*I.J. Information Engineering and Electronic Business*, 2019, 2, 35-43
Published Online March 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2019.02.05

# Security Risk Analysis and Management in Banking Sector: A Case Study of a Selected Commercial Bank in Nigeria

**Noah N. Gana**
Department of Cyber Security Science, Federal University of Technology Minna, Nigeria
Email: noah.gana@st.futminna.edu.ng

**Shafi'i M. Abdulhamid and Joseph A. Ojeniyi**
Department of Cyber Security Science, Federal University of Technology Minna, Nigeria
Email: {shafii.abdulhamid, ojeniyija}@ futminna.edu.ng

Received: 27 October 2018; Accepted: 14 December 2018; Published: 08 March 2019

***Abstract*—**In this paper research was carried out in order to evaluate the security risk analysis and management in banking company through the use of a questionnaire to determine the level of risk that customer of the financial institution is likely to encounter. It was discovered that though the majority of financial institution users are familiar with the possible risk associated with some banking transaction, some aspect still exists that financial institution users are not familiar with which serves as a vulnerable point that could be exploited. The study makes a recommendation for proper enlightenment of financial institution users so as to stay abreast with possible security challenge associated with some banking transaction processes to be able to mitigate possible exploit.

***Index Terms*—**ATM Card, Risk, Risk Management, Risk Assessment

## I. Introduction

The banking industries are systematically based on new innovation, product, and services as well the unique style of doing business. Based on this the banking sector has experienced notable changes over the past years and this has led to exploring the use of technologies such as information technology to ease the style of doing business [7]. In respect to this, it is therefore paramount to be able to quantify and know the associated risk that comes along with the implementation of new innovation and new styles that are integrated into the banking company such as the use of information technology infrastructures.

This will enable proper arrest of possible catastrophic that the bank may be exposed to, this now led the author to the issue of security risk analysis and management in the banking company. A risk is defined as anything that can create hindrances in the way of achievement of certain objectives. It can be because of either internal factors or external factors, depending upon the type of risk that exists within a particular situation [4]. Risk Management is a measure that is used for identifying, analyzing and then responding to a particular risk. It is a process that is continuous in nature and a helpful tool in the decision-making process [4]. Risk management is a systematic process of understanding, evaluating and addressing risks to maximize the chances of objectives being achieved and ensuring organizations, individuals and communities are sustainable [2].

The aim of this research is to evaluate the level of security risk awareness in financial institution in respect to the financial institution client as it has been established the user is the weakest link in the security chain [10], and to shade light on areas of improvement in terms of awareness and improvement based on the risk associated with financial transaction [9], thus far, the research has been able to establish that financial institution users have slim knowledge of potential risk associated with the following; using free access point for transaction, passwording devices used for online transaction, observing security logo on transaction web pages before initiating online transaction and also having licensed antivirus installed on devices used for online transaction, all of which if not properly managed can be exploited.

The organization of this research is as follow; review of related literature in terms of security risk analysis and management in the financial sector in section 2, the methodology employed in this research in section 3, result and discussion in section 4, while conclusion and recommendation are found in sections 5 and 6 respectively.

## II. Related Works

[8] A keen planning is of most important if a full benefit of internet transaction is to be actualized, of which it was discovered that the use of biometric technology has a key role to play in managing risk factors

 

through authentication of a system. Further buttress was made on the risk assessment that internet banking is exposed to prior to implementation of authentication mechanisms. And to further improve on the authentication methodologies requires adherence to security standards as may be spelled out by banking information security framework.

Information risk security management tool (COBRA$^{TM}$) was used to evaluate the quantitative risk assessment and classification of risk management control of major banks operating in Pakistan, the analysis was used to secure critical information [6]. Risk evaluation performed using (COBRA) revealed the following consolidated high-level risk assessment of five major banks in Pakistan, as the management control in all banks individually and consolidated reports has been low at 23% which is not COBRA recommended mark which is almost 50%, and recommend that the risk associated to management control must be high in all banks to fit in to COBRA report. The consolidated analysis of management control which was a survey using questionnaire to evaluate the COBRA result as well as check the maturity level of management control in these banks based on the following classification poor, fair, solid and superior respectively gave the result that all bank management control lied at the solid level and not at superior level in which it encompasses policy of information been rolled out, standards And procedures been developed, awareness of employees, confidentiality, integrity, and availability of information been considered as well as contingency, plans put in place.

[3] make use of blog mining research methodology to analyze banking on mobile application platform, to this end, to assist in forestalling the security risk associated with mobile banking application of which was pointed out as mobile malware, third-party application threat, phishing, wifi networks that are unprotected and flaws that exist in banking applications, a protection strategy, and best practices was recommended which includes the use of second factor authentication, data concealment, site key with security question and images, registered mobile device authentication and anti-virus software.

Risk management in commercial institutions in Nigeria are not given preference, likewise implementation of risk management strategies, this has led to a confusion in the financial institution, however, if proper risk management practices can be adhered to, it will lead to an exponential improvement in terms of customers and asset as it related to growth, profitability and business liquidity [2].

