International Journal of Business & Entrepreneurship Research
ISSN: 2360-989X. Volume 14, Issue 10, (September, 2023) pages 35 – 46
DOI: 2726145237114104
arcnjournals@gmail.com
https://arcnjournals.org

Information Security Management and Organisational Agility of Deposit Money Banks in Port Harcourt, Rivers State

Omunakwe, Priscilla Obunwo
Department of Office and Information Management, Faculty of Management Sciences, Rivers State University

Abstract: *This study investigated the relationship between information security management and organisational agility of deposit money banks in Port Harcourt. The study adopted the cross-sectional research survey design. Primary data was collected using structured questionnaire. The study population comprised of 100 leaders of deposit money banks who were chosen through a census. 5 managers were surveyed from 20 branches. The study sample was 100. The hypotheses were tested using the Spearman's Rank Order Correlation Statistics. The tests were carried out at a 0.05 significance level. The findings revealed that there is a positive and significant relationship between information security management and organisational agility. Therefore, the study concludes that information security management positively enhances organisational agility of deposit money banks in Port Harcourt. Hence, deposit money banks should foster a culture of integrity from top management down to every employee. This involves promoting ethical behaviour, transparency, and honesty in all aspects of the bank's operations. A culture of integrity builds trust among stakeholders and enhances the bank's reputation. Deposit money banks should implement a robust data classification framework that categorizes information based on sensitivity. Combine this with strict access controls to ensure that only authorized personnel can access confidential data. This reduces the risk of unauthorized access and data breaches. Deposit money banks should consider adopting cloud-based solutions and hybrid IT environments to enhance scalability and availability. Cloud services can provide additional capacity during peak periods and offer built-in redundancy for critical systems.*

Keywords: *Information Security Management, Integrity, Confidentiality, Availability, Organisational agility, Innovative & Collaboration*

INTRODUCTION

In order to successfully navigate the stiff competition and remain sustainable, organisations in the 21st century are required to be able to adapt quickly to the consistent changes in their business environment, by being dynamic and agile, basically because of the unpredictable nature of businesses. Being agile means that an organisation can regularly adjust their strategies effectively to react to shifting markets, new technologies, best practices and competition. Agile organisations also focus on creating a more collaborative and innovative work environment and culture. This could mean using technologies to streamline processes or enabling cross-team collaboration for better project success. (Navaro et al., 2015) defines organisational agility (OA) as the ability of organisations to respond and adjust itself for the sudden market changes and rapid innovative behaviours in the market. Owning an agile organisation is a prerequisite and substantial to perform better in the turbulent economic environment. Organisational agility is a fundamental requirement for firms to face for the change in main production factors to achieve goals and objectives of the organisation, shareholders, employees, and other stakeholders. Thus, organisational agility

necessitates firms to quickly manage their knowledge resources to respond to the dynamic environmental conditions of the business (Theyel & Hofmann, 2020; Navaro et al., 2015). By so doing, organisational agility is recognised as a direct source of superior organisational performance. And this superior organisational performance is only sustainable when organisation's most valuable assets (information) are successfully protected from unauthorised users.

According to Nwinyokpugi & Brown (2022), Information Security Management relates to the protection of valuable assets against unavailability, loss, misuse, disclosure or damage. In this context, valuable assets are the information recorded on, processed by, stored in, shared by, transmitted from or retrieved from any medium. The information must be protected against harm from threats leading to different types of impacts, such as loss, inaccessibility, alteration or wrongful disclosure. Threats include errors and omissions, fraud, accidents, and intentional damage and these are the measures adopted by creative organizations in order to remain competitive and relevant. Information security management is a key aspect of IT governance, and it is an important issue for all computer users to understand and address. As computer systems have become more and more commonplace in all walks of life, from home to school and the office, unfortunately, so too have the security risks. The widespread use of the Internet, handheld and portable computer devices, and mobile and wireless technologies has made access to data and information easy and affordable. On the other hand, these developments have provided new opportunities for IT-related problems to occur, such as theft of data, malicious attacks using viruses, hacking, denial-of-service (DoS) attacks and even new ways to commit organized crime. These risks, as well as the potential for careless mistakes, can all result in serious financial, reputational and other damages.

