IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 6)
Available online at: www.ijariit.com

Security risk assessment in pension fund administration using ARM as a case study

Samuel
prideofsani@gmail.com
Federal University of Technology, Minna, Nigeria

J. A. Ojeniyi
ojeniyija@futminna.edu.ng
Federal University of Technology, Minna, Nigeria

M. Olalere
morufu.olalere@futminna.edu.ng
Federal University of Technology, Minna, Nigeria

S. M. Abdulhamid
shafii.abdulhamid@futminna.edu.ng
Federal University of Technology, Minna, Nigeria

ABSTRACT

In the current age of information systems, computers and related technologies have become inevitable to business. Financial institutions are among the top sectors that rely heavily on information systems for ease of operation. Information security comprises of risk assessment and risk management which plays a vital role in identifying risk, threats, and vulnerabilities. This paper makes an attempt to perform an assessment on risk management in Pension Fund Administrators (PFA); a subsector of the financial institution. This study used a survey method to actually assess the risk that PFA customers are actually exposed to. In this study, we focused on only one PFA which is ARM Pension.

Keywords— *Pension fund administration, Risk assessment, Risk management, Information security*

1. INTRODUCTION

Information technology has witnessed enormous growth globally and its application can be seen in various fields ranging from the health sector, educational sector, financial sector, and the transportation sector and so on. Nigeria with a population of over 190 million has tapped into this advancement in technology with significant growth witnessed in web and mobile application, especially in the financial sector. With a population of over 190 million, about 108 million belong to the working for and 60 million of these workable categories are employed either in the private and public sector.

According to pension reform act 2014, every Nigerian that is employed within the public and private sector is required to have a Retirement Savings Account (RSA). This is to be handled by Pension Fund Administrators (PFA) governed by the Pension Commission (PENCOM) thereby making the industry classified under the financial sector. The pension industry has witnessed significant growth over the years with about 21 pension administrators licensed in Nigeria and this has made them rely heavily on information technology in order to meet up with customer satisfaction. Amongst some of the technology used to enhance services rendered is the use of web and mobile application which opened the PFA to an attack surface area. Implementing and deploying information technology solutions in the pension industry requires a risk and threat assessment on various components that support the operation of the organization.

The aim of this paper is to identify the risk in which a Pension Fund administrator may encounter, determine what level of impact the risk will have and calculate the probability of the risk data collected.

The scope of this paper is limited to just a single pension administrator. The preferred choice of PFA is ARM Pension which is amongst the first PFA’s licensed by the National Pension Commission in December 2005. It is a subsidiary of Asset and Resource Management Company Limited.

2. RELATED WORKS

(Anthony, 2008) published an article titled “Risk management in pension fund administration in Nigeria”. His publication took a critical look into different types of risk that are peculiar to the pension fund industry. He classified the types of risk into three (3) types which are: Financial and Non-Financial risk which may or may not involve financial loss, Static and Dynamic risk and lastly, fundamental and particular risk. He reviewed the work of (Emmeth & Therese, 2003) where risk management was defined as a scientific approach to the problem of pure risk facing the firm or organization. A systematic approach was revealed in his article as a way in which risk can be identified in the pension industry. The systematic approach can be achieved by considering what risk the organization faces on a micro and macro front.

The study of (Kiran, Srivatsava, & Devi, 2014) on risk management in mobile banking gave an insight into the insecurity in mobile banking. Technology has grown over the years and one major sector that has experienced this tremendous growth in the banking sector. The banking sector has witnessed fundamental growth in mobile banking and millions of already using a wide array of mobile devices for banking. Their study focused on risk analysis and management of mobile devices used for banking identifying a key security risk that contributes to the insecurity of mobile banking. One of the major challenges perceived in the adoption of mobile banking technology and services is the perception of insecurity. Among some of the identified security risks are:

(a) Mobile device and application vulnerabilities b. Privacy
(b) Wireless carrier
(c) Payment technology

(Shehu, 2011) in his publication tried to unravel the multifarious that were contained in pension fund investment. His work revealed two major risks: financial market-related risk and non-financial market-related risk. He explained that the pension industry has witnessed incessant reforms globally with many countries shifting from government managed pension to the privately managed pension system. He went further to point out that a paradigm shift has occurred in the way to view risk management. The trend is to take a holistic view of risk management. There is no doubt that every investment is associated with risk and these risk need to be analyzed. He categorized the risk of security into two: systematic risk which is caused by overall market risk such as changes in the economy, stock market crash, exchange rate fluctuation and so on. Unsystematic risk caused by factors unique to a particular company such as strikes. He concluded by recommending that Pension companies should establish an Enterprise Risk Management (ERM) unit to evaluate risk and reduce the amount of risk.