[1], Identify security based on secure information system in order to determine user vulnerability to phishing in banking, a controlled phishing experiment was conducted in a university and out of the users that where unwittingly attacked 8% of the users revealed their online confidential details despite warning emails about possible security threats that were sent prior to and during the controlled survey exploits. Also, an OpenPGP standard was preferred for implementation in online financial communication over SSL based on its capacity to encrypt and also offers digital signatures or files to ensure data security.

Understanding security challenges from the perspective of the financial institution customer, will offer clear-cut information security solutions to banks [7]. It is in the light of this and the reviewed challenges that prompt for proper security risk analysis and management in a banking company, in order to curtail the threat and achieve a steady financial flow, and likewise enhance the overall performance of doing business [5]. A holistic look at risk management strategy is key to counteract against the rising growth of threat in the banking sector. The case of cyber-attacks, information security which is a critical aspect in the 21$^{st}$ century is greatly dependent on the use of information technology for operation, and so, comes with its associated risks such as physical attacks, environmental threats as well as even operational sabotages. The banking industry which is a key target of the malicious entity that may eventually lead to the possible breach of the security systems put in place can be said to be lacking proper identification of risks and deployment of countermeasures, of which quantification of damages on the account of information security is hard to estimate.

## III. Methods

This study was carried out to analyze information risk associated with banking company using a selected named Commercial Bank A as a case study. A questionnaire was designed to analyze possible risk associated with information security of transaction in the banking sector. The questionnaire was developed using Google form and was administered to financial institutions' client across the different geopolitical zone in Nigeria. The total number of 58 respondents was sampled.

A five scale rating system of very frequently, frequently, occasionally, rarely and never was used in the administered questionnaire, in order to obtain the risk impact associated to questions as contained in the administered questionnaire, some of the initial five scale ratings were merged as follow; very frequently and frequently scales were merged to obtain the value of low-risk impact, the occasional scale was mapped to medium risk impact, while the scale rating of rarely and never was merged to obtain the value of high-risk impact, furthermore, the risk impact with the highest frequency was used to represent the overall risk impact.

Though, it may not be possible to assign a financial value to an eventual risk impact, as a result of this challenge the use of the above scale rating system was implemented.

## IV. Results and Discussion

The research discovered that 71.1% of the respondents are male, while 25.9% are female indicating that most of the bank user is male as indicated in fig. 1 below, 53.3%

 

of the respondents are between the age of 19 – 30years, while 41.4% of the respondents are between the age of 31 – 40, 5.2% of the respondents are 41 years and above, indicating that most of the respondent between the age bracket of 19 -30 years which are youthful are involved in internet transaction activity as represented in fig. 2.

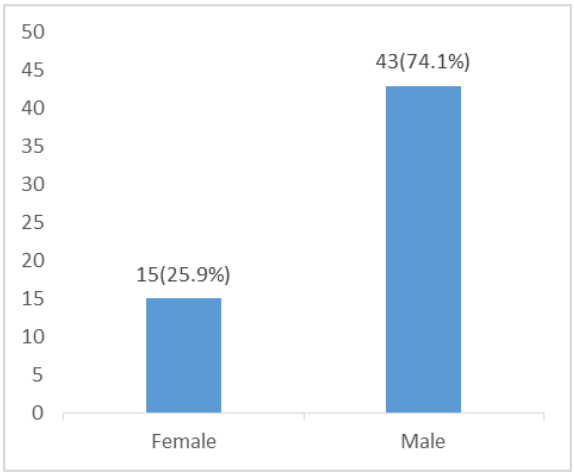


Fig.1. Gender Distribution

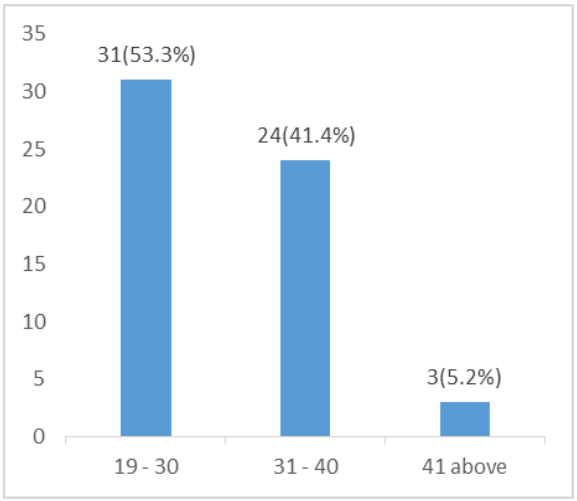


Fig.2. Age Distribution

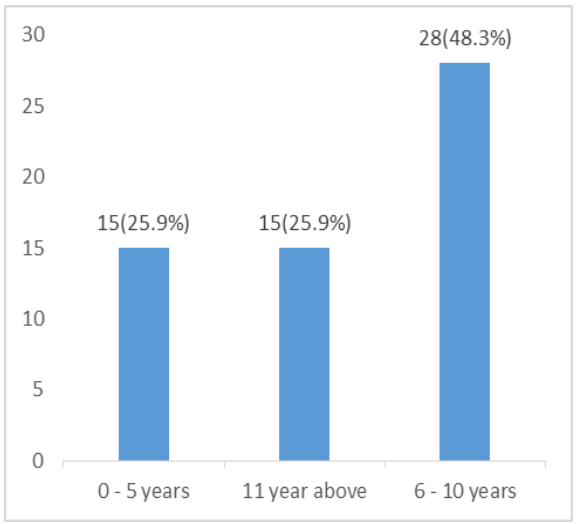


Fig.3. Banking Experience Frequency

Fig.3. above shows the years of experience the respondents have in a banking institution, 48.3% of the respondents have 6 -10 years banking experience, while 25.9% of the respondents have 11 years and above likewise 0 – 5 years of banking experience respectively. This indicates the most of the respondent have good numbers of years of experience banking