Generally speaking, the business value of information security management can be calculated on the basis of risk reduction, security as a (decreasing) cost of doing business and return on investment via enhanced trust relationships and improved business opportunity. Few enterprises that have strong security will brag about it publicly. Instead, code words such as "risk" and "trust" will be used to signal superior security to markets, trading partners and customers. In any case, unsecured enterprises will face higher costs from poorly administered, expensive security programs, intellectual property losses, theft and lawsuits. Superior security is a competitive advantage, and poor security will be increasingly disadvantageous. Good security allows you to achieve a primary goal of the e-business era: reaching a greater number of customers with enhanced products and services. Information security management becomes an area of interest considering the pivotal role that information plays in the life of every organisation. Therefore, this study seeks to investigate information security management and organisational agility of deposit money banks in Port Harcourt.

THE PROBLEM

Information is a crucial organisational resource that is integral to all organisational operations; as such it must be duly protected from unauthorised users so as not to endanger the success and over all sustainability of such firms. It becomes a concern when organisational information is not protected against malicious attacks by adopting necessary information security measures needed to mitigate unauthorized access to such information. It is also a concern if the identities of information users are not authenticated before being granted access; it is also a huge source of concern when the integrity of organisational most valuable assets is not protected, neither are they made available to the right users who may need access to such information. It is also a disservice

if deposit money banks are not proactive enough to deploy necessary information security strategies capable of properly protecting their information repositories against unforeseen attacks.

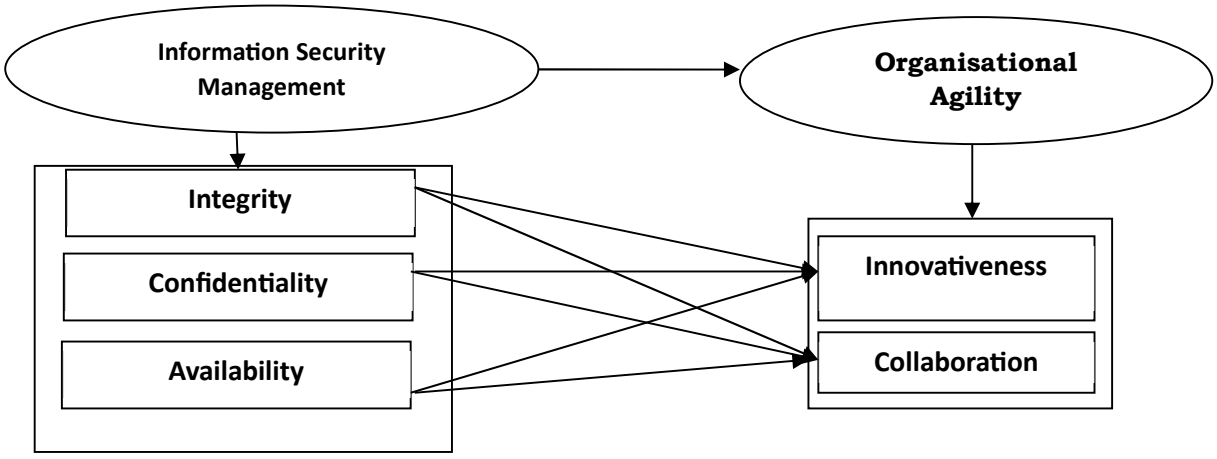

Fig.1.1: Conceptualisation of Information Security Management and Organisational Agility

RESEARCH /QUESTIONS

The main objective of this research was to investigate the relationship between information security management and organisational agility of deposit money banks in Port Harcourt. In achieving the general objective, the study specifically explored;

- The role of integrity in enhancing organisational agility of deposit money banks in Port Harcourt.
- How confidentiality enhances organisational agility of deposit money banks in Port Harcourt.
- The role of availability in enhancing organisational agility of deposit money banks in Port Harcourt.
- To what extent does integrity enhance organisational agility of deposit money banks in Port Harcourt?
- How does confidentiality enhance organisational agility of deposit money banks in Port Harcourt?
- To what extent does availability enhance organisational agility of deposit money banks in Port Harcourt?