(Chornous & Ursulenko, 2013) wrote an article titled "Risk management in banks: New approaches to risk assessment and information support" analyzes the characteristics of banking risk, the main methods of assessment used in practice. Their study was aimed at improving banking risk management taking into account new regulatory and technological requirements. They proposed new perspective approaches to assessment based on the most modern methods of data analysis.

3. METHODOLOGY

To obtain first-hand information on pension account owners and their experiences in Nigeria, primary data were collated. In total, 50 questionnaires were distributed. 45 were returned. Some of the questionnaires were not filled due to the fact that those who received it don't have a Retirement Savings Account with any Pension Fund Administrators.

3.1 Data analysis procedure

For the purpose of analysis, descriptive statistics were applied and data gathered. The descriptive statistics helps to summarize the samples, present qualitative description in a manageable form and describe the basic features relating to data in the study (Descriptive Statistics, n.d 2014). Information from the descriptive data analysis is presented in pie charts.

3.2 Research instrument

The primary data were collected through the use of questionnaires. This method was selected based on the reason that it is cheap. It allows respondent to provide the necessary information with minimum coercion and lastly because it allows the respondent to provide answers at their convenience.

An online survey was created based on the practical threat assessment model to identify potential entry point, assets and risk factors that may affect the Pension Fund Administrator. ARM pension was used as a case study in this paper. Respondents from various age groups were sent the survey in order to get their feedback. Link to survey: *https://goo.gl/forms/41yacOHhHBabGcfF3*

4. RESULTS AND DISCUSSION

The analysis of data relating to this work was carried out on data emanating from the survey conducted.

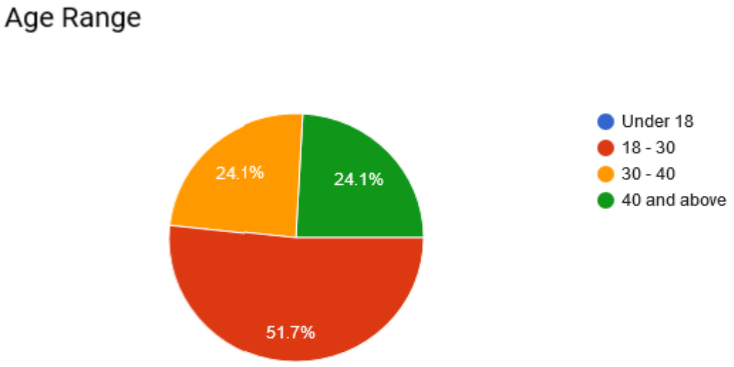

Fig. 2: Age groups

From the chart above it can be seen that majority of those that took part in the survey and have a Retirement Savings Account (RSA) are those within the age range of 18 – 30 with a total of 51.7%. This is due to the fact that the current pension reform act mandates employees to register their employers with a PFA. It is therefore observed that there is a tie in the percentage of those in the last two categories. This could be seen as a result of those that were employed prior to the new reform act especially those within the private sector