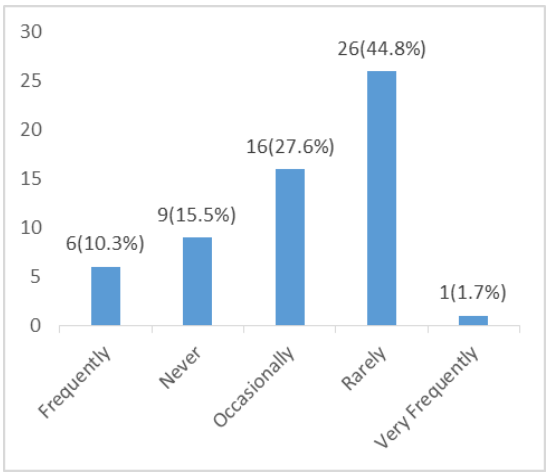


Fig.4. Confidentiality Level Frequency of ATM

The above fig. 4., indicates how likely respondents leave their (Automated Teller Machine) ATM Card exposed, 44.8% of the respondents rarely leave their ATM Card exposed, 27.6% of the respondents occasionally leave their ATM Card exposed, 15.5% of the respondents never leave their ATM Card exposed, 10.3% of the respondent frequently leave their ATM Card exposed while 1.7% of the respondents leave their ATM Card exposed very frequently

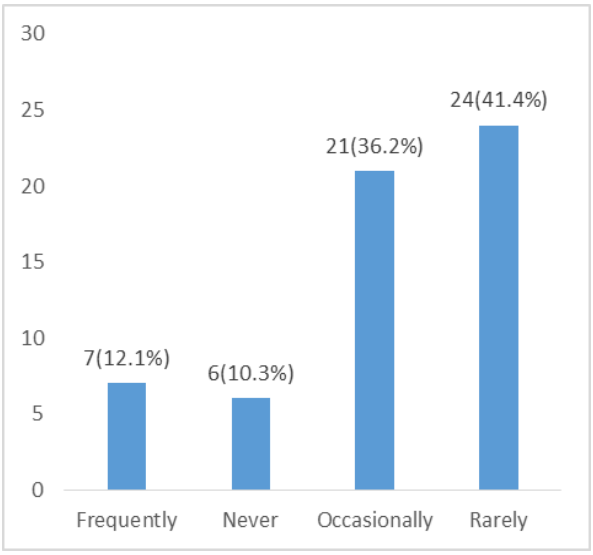


Fig.5. Confidentiality Level Frequency of ATM Card and PIN

The above fig. 5., indicate the 41.4% of the respondents rarely give out their ATM Card and (Personal Identification Number) PIN to a third party, 36.2% occasionally give out their ATM Card to a third party, 12.1% of the respondents frequently give out their

ATM Card to the third party, while 10.3% of the respondents never give out their ATM Card and PIN to the third party.

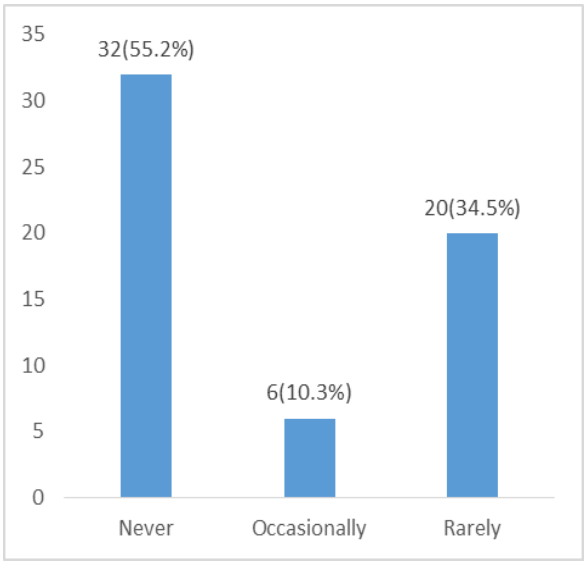


Fig.6. Online Transaction Support Frequency

The above fig. 6., indicate that 55.2% of the respondents do not seek for assistance during an online transaction, 34.5% of the respondents rarely seek for assistance during an online transaction, while 10.3% of the respondents occasionally seek for assistance during an online transaction.