HYPOTHESES

In order to provide answers to research questions proposed earlier, the following hypothesis are formulated to guide the study;

H_{o1}: There is no significant relationship between integrity and innovativeness of deposit money banks in Port Harcourt.

H_{o2}: There is no significant relationship between integrity and collaboration of deposit money banks in Port Harcourt.

H_{o3}: There is no significant relationship between confidentiality and innovativeness of deposit money banks in Port Harcourt.

H_{o4}: There is no significant relationship between innovativeness and collaboration of deposit money banks in Port Harcourt.

H_{o5}: There is no significant relationship between availability and innovativeness of deposit money banks in Port Harcourt.

H_{o6}: There is no significant relationship between availability and collaboration of deposit money banks in Port Harcourt.

THEORETICAL FRAMEWORK: Resource Based Theory (Jay Barney 1990)

The baseline theory associated with this study is the resource-based theory basically because the resource-based theory suggests that resource that are valuable, rare, difficult to imitate and no substitutable best position organisations for long-term success. These strategic resources can provide the foundation to develop the organisations' capabilities that can lead to superior performance over time.

INFORMATION SECURITY MANAGEMENT

Information security management, according to the International Standards Organization (ISO), is the "protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities" (ISO, 2005). Information security management, according to the National Institute of Standards and Technology's (NIST) Information Security Handbook, involves planning for and implementing a structure as well as the processes that provide for the alignment of information security strategies with business objectives and applicable laws and industry standards (Bowen, Hash, & Wilson, 2006).

The ISO Information technology security techniques; Code of practice for Information Security management (ISO, 2005) argued that information security is becoming increasingly more important for both public and private sector businesses as the interconnection of public and private networks and the sharing of information resources increase the complexity of controlling access and preserving the confidentiality, integrity, and availability of data. Jenkins (2002) noted that information that is lost or stolen often causes financial damage and may tarnish the public image of an organization. Von Solms & Von Solms (2000) believed that securing information is one of the most important aspects in any organization today and that the primary aim of information security is to protect the organization and its assets (such as sensitive information) against attempts of intrusion and corruption.

ELEMENTS OF INFORMATION SECURITY MANAGEMENT

Integrity

Integrity in the area of information flow often means that trusted output is independent from untrusted input (Biba, 2007). This is dual to the classical models of confidentiality, where public output is required to be independent from secret input. Integrity in the area of access control (Sandhu, 2004) is concerned with improper/unauthorized data modification. The focus is on preventing data modification operations, when no modification rights are granted to a given principal. Integrity in the context of fault-tolerant systems is concerned with preservation of actual data. For example, a desired property for a file transfer protocol on a lossy channel is that the

integrity of a transmitted file is preserved, i.e., the information at both ends of communication must be identical (which can be enforced by detecting and repairing possible file corruption). Integrity in the context of databases often means preservation of some important invariants, such as consistency of data and uniqueness of database keys. Sabelfeld and Myers observed that integrity has an important difference from confidentiality; a computing system can damage integrity without any external interaction, simply by computing data incorrectly. Thus, strong enforcement of integrity requires proving program correctness. Information integrity is a critical issue in information security management, and integrity policies that seek to prevent accidental or malicious destruction of information have long been recognized as important.

Confidentiality

Organisational information contains sensitive information such as patent rights, if revealed to just anyone, competitive advantage can be lost in split seconds to a competitor all because of the disclosure of information to the wrong person. As a result, organisational information has to be protected at all cost, since it is a veritable tool that drives decision making that is critical to the attainment of organisational objectives. That is why agile organisations are encourage to take full advantage of the available information security management strategies to protect organisation's most valuable assets so as to avoid the disclosure of sensitive information to malicious users or competitors.

