Information Security and Organizational Efficiency of Deposit Banks in Port Harcourt Rivers State.

Ebikibina Tantua, PhD.

And

Princess G. James

Department of Office and Information Management

Rivers State University

Port Harcourt.

Abstract

This research examined the relationship between information security and organizational efficiency in selected Banks in Port Harcourt Rivers State. Confidentiality was conceptualized as the dimension of the independent variable while reliability and profitability were used as measures of the dependent variable while the study had technology as moderating variable. The study adopted the cross-sectional survey in its investigation of the variables. Primary source of data was generated through self- administered questionnaire. The population of the study was 120 employees of 5 selected banks in Port Harcourt. A sample of 92 respondents was calculated using the Taro Yamane's formula for sample size determination. The research instrument was validated through supervisor's vetting and approval while the reliability of the instrument was achieved by the use of the Cronbach Alpha coefficient with all the items scoring above 0.70. Data generated were analyzed and presented using both descriptive and inferential statistical technique. The findings of the study revealed that a significant relationship between information security and organization efficiency of deposit money banks in Port Harcourt. Therefore, the study recommends that the banks in Port Harcourt, Rives State should enforce proper Information security in banks in Port Harcourt Rivers State.

Key words: Information Security, organizational Efficiency

1. Introduction

Information is an essential component of organizational efficiency assets, securing the information system implies securing the assets of that organization (Bjorck, 2001). The competitive nature of businesses necessitated the proper security of organizational efficiency information or database, loosing vital information to the competitors or thief can result to total collapse of the organization. The increase in knowledge and Information Technology and its numerous users (both good and bad) of information system has been one of the major problems operating business on the internet despite its numerous advantages (Schlienger, & Teufel, 2003). The world today is a global village that has necessitated movement of businesses towards the internet, as they are now referred to as internet driven business. The benefit of operating on the internet greatly out weight the local and manual process, but one attack can totally destroy all the days harvest, that is why it is necessary to be conscious of every given situation when you are online, this called for information security. On the internet several computers are linked together, so that different database, companies, people are in constant communication with one another, so there is different behaviour and interest (good and bad) or intension, most Information Technology experts are not to improve productivity but their aim of learning is for criminal activities like the hackers. Whatever venture man go into, the greater the risk, the higher the benefit, the only solution in achieving these great benefit is how the security of information be properly enforced. Information security is a way of solving the problems of business operating online (Kruger & Kearney, 2006).Information security answered the question of business online and need to be a continued process as a result of new hijackers and new competitors. Different researcher has defined information in different concept as follows; Information is an intellectual property of an organization, it constitutes a decision process or a comprehensive decision reach by the management of the organization stored in the database of the organization(Shaw, 2010).In the banking sector, it is the unit of financial transaction, this includes

the customers' name, phone number, address, account name, account number, value or amount deposited in the bank, account type and other necessary documents that will separate one person or customers from the other. Globally, the Banking industry has undergone significant changes as a result of Information Technology and Communication (ITC). This has transformed the industry in countless ways over the past 30 years. The emergence of digital technology trends such as cloud computing, social media, big data, technology outsourcing and mobility has driven the innovativeness in operations and customer service in the Banking institutions. These trends are touted to solving the challenges of the 21st Century Bank, handling the increasing complexities of business while satisfying the customers need for convenience and to abide by increasingly complex regulatory rules. Successful Banking institutions are customer focused. The adoption of digital and mobile technology by consumers has raised the expectations to an always available, real-time, on-line customer experience across all service channels.

Today, banks are often faced with operational risk because of the high Information Technology level of these criminal, they want to force into the database of the organization, therefore there is need for improvement on the security measure to ensure people's assets are save and the business will continue to do well. Information security should be able to keep track of the sources of or possible area through which the unauthorized may plan to attack. In this respect information security is proactive, it should not allow the crime to happen but should be able to prevent it from happening. According to Singh (2009). Secured information must obey basic and sensitive properties called the triad of information security; one of which is Information confidentiality.Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred. Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information is stored in the database of the organization (Xuemei, Yan, & Lixing,2009).