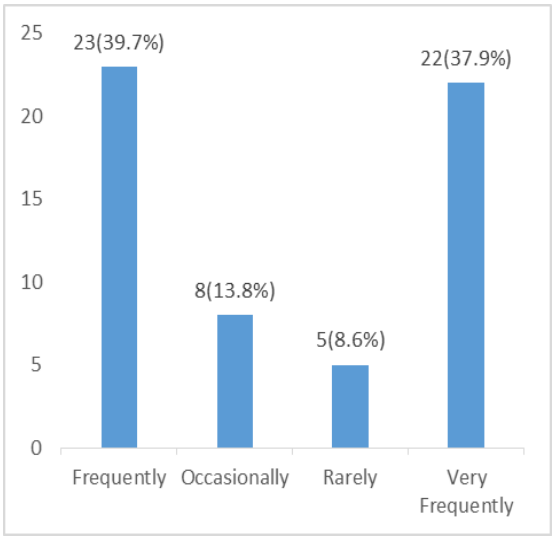


Fig.7. Frequency of Smart Device Usage for Financial Transaction

In the fig. 7., above 39.7% of the respondents frequently use their device to perform a financial transaction, 37.9% of the respondents use their devices very frequently for a financial transaction, 13.8% of the respondents occasionally use their devices for the financial transaction while 8.6% of the respondents rarely use their devices for a financial transaction.

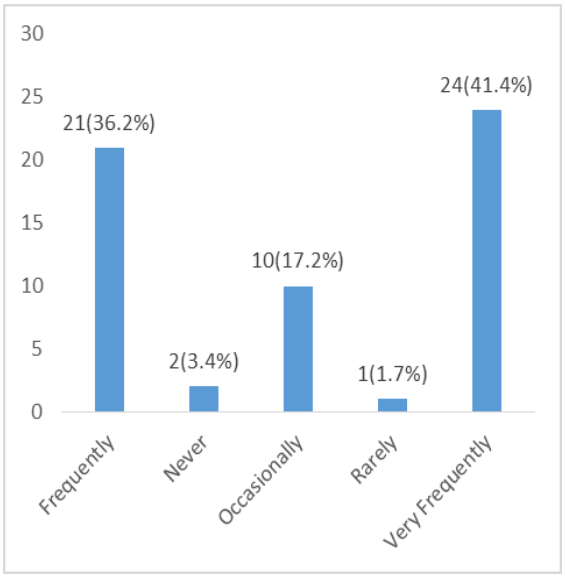


Fig.8. Frequency of Passwording Smart Devices Used for Financial Transaction

The fig. 8., above also indicate that 41.4% of the respondents feel it is necessary to password their devices used for online transaction very frequently, 36.2% of the respondents feel that devices should be passworded frequently, 17.2% of the respondents feel that devices should be passworded occasionally, while 3.4% of the respondents feel that devices should never be passworded and 1.7% of the respondents feel that devices should be rarely passworded

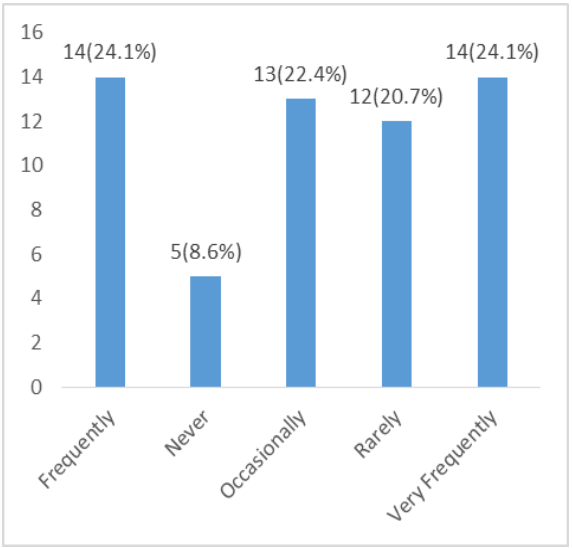


Fig.9. Frequency of Security Logo Identification during Online Transaction

The responses fig. 9., above indicates how often respondents note security logo during an online transaction; 24.1% responded as frequently and very frequently respectively, 22.4% responded occasionally, while 20.7% responded rarely and 8.6% responded never.

 

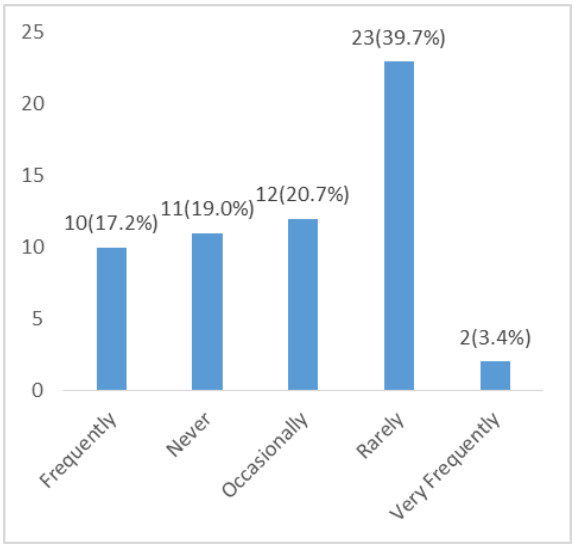


Fig.10., Frequency of Free Wireless Access Point Usage for Online Transaction

The fig. 10., above indicate that 39.7% of the respondents use free wireless access point for online transaction rarely, 20.7% of respondents occasionally use free wireless access point for online transaction, 19.0% of the respondents never use free wireless access point for online transaction, 17.2% of respondents frequently use free wireless access point for online transaction and 3.4% of respondent used free wireless access point for online transaction very frequently.