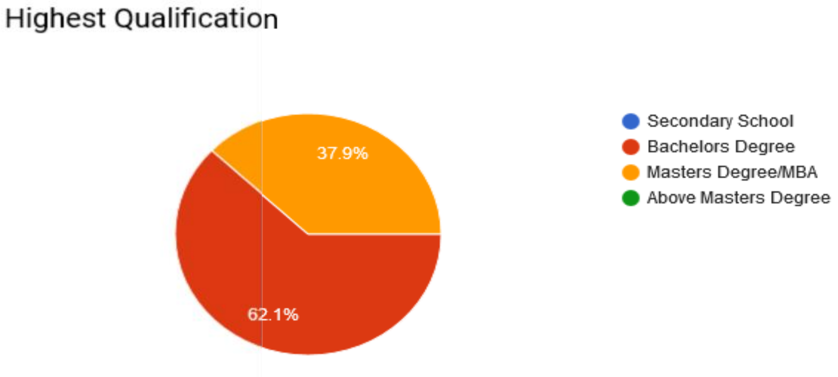

Fig. 3: Educational qualification

The survey recorded those with bachelors' degree as being the highest respondents having retirement savings account making a total of 62.1%. Following closely are those with Master's degree/MBA with 37.9%. However other categories were not captured due to the limited number of questionnaires supplied to respondents that may belong to other categories in this section.

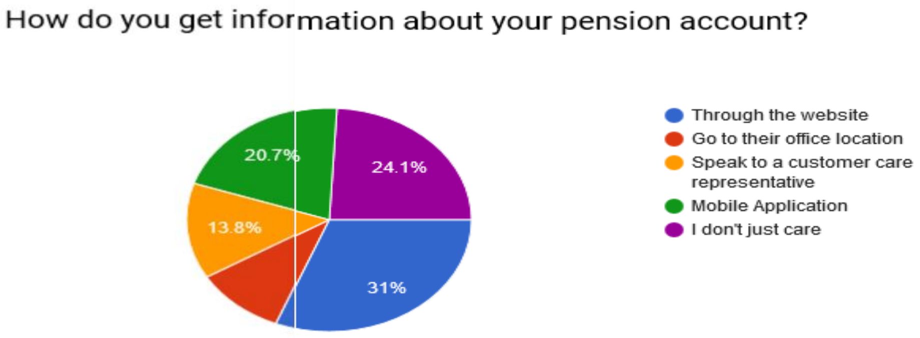

Fig. 4: Customer interactions with PFA

From the chart above, 31% admitted that the use their PFA's web application to find out what they need to know about the retirement savings account. This could be in the form of checking the last amount remitted, the last contributor, the total amount saved in your account, personal information. Having such a platform open a window for an attack surface area either on the client end or server side. This calls for a need to carry out a risk assessment on PFA's infrastructure to safeguard their assets from threats. The likelihood of cyber-attacks, disasters disrupting business services is high. 24.1% pension account owners admit to not care about their savings account and therefore may not be aware if their PFA's have suffered an attack. It is, therefore, the responsibility of the PFA to ensure that their customer's data and records are safeguarded at all cost. 20.7% of the respondents admitted to having their PFA's mobile application installed on their Phones for ease of accessing their accounts. The last categories which make up about 13.8% prefer to speak to a customer representative about anything they wish to inquire.

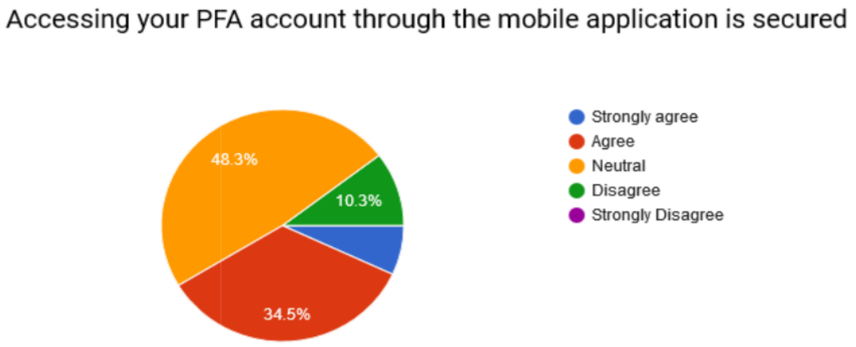

Fig. 5: Mobile Pension Users

The survey question above aimed to determine the perception of users who access their RSA using their PFA's mobile application. 48.3% admit that they neither agree nor disagree to the security of their mobile application. What risk does this pose compared to the overall security of the asset that supports this service and how well is this asset secured to ensure that the personal information of the end user is not at risk. This led to the survey question that seeks to know if the PFA's enable two factor authentication (2FA) on their mobile application for an added layer of security the result was surprising as 48.3% responded that 2FA was not enabled on the mobile application and 44.8% admitted that they have no idea what 2FA means. This means that risk due to hackers or unauthorized access is likely.