One major way to measure organizational efficiency is to measure performance targets (evaluation the performance of the organization), this set the pace for effectiveness and impact metrics, it does not assume the aspects of security operation of specific level of performance (like reducing the number of virus infected computers, decreasing the amount of easy-to-guess passwords.). Its concern with organizational information security performance goals and objectives, it is expressed in the form of high level policies and requirements. Existing laws, regulations and best practices. Haven understood the basic concept of information security (Information Security Tried), this study would measure effectiveness on the level of Information security of confidentiality.

This study will also be guided by the following research questions:

i. Does information confidentiality enhance organizational efficiency in selected Banks in Port Harcourt, Rivers State?
ii. To what extent does Information integrity enhance Organizational efficiency in selected Banks in Port Harcourt, Rivers State?

The study was guided by the following hypotheses

H_{01}: Information confidentiality does not significantly influence reliability of deposit money banks in Port Harcourt, Rivers State.

H_{02}: Information confidentiality does not significantly influence profitability of deposit money banks in Port Harcourt, Rivers State.

2. Theoretical framework

The theoretical foundation of this research is embedded in the system theory. Systems theory was introduced by biologist Lvon Bertalanffy in the 1930s as a modeling devise that accommodates the interrelationships and overlap between separate disciplines. The reality is that when scientists and philosophers first tried to explain how things worked in the universe, there were no separate disciplines. There were simply questions to be answered. But as we started understanding more and more, the sciences broke down into chemistry, physics, biology, and then biophysics, biochemistry, physical chemistry, etc. so that related components of a problem were investigated in isolation from one another. The Systems Theory introduced by Lvon Bertalanffy reminds us of the value of integration of parts of a problem. Problems cannot be solved as well if they are considered in isolation from interrelated components. An enormous advantage systems analysts have in knowing the definitions of systems theory is that they present us with ideal guidelines for our initial familiarization with a new problem, which of course is a new system. A system is a set of related components that work together in a particular environment to perform whatever functions are required to achieve the system's objective.Information security is classified into part of a system that human, and machine interact to achieve a definite objective.

2.1. Information Security

In general, security is "the quality or state of being secured from unauthorised users of the information system, or to be free from danger (Xuemei, Yan & Lixing,2009). It is the protection of organizational assets (digital asset) against adversaries, from those who would do harm, intentionally or otherwise. For example it is the objective of the National security of a state to protect its citizenry from any external attack or harm (Mathisen 2010). The security department protects the sovereignty of a state, its assets, its resources, and its people. Achieving the appropriate level of security for an organization also requires a multifaceted system, the software, the hardware and the user cooperative to achieve the same goal (Bazzina, 2006). For an information system to be successful, the following multiple layers of security is put in place to protectits operations:

- Physical security, to protect physical items, objects, or areas from unauthorized access and misuse
- Personnel security, to protect the individual or group of individuals who are authorized to access the organization and its operations
- Operations security, to protect the details of a particular operation or series of activities
- Communications security, to protect communications media, technology, and content
- Network security, to protect networking components, connections, and contents
- Information security, to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology.

2.2. Information Confidentiality

The development of a computer system borrowed its knowledge from the human behaviour, confidentiality does not means the denied of access, but the right person having access to the right information. Confidentiality is upheld when the assurance of accuracy and reliability of information and systems is provided and unauthorized modification is prevented(Oscarson 2003). Some information is more sensitive and requires a higher level of confidentiality. Control mechanisms need to be in place to dictate who can access data and what the user can do with it once they have accessed it. These activities need to be controlled, audited and monitored (Kraus 2010).For example, financial information (record), criminal records, source code of programme (the source code of programmes are the procedure and process written by the programmer), trade secrets and military tactical plans can be termed confidential, they can only be access by the right users.Various security mechanisms that provide confidentiality are encryption, logical and physical access controls, transmission protocols, database views andcontrolled traffic flow. Confidentiality can also counteract identity theft where one individual misrepresents himself as another, usually for fraudulent financial gain. Thus confidentiality of data or systems covers the processes, policies and controls employed to protect information of the system and the institution against unauthorized access or use (Kraus 2010).