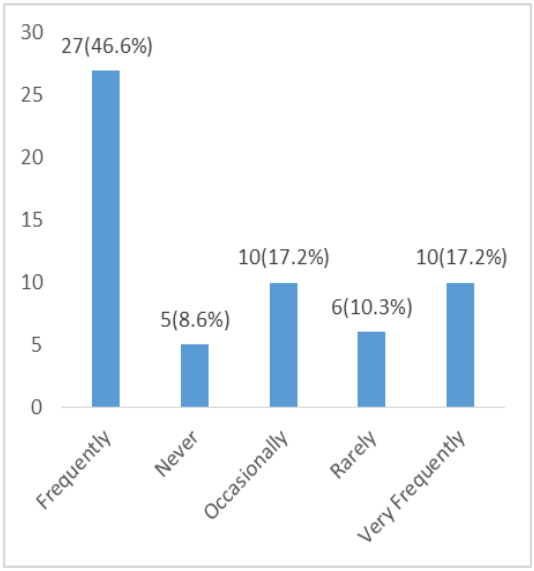


Fig.11. Frequency of Having Antivirus Installed on Devices Used for Online Transaction

The above fig. 11., indicate that 46.6% of the respondents do feel that it is necessary to have a licensed antivirus installed on the devices used for online transaction, 17.2% of the respondents responded that having a licensed antivirus installed on devices used for online transaction should be very frequently and occasional respectively, 10.3% of the respondents feel that it is necessary to have a licensed antivirus installed on the devices used for online transaction rarely, while 8.6% of the respondents selected never to have a licensed antivirus installed on devices used for online transaction.

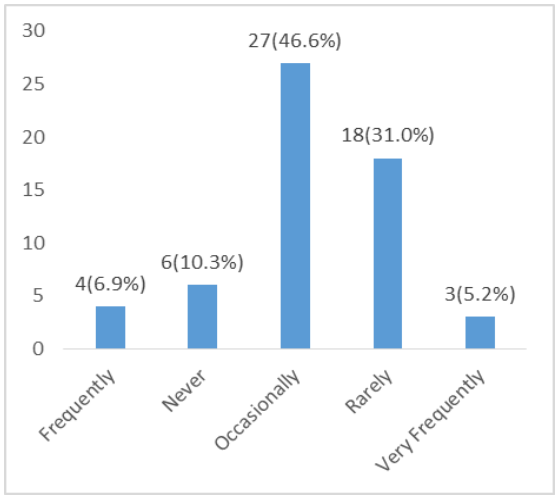


Fig.12. Frequency of Experiencing Debit without Successful Transaction

The fig. 12., above, indication that 46.6% of the respondents occasionally experience been debited without a successful transaction, 31.0% of the respondents rarely experience been debited without a successful transaction, 10.3% of the respondents never experience been debited without a successful transaction, 6.9% of the respondents frequently experience been debited without a successful transaction, while 5.2% of the respondents experience very frequently been debited without a successful transaction.

### *A. The Responses Obtained from Commercial Bank A Client*

The response indication from Commercial Bank A user, 11 respondents out of total respondents' use Commercial Bank A as their financial institution, Commercial Bank A plc was incorporated as a limited liability company licensed to provide commercial and other banking services to the Nigerian public in 1990. The Bank commenced operations in February 1991, and has since then grown to become one of the most respected and service focused banks in Nigeria, Commercial Bank A plc has 231 branches, 17 Cash Centres, 18 e-branches, 41 BankExpress locations, and more than 1165 ATMs in Nigeria, AREAS SERVED: Cote d'Ivoire, Kenya, Liberia, Gambia, Ghana, Nigeria, Rwanda, Tanzania, Uganda, United Kingdom.

Services offered by Commercial Bank A includes an electronic notification system which notifies customers about all transactions on their accounts via their phones and e-mail (On-Line Real Time). Also accessing of accounts through the Internet and mobile banking services, inclusive in other services and products offered by Commercial Bank A are; Relationship Management, Mobile/SMS banking, POS, Automated Teller Machine (ATM), Bank Automated Payment System and Statement by email.

Table 1., below indicates a breakdown of the responses obtained basically from those who bank with Commercial

Bank A, a five scale rating was used which are very frequently, frequently, occasionally, rarely and never, while the risk impact level was determined through the merging of very frequently and frequently to obtain the value of low-risk impact, medium risk impact was obtained through direct mapping to occasionally scale, and high-risk impact was obtained through the merging of the scales rarely and never, this scaling system was used throughout this study. Table 1. shows a breakdown of risk impact based on responses obtained about some components of performing banking transactions.