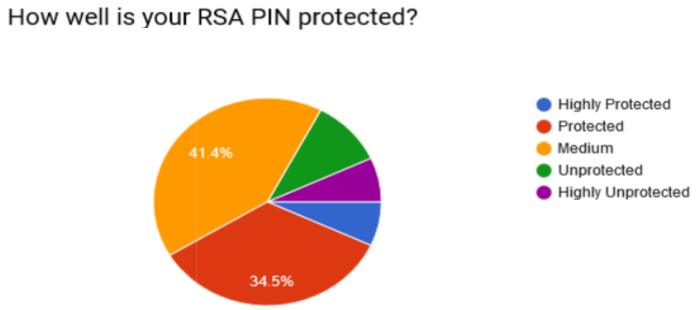

Fig. 6: Retirement Savings Account Personal Identification Number

RSA PIN is a uniquely generated pin for any pensioner who has an account with a PFA. This PIN is required before you can log in and access your dashboard using the website or the mobile application which means if it falls in wrong hands; it's an easy access to your account. The survey reported that 34.5% reported that their RSA PIN is highly protected while 41.4% suggests that their RSA PIN is moderately protected. With this result, the conclusion drawn is that the risk due to confidentiality is LOW.

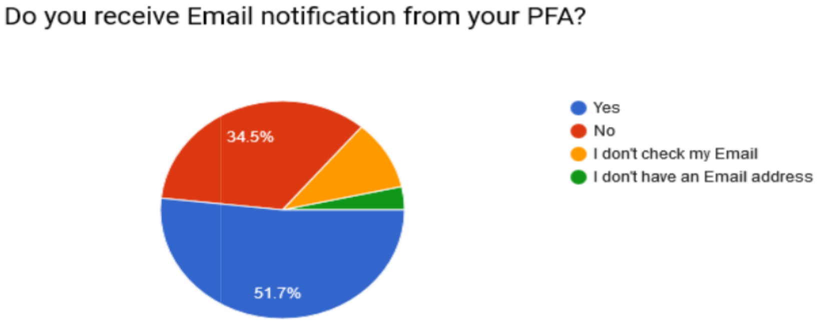

Fig. 7: Email notifications

Social engineering has been one of the most successful forms of attack that cyber criminals use today. Email service is a medium which they leverage to perpetrate their act. The survey aimed at identifying how many users receive email notifications from their PFA. The result shows that more than half the sample population receive notification via email and 34.5% said they do not receive email notifications. Email spoofing could be used to send malicious emails to specific PFA users upon successful compromise on the web server which could reveal email Ids of those registered demanding vital information from them of tricking them to install malware. The risk associated with this type of attack is high and can be possibly mitigated by enforcing adequate security measures on the web server.

Table 1: Summary of the Risk Assessment of PFA

Survey question	Response	Likelihood	Risk	Possible remediation
Customer's Interaction with PFA	31% of the 50 respondents reported that they use their PFA's website. 24.1% responded that they didn't care about their PFA after opening an account. 20% have their PFA's mobile application and 13.7% still prefer to speak to their customer representative.	MEDIUM	The risk of cross-site scripting could be used against users of the website to provide false data. User input which is not properly sensitized could lead to SQL injection attack and access into the database.	Quite a number of customers are found to be using the website to interact with the PFA, it is, therefore, necessary to ensure the web application is secured from all form of web attacks. Carry out vulnerability scans to identify vulnerabilities in web applications
Mobile application Users security	48.3% are not aware that their PFA owns a mobile application platform and hence they responded neutrally in its use. 34.5% agree that the mobile app is secured and 10.3% disagree.	MEDIUM	Mobile applications are susceptible to buffer overflow attacks which can lead to application crash and data leakage. Others include broken encryption, client-side injection and so on.	Perform code review to ensure that the mobile application is secured.
RSA PIN Protection	34.5% believe that their RSA PIN is protected. 41.4% chose the medium level of protection for their RSA PIN	LOW	Customers may poorly keep their RSA PIN which is required to log in to their application.	Educate customers on securing their RSA PINs and keep them safe. Encrypt databases that store RSA PINs.