Availability

According to (Khazanchi, & Martin, 2008), given the threat of disc operating systems (DoS), there is a growing demand to study, research and analyse availability for better understanding of "Availability as a security attribute" and also given the fact that Confidentiality and Integrity are the most researched and studied attributes of Information Security Management. The paradigm needs to change and needs a shift from a state of Sustainable Information Availability to a state of providing complete Availability, as unavailability is not an option in today's context, given the heavy dependence of modern world on information resources and the demand for expected delivery of services in a timely and a reliable manner. To achieve this, creative organizations are adopting security measures advocated by security practitioners and they need a much better understanding of Information availability and study the factors that determine availability and can influence it under certain conditions (i.e. DoS attack). This will help security practitioners analyze the impact of each factor within the context of their enterprises and determine the changes if necessary, that will achieve the goal of information availability of the organization's critical resources (logical and physical IT resources).

CONCEPT OF ORGANISATIONAL AGILITY

According to Navaro et al., (2015), organisational agility is the ability of organisations to respond and adjust itself for the sudden market changes and rapid innovative behaviours in the market. Owning an agile organisation is a prerequisite and substantial to perform better in the turbulent economic environment. Organisational agility is a fundamental requirement for firms to face for the change in main production factors to achieve goals and objectives of the organisation, shareholders, employees, and other stakeholders.

Innovativeness

Innovation is a concept with a very large applicability, whose characteristics vary based on the field of reference. According to the National Institute of Statistics (2013), innovation is an activity

resulting in a new product (goods or services) or a significantly improved one, a new process or a significantly improved one, a new marketing method or a new organisational method. Glodeanu et al. (2009) quoted the definition of innovation established by the European Union as" an accomplishment of a new idea in the current direct practice, either in a commercial manner, or in a voluntary and public sphere", by" the diffusion, assimilation and the usage of invention in different fields of the society". They continued by adding that it is accomplished either by" the transfer of existing knowledge from one field to other fields (the leverage strategy)", by" using existing knowledge to redefine what is already known (the expansion strategy)", by" creating a new field of knowledge (the accomplishment strategy)", or by" creating a new field of knowledge around a vision or a vague idea on a future field of knowledge (the experimental strategy)" (Glodeanu et al., 2009).

Collaboration

Collaboration in the workplace could be the answer to success, the key to having a homogenous environment that is putting together their ideas and thinking towards a common goal. While relying on a strong sense of shared purpose and recognising the values of working together, collaboration is about bringing two or more people (groups) together. Teamwork is simply taken to a higher level to accomplish a task, with today's advanced technologies; collaboration has become a more productive way of doing things. It enables managers and organisations to draw together the diverse skills and strengths of different individuals, to create teams that are far more effective than working alone. An effective team is able to divide and conquer to achieve their goals as quickly and effectively as possible. It also enables problems to be solved faster and more innovatively. Under a "two heads are better than one" motto, collaboration has been found to encourage job satisfaction and employee retention. Working with others in a meaningful way often gives people a stronger sense of purpose and positive reinforcement than working on their own. People are more likely to stay at an organisation if they have strong bonds with colleagues and feel they are part of something important. However, collaboration can't be forced. If individuals don't see the value in collaboration, they're unlikely to contribute to the success of the team. Organisations are structured to measure output and success at the level of individual employees. Asking someone to subordinate individual goals in favour of team goals may be seen as diluting the individual's control over their ability to performance requirements, and thus achieve individual recognition and rewards.

METHODS

The population was drawn from the leadership of deposit money banks in Port Harcourt. Five managers were chosen through a census from 20 branches, making a total of 100 respondents which also doubles as the sample, due to the focus of the study. A cross sectional survey method was adopted for the study. The content validity of the instrument was established by giving a set of the draft questionnaire to five managers involved in daily decision-making in their organisations and five questionnaires to other researchers in the specific area of executive decision-making. These executives reviewed the content of the instrument and confirmed that the items were suitable for gathering relevant data for the research study.