Table 1. Evaluation of responses from Commercial Bank A Client (Risk Impact Table)

| Administered Questions | Scaling Rate | Responses | Percentage (%) | Risk Impact | Overall Risk Impact |
|---|---|---|---|---|---|
| How likely do you leave your ATM Card exposed? | Very frequently | 0 | 0 | Low(1) | **High** |
| | frequently | 1 | 9.1 | | |
| | occasionally | 3 | 27.3 | Medium(3) | |
| | rarely | 6 | 54.5 | High(7) | |
| | never | 1 | 9.1 | | |
| How often do you give out your ATM Card and PIN to a third party (e.g friend, family member or colleague) for a transaction? | Very frequently | 0 | | Low(2) | **High** |
| | frequently | 2 | 18.2 | | |
| | occasionally | 4 | 36.4 | Medium(4) | |
| | rarely | 4 | 36.4 | High(**5**) | |
| | never | 1 | 9.1 | | |
| How often do you seek assistance during an online transaction? | Very frequently | 0 | 0 | Low(0) | **High** |
| | frequently | 0 | 0 | | |
| | occasionally | 1 | 9.1 | Medium(1) | |
| | rarely | 4 | 36.4 | High(**10**) | |
| | never | 6 | 54.5 | | |
| How often do you seek for assistance when performing a transaction using ATM Machine? | Very frequently | 0 | 0 | Low(0) | **High** |
| | frequently | 0 | 0 | | |
| | occasionally | 0 | 0 | Medium(0) | |
| | rarely | 3 | 27.3 | High(**11**) | |
| | never | 8 | 72.7 | | |
| Do you feel it is necessary to password devices used for the online transaction(e.g smartphone)? | Very frequently | 5 | 45.5 | Low(**7**) | **Low** |
| | frequently | 2 | 18.2 | | |
| | occasionally | 3 | 27.3 | Medium(3) | |
| | rarely | 0 | | High(1) | |
| | never | 1 | 9.1 | | |
| How often do you take note of the security logo during an online transaction? | Very frequently | 5 | 45.5 | Low(**6**) | **Low** |
| | frequently | 1 | 9.1 | | |
| | occasionally | 0 | 0 | Medium(0) | |
| | rarely | 5 | 45.5 | High(5) | |
| | never | 0 | 0 | | |
| How often do you use a free wireless access point (e.g hotspot) for online transaction? | Very frequently | 1 | 9.1 | Low(4) | **High** |
| | frequently | 3 | 27.3 | | |
| | occasionally | 2 | 18.2 | Medium(3) | |
| | rarely | 1 | 9.1 | High(**5**) | |
| | never | 4 | 36.4 | | |
| Do you feel it is necessary to have a licensed antivirus installed on the device used for online transaction? | Very frequently | 0 | 0 | Low(**5**) | **Low** |
| | frequently | 5 | 45.5 | | |
| | occasionally | 3 | 27.2 | Medium(3) | |
| | rarely | 2 | 18.2 | High(3) | |
| | never | 1 | 9.1 | | |
| How often have you experienced been debited without a successful transaction? | Very frequently | 0 | 0 | Low(0) | **High** |
| | frequently | 0 | 0 | | |
| | occasionally | 3 | 27.3 | Medium(3) | |
| | rarely | 6 | 54.5 | High(**8**) | |
| | never | 2 | 18.2 | | |

From the response information of table 1., above it indicates that the ATM Card should be given high priority due to the fact that its exposure can lead to the compromise of the account of a financial institution user, the sharing of the ATM Card and PIN with the third party should be avoided as this can have a high risk on the side of the actual owner of the ATM Card who stands a chance of been impersonated through transaction, assistance while performing online transaction as well as transaction using ATM Machine should be avoided as this can lead to a high risk when transaction details are spy on such passwords of devices and transaction passwords, taking note of online security logo and having licensed antivirus installed in devices used for online transaction has a low impact on transaction as indicated by the respondents but this should not be taken lightly as information theft and the bridge of transaction can occur, the use of free access point potent a high risk as

transactions can be monitored due to the unsecured nature of the access point most at time, while been debited without a successful transaction indicates a high-risk impact as transaction can be high jack at the point of service failure.

### *B. The Commercial Bank 'A' And Other Financial Institution User Responses*

About 6.3% of respondents bank with Commercial Bank A, Union Bank of Nigeria, First Bank Nigeria Ltd, 12.5% of the respondents bank with Access Bank PLC and Commercial Bank A, 6.3% of the respondents bank with Commercial Bank A and first bank Nigeria, 25.0% of the respondents bank with Commercial Bank A and Commercial Bank B, 6.3% of the respondents bank with Commercial Bank A and Commercial Bank C, 6.3% of the respondents bank with Commercial Bank D, Commercial Bank A, Commercial Bank E and Commercial Bank F, 6.3% of the respondents bank Commercial Bank A, Commercial Bank G, Commercial Bank H, 6.3% of the respondents bank with Commercial Bank E, Commercial Bank A, Commercial Bank I, Commercial Bank B, 6.3% of the respondents bank with diamond bank, Commercial Bank J, Commercial Bank A, First Bank Nigeria Ltd, 6.3% of the respondents bank with Commercial Bank A, Commercial Bank I, Commercial Bank B, 6.3% of the respondents bank with Commercial Bank I, Commercial Bank F, Commercial Bank A, 6.3% of the respondents bank with Commercial Bank A, Commercial Bank K.