3. Organizational efficiency

Efficiency measures relationship between inputs and outputs or how successfully the inputs have been transformed into outputs (Low, 2000). To maximize the output Porter's Total Productive Maintenance system suggests the elimination of six losses, which are: (1) reduced yield – from start up to stable production; (2) process defects; (3) reduced speed; (4) idling and minor stoppages; (5) set-up and adjustment; and (6) equipment failure. The fewer the inputs used to generate outputs, the greater the efficiency. According to Pinprayong and Siengthai (2012) there is a difference between business efficiency and organizational efficiency. Business efficiency reveals the performance of input and output ratio, while organizational efficiency reflects the improvement of internal processes of the organization, such as organizational structure, culture and community. Excellent organizational efficiency could improve entities performance in terms of management, productivity, quality and profitability. The Pinprayong and Siengthai (2012) introduced seven dimensions, for the measurement of organizational efficiency:

- Organizational strategy
- Corporate structure design;
- Management and business system building;
- Development of corporate and employee styles;
- Motivation of staff commitment;
- Development of employee's skills;
- Subordinate goals.

Effectiveness and efficiency are exclusive, yet, at the same time, they influence each other; therefore it is important for management to assure the success in both areas. Pinprayong and Siengthai (2012) suggest that ROA is a suitable measure of overall company performance, since it reveals how profitable organizations assets are in generating revenues

Organizational performance = effectiveness x efficiency;

$$\therefore Efficiency = \frac{Organizational\ \ performance}{Effectiveness}$$

Total asset turnover ratio measures the ability of a company to use its assets to efficiently generate sales; therefore it can be treated as efficiency. Profit margin ratio is an indicator of a company's pricing strategies and how well it controls the costs, also it is a good measure for benchmarking purposes; therefore it could be treated as effectiveness. As a result, overall performance can be measured by quantifying the efficiency and the effectiveness. Efficiency is all about resource allocation across alternative uses (Kumar and Gulati, 2010). It is important to understand that efficiency doesn't mean that the organization is achieving excellent performance in the market, although it reveals its operational excellence in the source of utilization process.

In much of the open literature over the last four decades, efficiency has typically been defined using data envelope analysis, subset of firms within an industry which have the "best" output-to-input ratios (i.e.,best productivity) define a data frontier, as exemplified by the dashed green line. Organizations can be managed effectively, yet, due to the poor operational management, the entity will be performing inefficiently (Karlaftis, 2004). Inefficient and ineffective organization is set for an expensive failure. In such case there is no proper resources allocation policy and there is no organizational perspective of their future. Organization has leadership issues, high employee turnover rate and no clear vision where the organization will be standing tomorrow. If the organization is able to manage its resources effectively, yet it does not realize its long term goals, it will bankrupt slowly. This strategy is cost efficient but it is not innovative and creates no value. Management has no clear customer oriented policy set in place, which leads to constant focus on efficiency. Such organization uses all its efforts to implement strict resource allocation policy, which translates into strict staff cost control, training cost reduction or even elimination. These actions lead to low morale of the organization high turnover rate of the employees and low customer satisfaction. Efficient but ineffective organization cannot be competitive and it will bankrupt eventually.

3.1 Information security and banks profitability

In today's business environment, information systems (ISs) are an absolute necessity in order for companies to attain strategic goals and improve organizational profitability (Jeong & Stylianou,2010). The United States (U.S.) Department of Commerce, National Institute of Standards and Technology (NIST) defines IS as a set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. There are costs associated with managing IS including security, storage, and retrieval therefore ongoing IS investments are required (Kendall & Kendall, 2008). Investments refer to expenditures to acquire property, equipment or other capital assets intended to produce revenue or to an investment ofeffort and time on the part of an individual who wants to reap profits from the success of his labor (Siegel & Shim, 2010).IS investments have dramatically affected the U.S. banking industry (Howell & Wei, 2010). The U.S. banking industry was one of the first to adopt Internet technologies and innovate with online brokerage, banking, and mortgage lending (Zhu, Kraemer, Xu, & Dedrick, 2004). At the time of their introduction online banking services, commonly referred to as electronic or ebanking services, were primarily developed and implemented by banks to integrate older IS banking operations with newer information technologies such as the Internet in order to deliver innovative online banking services to customers (Liao & Wong, 2008).