Data Analysis

To empirically evaluate the relationship between the predictor and criterion variables of this study (including their dimensions and measures), the spearman's rank order of correlation coefficient (RHO) was adopted. As a tool, it is considered to be more flexible and it is not limited or confined to parameters statistical assumption such as applicable in the Pearson's product moment correlation. The analysis was done using the scientific package for social sciences (SPSS) version 23 software.

We begin by showing evidence of a relationship between the variables.

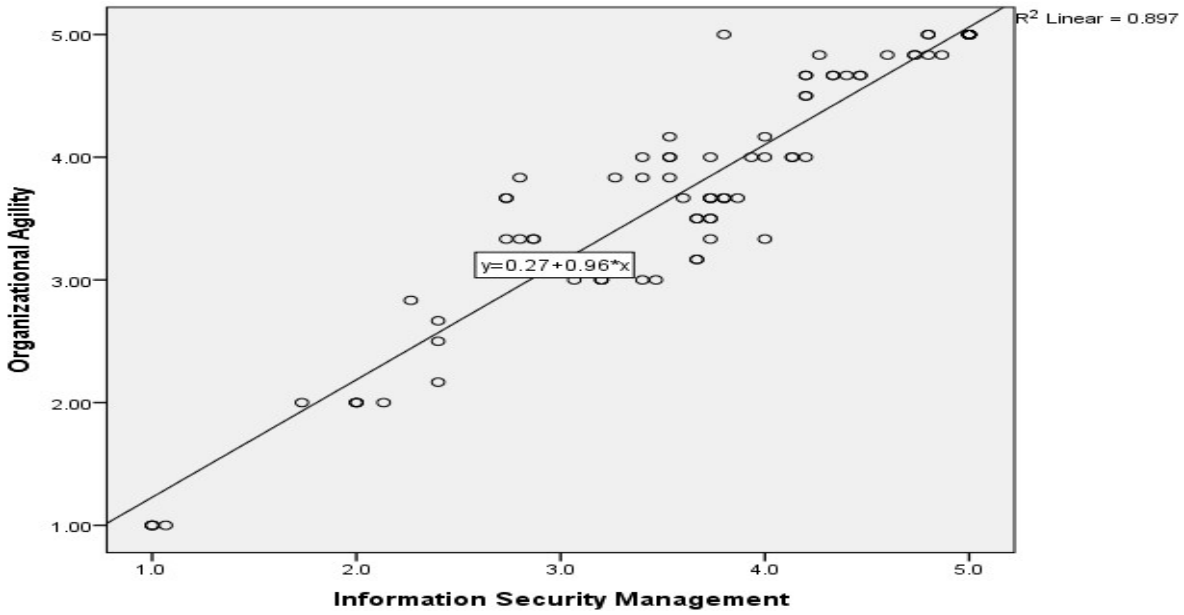

Figure 1: Scatter plot for information security management and organisational agility

Figure 1 shows a strong relationship between information security management (independent variable) and organisational agility (dependent variable). The scatter plot graph shows that the linear value of (0.897) depicting a very strong viable and positive relationship between the two constructs. The implication is that an increase in information security management simultaneously brings about an increase in the level of organisational agility. The scatter diagram has provided vivid evaluation of the closeness of the relationship among the pairs of variables through the nature of their concentration.

Table 1: Correlations for Integrity and Organisational Agility Measures

			Integrity	Innovativeness	Collaboration
Spearman's rho	Integrity	Correlation Coefficient	1.000	.829**	.744**
		Sig. (2-tailed)	.	.000	.000
		N	90	90	90
	Innovativeness	Correlation Coefficient	.829**	1.000	.764**
		Sig. (2-tailed)	.000	.	.000
		N	90	90	90
	Collaboration	Correlation Coefficient	.744**	.764**	1.000
		Sig. (2-tailed)	.000	.000	.
		N	90	90	90

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

Source: SPSS Output

Ho_1: There is no significant relationship between integrity and innovativeness of deposit money banks in Port Harcourt.