Table 2. indicate the respondents have good background knowledge in banking company 50% have 6 – 10 years of experience banking, 37.5% of the respondents have 11 years and above experience banking, while 12.5% of the respondents have 0 – 5 years of experience banking.

Majority of the respondents are male which total to 81.3%, while female respondents are 18.8%, meanwhile, the age bracket of 31 – 40 years of the respondents is 43.8%, 19 – 30 years of the respondents is 50%, while 40 years and above of the respondents is 6.3%.

Table 2. A distribution of years of experience respondents of Commercial Bank 'A' and other financial institution users have with a banking institution

| | 0 – 5 years | 6 – 10 years | 11 years and above |
|---|---|---|---|
| Percentage (%) | 12.5 | 50.0 | 37.5 |
| Number of respondents | 2 | 8 | 6 |

Table 3. Evaluation of responses from Commercial Bank A and others Financial Institutions Client (Risk Impact Table)

| Administered Questions | Scaling Rate | Responses | Percentage (%) | Risk Impact | Overall Risk Impact |
|---|---|---|---|---|---|
| How likely do you leave your ATM Card exposed? | Very frequently | 0 | 0 | Low(0) | **High** |
| | frequently | 0 | 0 | | |
| | occasionally | 5 | 31.3 | Medium(5) | |
| | rarely | 10 | 62.5 | High(**11**) | |
| | never | 1 | 6.3 | | |
| How often do you give out your ATM Card and PIN to a third party (e.g friend, family member or colleague) for a transaction? | Very frequently | 0 | | Low(1) | **High** |
| | frequently | 1 | 18.2 | | |
| | occasionally | 6 | 37.5 | Medium(6) | |
| | rarely | 9 | 56.3 | High(**9**) | |
| | never | 0 | 0 | | |
| How often do you seek assistance during an online transaction? | Very frequently | 0 | 0 | Low(0) | **High** |
| | frequently | 0 | 0 | | |
| | occasionally | 3 | 18.8 | Medium(3) | |
| | rarely | 5 | 31.3 | High(**13**) | |
| | never | 8 | 0.0 | | |
| How often do you seek for assistance when performing a transaction using ATM Machine? | Very frequently | 0 | 0 | Low(0) | **High** |
| | frequently | 0 | 0 | | |
| | occasionally | 0 | 0 | Medium(0) | |
| | rarely | 3 | 18.8 | High(**16**) | |
| | never | 13 | 81.3 | | |
| Do you feel it is necessary to password devices used for the online transaction(e.g smartphone)? | Very frequently | 8 | 50.0 | Low(**13**) | **Low** |
| | frequently | 5 | 31.3 | | |
| | occasionally | 3 | 18.8 | Medium(3) | |
| | rarely | 0 | | High(0) | |
| | never | 0 | 0 | | |
| How often do you take note of the security logo during an online transaction? | Very frequently | 4 | 25.0 | Low(**8**) | **Low** |
| | frequently | 4 | 25.0 | | |
| | occasionally | 4 | 25.0 | Medium(4) | |
| | rarely | 2 | 12.5 | High(4) | |
| | never | 2 | 12.5 | | |

 

| | | | | | |
|---|---|---|---|---|---|
| How often do you use a free wireless access point(e.g hotspot) for online transaction? | Very frequently | 0 | 0 | Low(2) | **High** |
| | frequently | 2 | 12.5 | | |
| | occasionally | 2 | 12.5 | Medium(2) | |
| | rarely | 11 | 68.8 | High(**12**) | |
| | never | 1 | 6.3 | | |
| Do you feel it is necessary to have a licensed antivirus installed on the device used for online transaction? | Very frequently | 3 | 18.8 | Low(**10**) | **Low** |
| | frequently | 7 | 43.8 | | |
| | occasionally | 4 | 25.0 | Medium(4) | |
| | rarely | 1 | 6.3 | High(2) | |
| | never | 1 | 6.3 | | |
| How often have you experienced been debited without a successful transaction? | Very frequently | 0 | 0 | Low(0) | **High** |
| | frequently | 0 | 0 | | |
| | occasionally | 8 | 50.0 | Medium(8) | |
| | rarely | 7 | 43.8 | High(**8**) | |
| | never | 1 | 6.3 | | |

Based on the response obtained from those that make use of Commercial Bank A and other banking financial institution as displayed in table 3., 16 respondents took part in the study, the study further revealed that exposing your ATM Card will have a high impact of risk on the client, while sharing of ATM Card and PIN with third party also has a high impact risk on the customer, seeking for assistant while performing online and ATM transactions gives high impact risk, while the necessity of passwording devices used for online transaction and having a licensed antivirus installed on the devices used for online transaction indicate a low impact risk, which is also applicable to taking note of security logo during online transaction, using a free wireless access point and been debited without a successful transaction all have a high impact risk on financial institution.