Over time information systems and technologies have transformed the structure of banking transactions and fundamentally altered the way banks conduct business since less physical money is used on a daily basis and instead, financial transactions are increasingly conducted virtually through a combination of devices ranging from e-banking servers and public and private networks to personal computers (PCs) and smart phones (Howell & Wei, 2010).Financial institutions around the globe know they must proactively work to protect customer dataand transactions as well as their own IS assets (Ifinedo, 2008). To ensure a secure e-banking environment, rigorous measures must be implemented including the restriction of unauthorized access, the control of allowable transactions, and the protection of online data, which are all required (Liao & Wong, 2008). Implementing protective measures intended to detect and prevent security breaches, guard against vulnerabilities, and manage online attacks create new costsitems in IS budgets (Anderson & Choobineh, 2008).IS security is no longer just good business practice, it is also a legal obligation (Smedinghoff,2007). The banking industry is one of the most highly regulated industries in the U.S. with approximately 4,000 federal, state, and local laws as well as regulations that must be followed when managing electronic records (Burns & Peterson, 2010). Laws and regulations impose requirements on IS business practices, products, as well as services to achieve goals such asprivacy, safety, and accessibility (Breaux, Anton, Boucher, & Dorfman, 2009).

Firms that comply with regulatory requirements generally experience improvements in IS security and, thereby, reduce their risk posture. NIST defines IS security as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality**.** Further, IS security is a dynamic process that must be proactively managed for an organization to effectively identify and respond to new system threats and vulnerabilities. These activities ensures that profit is generated because of the reduction in risk that would have cost the banks in huge amount of money(Gant, 2009).

From the foregoing point of view, we hereby hypothesized thus:

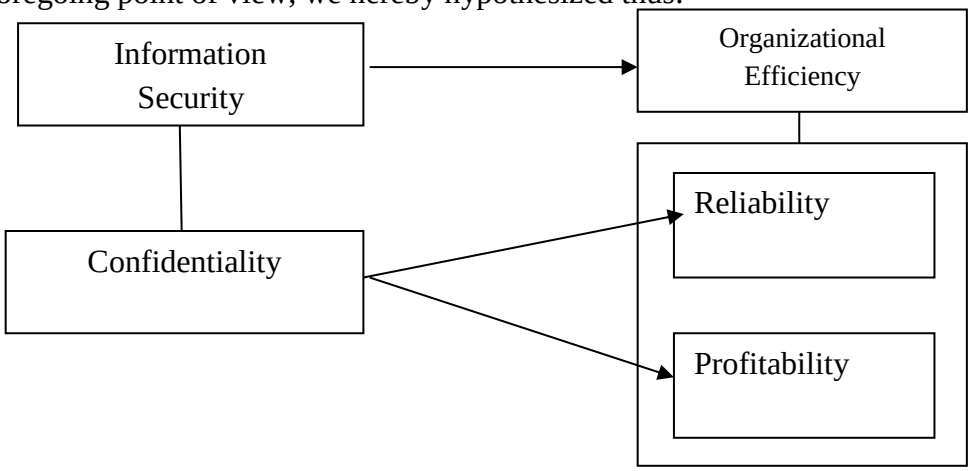

Figure 1: Conceptual framework depicting information security and organizational efficiency
Source: Researcher's Conceptualization, 2018.

