commercial Banks in Rivers State was rejected. This indicates that there is a significant correlation between data loss prevention mechanism and objectivity of Commercial Banks. With a correlation value of 0.315, the result reveals that data loss prevention has a moderate positive relationship with objectivity of Commercial Banks in Rivers State. This equally implies that improvement data loss prevention brings about significant improvement in the objectivity of information in Commercial banks in Rivers State, Nigeria.

Column three of table 1 above shows a correlation value of 0.222 at a significance level of 0.000 which is less than the chosen alpha level of 0.05 for the hypothesis relating to data loss prevention and traceability.

Since the significance value is less than the alpha level of 0.05, the null hypothesis (Ho_2) which states that data loss prevention does not have any significant relationship with traceability of Commercial Banks in Rivers State was rejected. This indicates that there is a significant correlation between data prevention and traceability. With a correlation value of 0.222, the result reveals that data loss prevention has a weak relationship with traceability of Commercial Banks in Rivers State. This equally implies that increase in data loss prevention for enhanced information reliability brings about little improvement in the traceability Banks in Rivers State, Nigeria.

Ho_3: Security file transfer does not have any significant relationship with objectivity of Commercial Banks in Rivers State.

Ho_4: Security file transfer does not have any significant relationship with traceability of commercial Banks in Rivers State.

Table 2: Correlation between Security File Transfer and Information Puritanism

		Predictor	**Dependent**	
		Security File Transfer	Objectivity	Traceability
Security	Rho	1.000	.935**	.404**
File	Sig.	.	.016	.000
Transfer	N	95	95	95

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

Source: SPSS Output from Field Data (2024)

Column two of table 2 above shows a correlation value of 0.315 at a significance level of 0.00 which is less than the chosen alpha level of 0.05 for the hypothesis relating to off-the-job training and productivity. Since the significance value is less than the alpha level of 0.05, the null hypothesis (Ho_3) which states that security file transfer does not have any significant relationship with objectivity of commercial Banks in Rivers State was rejected. This indicates that there is a significant correlation between security file transfer and objective. With a correlation value of 0.935, the result reveals that security file transfer has a very strong positive relationship with objectivity of commercial Banks in Rivers State. This equally implies that increase in security file transfer brings about significant improvement in the objective of employees of commercial Banks in Rivers State.

Column three of table 2 above shows a correlation value of 0.222 at a significance level of 0.00 which is less than the chosen alpha level of 0.05 for the hypothesis relating to security file transfer and traceability. Since the significance value is less than the alpha level of 0.05, the null hypothesis (Ho_4) which states that security file transfer does not have any significant relationship with traceability of commercial Banks in Rivers State was rejected. This indicates that there is a significant correlation between security file transfer and traceability. With a correlation value of 0.404, the result reveals that security file transfer has a moderate relationship with traceability of commercial banks in Rivers State.

Discussion of Finding:

Ho_1: Data Loss Prevention and Objectivity

Result reveals that there is significant correlation between data loss prevention mechanism and objectivity of Commercial Banks. With a correlation value of 0.315, the result reveals that data loss prevention has a moderate positive relationship with objectivity of Commercial Banks in Rivers State. This equally implies that improvement data loss prevention brings about significant improvement in the objectivity of information in Commercial banks in Rivers State, Nigeria. This result is in line with the finding of Piskovski et al. (2020) which discuss the importance of securing personal data and overcoming depersonalization through information links. This aligns with the idea of maintaining objectivity in commercial banks by preventing data loss and ensuring data integrity.

Also this result aligns with the work of Kumar & Singh (2013) which highlight the impact of security risks on information system architecture, emphasizing the need for secure designs to protect data. This supports the finding that data loss prevention mechanisms can enhance the objectivity of commercial banks.

Ho_2: Data Loss Prevention and Traceability

Result reveals that there is a significant correlation between data prevention and traceability. With a correlation value of 0.222, the result reveals that data loss prevention has a weak relationship with traceability of Commercial Banks in Rivers State. This equally implies that increase in data loss prevention for enhanced information reliability brings about little improvement in the traceability Banks in Rivers State, Nigeria. This result aligns with the work Piskovski et al. (2020) which propose using distributed ledger architecture for tracking data access, which relates to traceability. This aligns with the finding that data loss prevention mechanisms improve traceability, albeit weakly. Also the work Park et al. (2000) agree with the findings above by identify security architectures to provide control and tracking capabilities for digital information dissemination. This relates to enhancing traceability through robust security measures.

Ho_3: Security File Transfer and Objectivity

Result reveals that there is a significant correlation between security file transfer and objective. With a correlation value of 0.935, the result reveals that security file transfer has a very strong positive relationship with objectivity of commercial Banks in Rivers State. This equally implies that increase in security file transfer brings about significant improvement in the objective of employees of commercial Banks in Rivers State. This result agrees with DuraiPandian et al. (2006) that discuss context-aware access control models, which ensure secure and controlled access to information. This can be linked to improved objectivity in commercial banks through secure file transfer mechanisms.