Table 1 shows a Spearman Rank Order Correlation Coefficient (rho) of 0.829 on the relationship between integrity and innovativeness. This value implies that a very strong relationship exists between the variables. The direction of the relationship indicates that the correlation is positive; implying that an increase in innovativeness was as a result of the integrity. Table 1 also shows the statistical test of significance (p-value) which makes possible the generalization of our findings to the study population. From the result obtained the sig- calculated is less than significant level ($p = 0.000 < 0.05$). Therefore, based on this finding the null hypothesis earlier stated is hereby rejected and the alternate upheld. Thus, there is a significant relationship between integrity and innovativeness of deposit money banks in Port Harcourt.

Ho_2: There is no significant relationship between integrity and collaboration of deposit money banks in Port Harcourt.

Table 1 shows a Spearman Rank Order Correlation Coefficient (rho) of 0.744 on the relationship between integrity and collaboration. This value implies that a strong relationship exists between the variables. The direction of the relationship indicates that the correlation is positive; implying that an increase in collaboration was as a result of the integrity. Table 1 also shows the statistical test of significance (p-value) which makes possible the generalization of our findings to the study population. From the result obtained the sig- calculated is less than significant level ($p = 0.000 < 0.05$). Therefore, based on this finding the null hypothesis earlier stated is hereby rejected and the alternate upheld. Thus, there is a significant relationship between integrity and collaboration of deposit money banks in Port Harcourt.

Table 2: Correlations for Confidentiality and Organisational Agility Measures

			Confidentiality	Innovativeness	Collaboration
Spearman's rho	Confidentiality	Correlation Coefficient	1.000	.814**	.847**
		Sig. (2-tailed)	.	.000	.000
		N	90	90	90
	Innovativeness	Correlation Coefficient	.814**	1.000	.764**
		Sig. (2-tailed)	.000	.	.000
		N	90	90	90
	Collaboration	Correlation Coefficient	.847**	.764**	1.000
		Sig. (2-tailed)	.000	.000	.
		N	90	90	90

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

Source: SPSS Output

H_{O3}: There is no significant relationship between confidentiality and innovativeness of deposit money banks in Port Harcourt.

Table 2 shows a Spearman Rank Order Correlation Coefficient (rho) of 0.814 on the relationship between confidentiality and innovativeness. This value implies that a very strong relationship exists between the variables. The direction of the relationship indicates that the correlation is positive; implying that an increase in innovativeness was as a result of the confidentiality. Table 2 also shows the statistical test of significance (p-value) which makes possible the generalization of our findings to the study population. From the result obtained the sig- calculated is less than significant level ($p = 0.000 < 0.05$). Therefore, based on this finding the null hypothesis earlier stated is hereby rejected and the alternate upheld. Thus, there is a significant relationship between confidentiality and innovativeness of deposit money banks in Port Harcourt.

H_{O4}: There is no significant relationship between confidentiality and collaboration of deposit money banks in Port Harcourt.

Table 2 shows a Spearman Rank Order Correlation Coefficient (rho) of 0.847 on the relationship between confidentiality and collaboration. This value implies that a strong relationship exists between the variables. The direction of the relationship indicates that the correlation is positive; implying that an increase in collaboration was as a result of the confidentiality. Table 2 also shows the statistical test of significance (p-value) which makes possible the generalization of our findings to the study population. From the result obtained the sig- calculated is less than significant level ($p = 0.000 < 0.05$). Therefore, based on this finding the null hypothesis earlier stated is hereby rejected and the alternate upheld. Thus, there is a significant relationship between confidentiality and collaboration of deposit money banks in Port Harcourt.

Table 3: Correlations for Availability and Organisational Agility Measures

			Availability	Innovativeness	Collaboration
Spearman's rho	Availability	Correlation Coefficient	1.000	.870**	.745**
		Sig. (2-tailed)	.	.000	.000
		N	90	90	90
	Innovativeness	Correlation Coefficient	.870**	1.000	.764**
		Sig. (2-tailed)	.000	.	.000
		N	90	90	90
	Collaboration	Correlation Coefficient	.745**	.764**	1.000
		Sig. (2-tailed)	.000	.000	.
		N	90	90	90

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

Source: SPSS Output

H_{O5}: There is no significant relationship between availability and innovativeness of deposit money banks in Port Harcourt.