4. Methodology

The study used a cross-sectional design. The population of this study consists of one hundred and twenty (120) respondent randomly selected from the five banks in Port Harcourt, Rivers State. The respondent comprises of management staff, senior staff, and junior staff of the five selected banks. The sample size for the study therefore was 92. The sampling technique applied in selecting a sample in this study was the purposive sampling in which every member has an equal chance of being selected. Descriptive statistics and Spearman Rank Order Correlation Coefficient for data analysis and hypothesis testing with the help of the SPSS version 23 package.

5. Results and Discussions

Bivariate Analysis

Data analysis was carried out using the Spearman rank order correlation tool at a 95% confidence interval. Specifically, the tests cover a Ho1 hypothesis that was bivariate and declared in the null form. We have based on the statistic of Spearman Rank (rho) to carry out the analysis. The level of significance 0.05 is adopted as a criterion for the probability of accepting the null hypothesis in (p> 0.05) or rejecting the null hypothesis in (p <0.05).

Table 1Relationship between Confidentiality and Reliability

			Confidentiality	Reliability
Spearman's rho	Confidentiality	Correlation Coefficient	1.000	.398**
		Sig. (2-tailed)	.	.000
		N	80	80
	Reliability	Correlation Coefficient	.398**	1.000
		Sig. (2-tailed)	.000	.
		N	80	80

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

Source: Research Data 2018, (SPSS output version 23.0)

Table 1 shows the Spearman's correlation coefficient; r = 0.388**, indicating a weak positive relationship between Confidentiality and Reliability of banks in Rivers State. The result is statistically significant with Probability Value *(PV)* = 0.000< 0.05 at 95% Level of Freedom. Therefore, increasing the level of Confidentiality will also increase reliability of banks in Rivers State.

Decision Rule:

Reject $H_{01:}$ Accept H_{A1}:

H_{A1}: There is a positive relationship between Confidentiality and Reliability of banks in Rivers State

Table 2: Relationship between Confidentiality and Profitability

			Confidentiality	Profitability
Spearman's rho	Confidentiality	Correlation Coefficient	1.000	.423**
		Sig. (2-tailed)	.	.000
		N	80	80
	Profitability	Correlation Coefficient	.423**	1.000
		Sig. (2-tailed)	.000	.
		N	80	80

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

Source: Research survey, 2018

Table 2 shows the Spearman's correlation coefficient; r = 0.423**, indicating a weak positive relationship between Confidentiality and Profitability of banks in Rivers State. The result is statistically significant with Probability Value *(PV)* = 0.000< 0.05 at 95% Level of Freedom. Therefore, increasing the level of Confidentiality will also increase Profitability of banks in Rivers State.

Decision Rule:

Reject $H_{02:}$ Accept H_{A2}:

H_{A2}: There is a positive relationship between Confidentiality and Profitability of banks in Rivers State

6. Discussion of findings

The findings of this research shows that there is a positive relationship between Information Security and Organizational Efficiency of Banks in Rivers State. This support the work of Mathisen (2010) that Information Security is the protection of organizational assets (digital asset) against adversaries, from those who would do harm and also by Bazzina (2006) that achieving the appropriate level of security for an organization also requires a multifaceted system, the software, the hardware and the user cooperative to achieve the same goal. According to Oscarson (2003) Confidentiality is upheld when the assurance of accuracy and reliability of information and system is provided and unauthorized modification is prevented. This means that for banks to make profit, financial information needs to be keep confidential. This means that the confidentiality of data or system covers the processes, policies, and control employed to protect information the system and the institution against unauthorized access as stated by Kraus, (2010).

7. Conclusion and Recommendation

The descriptive statistics, bivariate relationship and the multivariate relationship, the results obtained were adequate considering the tools that was use in the process of analysis. The reliability study also shows that that the dimension were adequate and for the study. The statistical analysis results were all above the criterion mean of 2.50 for a four point Likert scale and the Spearman's Correlation Coefficient were all positively correlated. Base on the analysis, we therefore conclude

that Confidentiality is adequate to increase Organizational Efficiency (Reliability and Profitability). The researcher has shown that Information Security enhances Organizational Efficiency of Banks in Rivers State. Increasing Information Security with the aid of Technology will also increase Organizational Efficiency which is Reliability and Profitability.