Ho4: Security File Transfer and Traceability

Result reveals that there is a significant correlation between security file transfer and traceability. With a correlation value of 0.404, the result reveals that security file transfer has a moderate relationship with traceability of commercial banks in Rivers State. This equally implies that increase in security file transfer brings about significant improvement in the traceability of data of commercial Banks in Rivers State. The result of this study agrees with Park et al. (2000) on security architectures that track digital information dissemination also supports the correlation between secure file transfer and traceability.

Conclusion

Digital security architecture plays a crucial role in supporting and enhancing information puritanism by incorporating dimensions such as data loss prevention, secure file transfer, and multi-factor authentication, these dimensions of digital security architecture directly influence the measures of information puritanism, including objectivity, traceability, and credibility. Data Loss Prevention (DLP) implemented within digital security architecture contribute to the preservation of objectivity by safeguarding the integrity and accuracy of information, by preventing unauthorized access, leakage, or disclosure of sensitive data, DLP supports the principle of presenting information in an unbiased and transparent manner, in the same vain, secure file transfer: Secure file transfer mechanisms provided by digital security architecture contribute to the traceability of information by ensuring encrypted and authenticated transfers, it enhances the ability to track the sources, origins, and verifiability of information, aligning with the goal of transparent and accountable information dissemination, consequently, multi-factor authentication (MFA): MFA, as part of digital security architecture, reinforces the credibility of information by adding an extra layer of authentication security, by requiring multiple forms of authentication, MFA strengthens the trustworthiness of information and helps prevent unauthorized access or disclosure. When digital security architecture incorporates data loss prevention, secure file transfer, and multi-factor authentication, it supports the objectives of information puritanism.

It helps maintain objectivity by preserving the accuracy and integrity of information, enables traceability by ensuring transparency and accountability, and enhances credibility by implementing robust authentication mechanisms, by integrating these dimensions into digital security architecture, organizations can foster an environment of trustworthy and reliable information that aligns with the principles of information puritanism.

Recommendations

1. Commercial banks and other financial institution should implement DLP measures, it can ensure the integrity, accuracy, and reliability of information. DLP helps prevent unauthorized access, leakage, or tampering of data, maintaining the objectivity of information.
2. Financial institutions should improvise secure file transfer mechanisms protect information from unauthorized modifications or tampering during transit, preserving its objectivity and reliability.
3. organization should culturize multiple-factor authentication as it adds an extra layer of security, reducing the risk of unauthorized access, by implementing MFA, organizations enhance the credibility of information by ensuring that only authorized individuals can access sensitive data or systems.

REFERENCE

Abdul Kargbo, J. (2005). Archives management in post-war Sierra Leone: Luxury or necessity? *Journal of the Society of Archives, 26 (2)*.

Akotia, P. (2003). Public sector records systems in Ghana: Some lessons in development management. *African Journal of Library Archives and Information Science, 13 (2)*.

Bahman, A. (1991). Plan deputy and defense and Armed forces support Ministry plan:" The management information plan of Armed forces support Ministry plan". *The Report of Systems Management and Informatics.* p. 7.

Bendovschi, A. (2015). Cyber-attacks – trends, patterns and security countermeasures. *Procedia Economics and Finance*, 24-31. doi:10.1016/S2212-5671(15)01077-

Dervojeda, K., Verzijl, D., Nagtegaal, F., Lengton, M., & Rouwmaat, E. (2014). Innovative business models: Supply chain finance. Netherlands: *Business Innovation Observatory*; European Union.

DuraiPandian, N., Shanmughaneethi, V., & Chellappan, C. (2006). Information Security Architecture-Context Aware Access Control Model for Educational Applications. *IJCSNS*, *6*(12), 197.

Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. Journal of Cybersecurity, 3(1), 49–58. doi:10.1093/cybsec/tyw018

Henczel, S. (2000). *The information audit as a first step towards.* Brighton: Special libraries association.

Jams,S & Kent,L.(2003). *Information systems in management- By E-business and internet applications.* Tehran. Negah Danesh publication.

Kumar, R., & Singh, H. (2013). A qualitative analysis of effects of security risks on architecture of an information system. *ACM SIGSOFT Software Engineering Notes*, *38*(6), 1-3.

Park, J., Sandhu, R., & Schifalacqua, J. (2000, December). Security architectures for controlled digital information dissemination. In *Proceedings 16th Annual Computer Security Applications Conference (ACSAC'00)* (pp. 224-233). IEEE.

Piskovski, V. O., Grusho, A. A., Zabezhailo, M. I., Nikolaev, A. V., Senchilo, V. V., & Timonina, E. E. (2020). Security Architectures in Digital Economy Systems. *International Journal of Open Information Technologies*, *8*(9), 48-52.

Robertson, J. (2005). Ten principles of effective information management: Step two design limited. (http//.www.steptwo.com.au/papers/kmc_effectiveim/index.html).

Wang, W. T. (2011). *Examining knowledge management during issue management: anagement Research Review, 34(4), 436-449.*

Wüchner, T., & Pretschner, A. (2012, November). Data loss prevention based on data-driven usage control. In 2012 IEEE 23rd International Symposium on Software Reliability Engineering (pp. 151-160). IEEE.