Table 3 shows a Spearman Rank Order Correlation Coefficient (rho) of 0.870 on the relationship between availability and innovativeness. This value implies that a very strong relationship exists between the variables. The direction of the relationship indicates that the correlation is positive; implying that an increase in innovativeness was as a result of the availability. Table 3 also shows the statistical test of significance (p-value) which makes possible the generalization of our findings to the study population. From the result obtained the sig- calculated is less than significant level ($p = 0.000 < 0.05$). Therefore, based on this finding the null hypothesis earlier stated is hereby rejected and the alternate upheld. Thus, there is a significant relationship between availability and innovativeness of deposit money banks in Port Harcourt.

H_{O6}: There is no significant relationship between availability and collaboration of deposit money banks in Port Harcourt.

Table 3 shows a Spearman Rank Order Correlation Coefficient (rho) of 0.745 on the relationship between availability and collaboration. This value implies that a strong relationship exists between the variables. The direction of the relationship indicates that the correlation is positive; implying that an increase in collaboration was as a result of the availability. Table 3 also shows the statistical test of significance (p-value) which makes possible the generalization of our findings to the study population. From the result obtained the sig- calculated is less than significant level ($p = 0.000 < 0.05$). Therefore, based on this finding the null hypothesis earlier stated is hereby rejected and the alternate upheld. Thus, there is a significant relationship between availability and collaboration of deposit money banks in Port Harcourt.

FINDINGS

The result revealed that there is a positive and significant relationship between information security management and organisational agility of deposit money banks in Port Harcourt. Information security management plays a vital role in the banking sector, particularly in deposit money banks, as it ensures the protection and confidentiality of sensitive data and financial transactions. In today's digital age, where cyber threats are on the rise, it is imperative for banks to establish robust information security management systems to safeguard against potential risks and vulnerabilities. As highlighted by Adiele and Obara (2022), the integration of information security management practices with organizational agility is crucial for the effective functioning of deposit money banks. Organizational agility refers to the ability of an organization to respond quickly and effectively to changes and uncertainties in the business environment. By aligning information security management with organizational agility, banks can enhance their ability to adapt and respond to emerging cyber threats and technological advancements in a timely manner. This integration allows deposit money banks to develop agile strategies and implement proactive measures to mitigate risks, maintain customer trust, and ensure the continuity of critical banking operations. Furthermore, it enables banks to streamline their processes, foster innovation, and remain competitive in the dynamic banking landscape. Thus, the synergy between information security management and organizational agility is essential for deposit money banks to effectively address the challenges posed by rapidly evolving cyber threats and maintain a secure and resilient banking environment.

In today's digital era, organizations are increasingly recognizing the importance of information security management in fostering organizational agility. Information security management refers

to the processes and practices that aim to protect the confidentiality, integrity, and availability of an organization's information assets. On the other hand, organizational agility refers to an organization's ability to respond quickly and effectively to changes in its external environment. According to Zaini, Masrek, and Mahmood (2020), there is a positive relationship between information security management and organizational agility. This relationship can be attributed to several factors. Firstly, effective information security management ensures the protection of valuable organizational information, thus reducing the risk of data breaches and cyber-attacks. By minimizing the potential disruptions caused by security incidents, organizations can maintain their operational continuity and respond promptly to external changes. Additionally, a robust information security management system enables organizations to meet regulatory requirements and industry standards, enhancing their credibility and reputation. This, in turn, can foster trust among stakeholders and facilitate collaborations with external partners, further enhancing organizational agility. Furthermore, information security management practices, such as risk assessments and incident response planning, promote a proactive approach to identifying and mitigating potential threats. This proactive mindset is crucial for organizations to adapt to changes in the business environment and seize emerging opportunities. In conclusion, the positive relationship between information security management and o