Based on the findings obtained from summary of discussion and empirical findings the following recommendations are made:

1. Management of organization should endeavor to always provide warning before initiating disciplinary action on wanting employees. An offense should be state din clear terms instead of reciting company's regulation.

2. There is a need to encourage seminar and workshop so that to educate the employees about disciplinary issues as well as employees commitment on the successfulness of the organization. The seminars will help the employees to improve their performance and reduce the issues of reprimands.

References

Bazzina, M. (2006). Security Standard and Support System Report. A Collaborative Project review, the Commonwealth Attorney-General's Department and Standards Asustralia, NSW; Standard International.

Björck F (2001). *Security Scandinavian Style: Interpreting the Practice of Managing Information Security in Organisations*. Licentiate Thesis, Department ofComputer and Systems Sciences, Stockholm University/Royal Institute of Technology, Stockholm

Breaux, T., Anton, A., Boucher, K., & Dorfman, M. (2009). IT compliance: aligning legal and product requirements. *IEEE IT Professionals, 11*(5), 54-58.

Bazzina , M . (2006) Security Standards and Support Systems Report: A Collaborative Project Between the Commonwealth Attorney-General's Department and Standards Australia . Sydney, NSW: Standards Australia International .

Burns, R., & Peterson, Z. (2010). Security constructs for regulatory-compliant storage. *Communications of the ACM, 53*(1), 126-130.

Bazzina , M . (2006). Security Standards and Support Systems Report: A Collaborative Project Between the Commonwealth Attorney-General's Department and Standards Australia . Sydney, NSW: Standards Australia International .

Callahan, M. (2008). The weakest link in protecting corporate data. http://www.prosecurityzone.com

Gant, D. (2009). Obligation vs. opportunity. *Risk Management, 56*(7), 58-60.

Howell, J., & Wei, J. (2010). Value increasing model in commercial e-banking. *The Journal of Computer Information Systems, 51*(1), 72-81.

Ifinedo, P. (2008). IS security and privacy issues in global financial services institutions: Do socio economic and cultural factors matter? *Proceedings of the IEEE Sixth Annual Conference on Privacy, Security, and Trust,* Canada: 75-84.

Kruger, H. & Kearney, W. (2006). A prototype for assessing information security awareness. Computers & Security, 25(4), 289 – 296.

Liao, Z., & Wong, W. (2008). The determinants of customer interactions with Internet-enabled e-banking services. *Journal of the Operational Research Society, 59*(9), 1201-1210.

Mathisen, J. (2010) Measuring information security awareness - a survey showing the Norwegian way to do it. Master's thesis, Gjøvik University College.

Siegel, J., & Shim, J. (2010). Accounting handbook. New York: Barron's Educational Series, Inc

Singh, S(2009) Database systems: Concepts, Design and applications New Delhi: Pearson Education India

Shaw, R. S., Chen, C. C., (2009). The impact of information richness on information security awareness training effectiveness. *Computer. Education.*, 52, 92–100.

Schlienger, T. & Teufel, S. (2003). Analyzing information security culture: increased trust by an appropriate information security culture. In Database and Expert Systems Applications, Proceedings. 14th International Workshop, 405 – 409.

Smedinghoff, T. (2007). Where we're headed: New developments and trends in the law of information security. *Privacy & Data Security Law Journal*, *2*(2), 103-138.

Tiwari, R., Buse, S.& Herstatt, C. (2006).Customer on the move; Strategic Implication of Mobile Banking for Banks and Financial Enterprises. E-Commerce Technology.

Xuemei, L., Yan, L., & Lixing, D. (2009). Study on information security of industry management. In Information Processing,. APCIP, Asia-Pacific Conference, 1, 522 –524.

Zhu, K., Kraemer, K., Xu, S., & Dedrick, J. (2004). Information technology payoff in e-business environments: An international perspective on value creation of e-business in the financial services industry. *Journal of Management Information Systems*, *21*(1), 17-54.