## V. Conclusion

Discovered in this study was that most of the bank users have basic knowledge of security risk that is attached to some component of banking sector such as ATM Card exposure, sharing of ATM Card details with the third party, seeking for assistance while performing online and ATM transaction, use of free access point, however, more need to be done in some aspect through enlighten of the bank user in areas of passwording devices used for online transaction, noting of security logo when performing online transaction, and also having a licensed antivirus installed on devices used for online transaction as exploit of this area can lead to a great risk impact on banks and its clients.

## VI. Recommendation

The study recommended that more should be done in educating bank clients on issues of security consciousness of device used for an online transaction, use of free hotspot for banking transaction, likewise having a licensed antivirus installed on the devices used for a banking transaction. Meanwhile, future work will focus on evaluating the security risk that is associated with a platform that manages the use of information technology in performing banking activities.

## References

[1] Ambhire, V. R., & Teltumde, P. S. (2011). Information Security in Banking and Financial Industry, *14*(October), 101–105.

[2] Dugguh, S. I., Ph, D., & Diggi, J. (2015). Risk Management Strategies in Financial Institutions in Nigeria : the Experience of Commercial Banks, *2*(6), 66–73.

[3] He, W., Tian, X., & Shen, J. (2015). Examining Security Risks of Mobile Banking Applications through Blog Mining In *MAICS*,( pp. 103-108).

[4] Kanchu, T., & Kumar, M. M. (2013). RISK MANAGEMENT IN BANKING SECTOR -AN EMPIRICAL STUDY, *2*(2), 145–153.

[5] Mishra, S. K. (2015). Banking sector : emerging challenges and opportunities. In *International Conference on Issues in Emerging Economies (ICIEE), 29-30th January 2015 17* (Vol. 5, pp. 29–30).

[6] Munir, U., & Manarvi, I. (2010). Information Security Risk Assessment for Banking Sector-A Case study of Pakistani Banks. *Global Journal of Computer Science and Technology*, *10*(February), 44.

[7] Odhiambo, C., Jowi, N., & Abade, E. (2016). Evaluation of Information Security Risk Assessment for Internet Banking Among Commercial Banks in Kenya __ Science Publishing Group, *5*(3), 51–59. https://doi.org/10.11648/j.ajnc.20160503.11

[8] Sarma, G., & Singh, P. K. (2010). Internet Banking : Risk Analysis and Applicability of Biometric Technology for Authentication. *International Journal of Pure and Applied Sciences and Technology*, *1*(2), 67–78.

[9] Sheikh, B. A. (2015). Internet Banking, Security Models and Weakness. *International Journal of Research in Management & Business Studies (IJRMBS 2015)*, *2*(4).

[10] Zahoor, Z. (2016). Challenges in Privacy and Security in Banking Sector and Related Countermeasures. *International Journal of Computer Applications*, *144*(3), 24–35.

## Authors' Profiles

**Noah N. Gana**, a postgraduate student currently in the school of Information Communication Technology, Federal University of Technology(FUT), Minna, Nigeria. He is currently running his master's degree in the Department of Cyber Security Science, he completed his first degree in Computer Science (Cyber Security Science) at FUT Minna, Nigeria.

His research interest includes cyber security, network security, internet security, information security, cyber-physical system security, biometrics security.

**Joseph A. Ojeniyi**, He received his Ph.D. in Cyber Security Science from the same University, M.Sc. in Computer Science from the University of Ibadan, Nigeria and a B.Tech. in Mathematics/Computer Science from the Federal University of Technology Minna, Nigeria.

He is a lecturer in the Department of Cyber Security Science, School of Information and Communication Technology, (FUT) Minna, Nigeria. He has been appointed as a reviewer to several indexed Journals. He currently serves as the chairman of the Conference Organizing Committee of the faculty, 'ICTA 2018'. His area of interest includes Cyber Security, Digital Forensics, Deep Learning, Artificial Intelligence in Information Assurance/Security and Cyber-Physical Systems.

**Shafi'i M. ABDULHAMID** received his Ph.D. in Computer Science from Universiti Teknologi Malaysia (UTM), MSc in Computer Science from Bayero University Kano (BUK), Nigeria and a Bachelor of Technology in Mathematics/Computer Science from the Federal University of Technology Minna, Nigeria. His current research interests are in Cyber Security, Cloud computing, Soft Computing, and BigData. He has published many academic papers in reputable International journals, conference proceedings, and book chapters. He has been appointed as an Editorial board member for UPI JCSIT and IJTRD. He has also been appointed as a reviewer of several ISI and Scopus indexed International journals such as JNCA Elsevier, ASOC Elsevier, EIJ Elsevier, NCAA Springer, BJST Springer, & IJNS. He is a member of IEEE, IACSIT, IAENG, ISOC, Computer Professionals Registration Council of Nigeria (CPN), Cyber Security Experts Association of Nigeria (CSEAN) and Nigerian Computer Society (NCS). Presently, he is a Senior Lecturer at the Department of Cyber Security Science, Federal University of Technology Minna, Nigeria.

**How to cite this paper:** Noah N. Gana, Shafi'i M. Abdulhamid, Joseph A. Ojeniyi, "Security Risk Analysis and Management in Banking Sector: A Case Study of a Selected Commercial Bank in Nigeria", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.11, No.2, pp. 35-43, 2019. DOI: 10.5815/ijieeb.2019.02.05

 