The implications of the findings on the operations of deposit money banks in Port Harcourt are far-reaching and have significant implications for the banking sector in Nigeria. According to Nwulu and Asiegbu (2015), the study conducted in Port Harcourt revealed several important findings. Firstly, it was discovered that the level of competition among deposit money banks in the region is high. This finding suggests that banks operating in Port Harcourt need to continuously improve their products and services to stay competitive in the market. Additionally, the study found that customer satisfaction plays a crucial role in the success of deposit money banks. Banks that prioritize customer service and provide a positive banking experience are more likely to attract and retain customers. Moreover, the study highlighted the importance of technological advancements in the banking sector. It was found that banks that embraced technology and offered convenient digital banking solutions had a competitive advantage over those that did not. This finding indicates that deposit money banks in Port Harcourt need to invest in technology and innovative banking solutions to remain relevant and meet the evolving needs of their customers. Overall, the findings of the study underscore the need for deposit money banks in Port Harcourt to focus on competition, customer satisfaction, and technological advancements in order to thrive in the dynamic banking industry (Nwulu and Asiegbu, 2015).

CONCLUSION AND RECOMMENDATION

The study concludes that information security management positively enhances organisational agility of deposit money banks in Port Harcourt. By safeguarding sensitive information, protecting against cyber threats, and ensuring data integrity, banks create a solid foundation for agility in decision-making, service delivery, and customer engagement.

Therefore, based on the foregoing conclusion, the following recommendations were made:

i. Deposit money banks should foster a culture of integrity from top management down to every employee. This involves promoting ethical behaviour, transparency, and honesty in all aspects of the bank's operations. A culture of integrity builds trust among stakeholders and enhances the bank's reputation.

ii. Deposit money banks should implement a robust data classification framework that categorizes information based on sensitivity. Combine this with strict access controls to ensure that only authorized personnel can access confidential data. This reduces the risk of unauthorized access and data breaches.

iii. Deposit money banks should consider adopting cloud-based solutions and hybrid IT environments to enhance scalability and availability. Cloud services can provide additional capacity during peak periods and offer built-in redundancy for critical systems.

REFERENCE

Biba, K. (2007). Integrity considerations for secure computer systems. Technical Report ESDTR-76-372, USAF Electronic Systems Division, Bedford, MA, (Also available through National Technical Information Service, Springfield Va., NTIS AD-A039324.).

Bowen, P., Hash, J. & Wilson, M. (2006). Information Security Handbook: A Guide for Managers. National Institute of Standards and Technology publication 800-100.

Glodeanu, I., Hoffman, O., Leovaridis. C., Nica, E., Nicolaescu, A., Popescu, G., and Rașeev, S. (2009). New paradigms of innovation. Case study – the corporate university. Bucharest: Expert Publishing House.

ISO (2005). Information technology Security techniques: Code of practice for Information Security management. International Standards Organization (ISO) document. Reference number ISO/IEC 27002:2005(E).

Jenkins, G. (2002). Information Systems: Policies and Procedures Manual. Paramus, NJ: Prentice Hall

Khazanchi, D. & Martin, P. (2008). Information Availability. Handbook of Research on Information Security and Assurance. http://dx.doi.org/10.4018/978-1-59904-855-0.ch019

National Institute of Statistics (2013). Romania Statistical Yearbook 2012. Retrieved from http://www.insse.ro/cms/files/Anuar%20statistic/13/13.Stiinta,%20tehnologie%20si%20inovare_ro.pdf.

Nwinyokpugi, P. N. & Brown, M. I. (2022). Organizational Creativity: The Information Security Paradigm. International Academic and Research Consortium. Journal of Tourism and Business Management. IARJTBM: Volume-2: Issue-2

Sandhu, R. (2004). On five definitions of data integrity. In Proceedings of the IFIP WG11.3 Working Conference on Database Security VII, pages 257–267.

Theyel, G. & Hofmann, K.H. (2020). Manufacturing location decisions and organizational agility, Multinational Business Review, 29 (2), 166-188.

Von Solms, E. & Von Solms, S.H. (2000). Information Security Management Through Measurement. Norwell, MA: Kurwell Academic