Email Notification	51.7% replied that they get a notification through Email from their PFA. 34.5% said they don’t receive Emails from their PFA.	LOW	A successful breach of customer accounts through vulnerable website and applications could reveal Email addresses. The email address can be used be maliciously for social engineering attacks	Ensure that the Web Application Firewall is put in place to protect web applications. Patch security vulnerabilities as soon as they are discovered. Also, educate customers never to reveal sensitive information which the PFA will never ask for.

5. CONCLUSION

We focused on using the survey method to gather information about the risk involved in the Pension Industry. Questionnaires were developed and sent to respondents who took the survey. The result of the survey was then analysed to determine the risk factor and how it can be managed. The risk assessment carried out in this paper targeted only one PFA out of the numerous ones available. The choice PFA was ARM Pension and although the survey was not comprehensive enough, significant results were obtained.

6. RECOMMENDATIONS

The Pension industry is fast growing as one of the financial institutions in Nigeria and their heavy dependence on information technology has made risk management a very important aspect that every Pension Fund Administrator should adopt in their management plan for proper business handling. Risk management should be extended to various part of the organization from Networks, access controls, servers and databases, security devices (Firewalls, IDS, Web application Firewall).

7. ACKNOWLEDGMENT

I will like to thank almighty God for seeing me through the period of writing this paper and His wisdom to complete this work. I will also extend my gratitude to the Head of Cyber Security Department of the Federal University of Technology Minna. I will like to give lots of accolades to my lecturer Dr. J A Ojeniyi for his motivation, support, and patience during the period of this work. My thanks go to my Family and friends for their support with the survey.

8. REFERENCES

[1] Chornous, G., & Ursulenko, G. (2013). Risk Management in Banks: New Approaches To Risk Assessment and Information Support. *Ekonomika*, *92*(1), 120–132.

[2] Guarracino, F., Cabrini, L., Baldassarri, R., Petronio, S., De Carlo, M., Covello, R. D., … Ambrosino, N. (2010). Noninvasive Ventilation for Awake Percutaneous Aortic Valve Implantation in High-Risk Respiratory Patients: A Case Series. *Journal of Cardiothoracic and Vascular Anesthesia*. https://doi.org/10.1053/j.jvca.2010.06.032

[3] Kiran, K. V. D., Srivatsava, M. V. R., & Devi, K. G. (2014). Risk Management in Mobile Banking, *3*(3), 1526–1529.

[4] Anthony, A. O. (2008). Risk Management in Pension Fund Administration in Nigeria. Mondaq Shehu, A. A. (2011). A Study on Financial Risk Analysis in Pension Funds Investment: an Implication of Exchange Rate Exposure. *Proceedings of the 8Th International Conference on Innovation and Management*, 1301–1308.

[5] Source, D., Bureau, N., & Commission, N. P. (2017). Report Date : October 2017 Executive Summary Nigerian Pension Fund Administration Data - 2016 Appendix Methodology, (October).

[6] Altman, E. (2008). Managing Credit Risk. 2nd ed. – John Wiley and Sons, 450 p.

[7] Arora, N., Bohn, J.R., Zhu, F. (2005). Reduced Form vs. Structural Models of Credit Risk: A Case Study of Three Models – Moody’s KMV Company, 39 p.

[8] Basel (2000). Principles for the Management of Credit Risk. Basel Committee on Banking Supervision. Bank for International Settlements. Retrieved from: http://www.bis.org/publ/bcbs54.pdf.

[9] Basel (2006). Basel II: International Convergence of Capital Measurements and Capital Standards: A Revised Framework. Technical report. Bank for International Settlements. Retrieved from: http://www.bis.org/publ/bcbs128.htm.

[10] Basel (2011). Core Principles for Effective Banking Supervision. Basel Committee on Banking Supervision. Bank for International Settlements. Retrieved from: http://www.bis.org/publ/bcbs213.pdf.

[11] Big hitters target GRC. (2011). retrieved from: http://www.insurancebusinessonline.com.au/cri/article/big-hitters-target-grc-113782.aspx.