International Journal of Innovative Information Systems & Technology Research 13(4):265-279 Oct-Dec, 2025

© SEAHI PUBLICATIONS, 2025 www.seahipublications.org ISSN: 2467-8562

doi:10.5281/zenodo.17653257

Assessment Of Cybersecurity Risk Management Practices In The Financial Services Industry

George Ikwuje Agada; Paul Gideon; Prof. Uche Mbanaso & Dr. Steven bassey

ABSTRACT

Digital transformation has tremendously boosted the use of Cyberspace in delivering services in the Financial services industry globally. The attendant implication of this is the increase in Cyber threat targeted at the industry. This threat is largely believed to be motivated by the huge funds in the industry and the significant reputational damage that could be inflicted on institutions in the industry. The financial services industry in Nigeria as part of the global Financial services industry is also adversely impacted by the same threat hence the need for this study. This study aims to contribute to efforts geared towards reducing the risk exposure of the Nigerian Financial services industry to Cybersecurity risk through the assessment of current risk management practices in the industry, identification of existing gaps and the proffering of recommendations to close the identified gaps. In carrying out the study, a mixed-method approach was adopted comprising structured interviews and online questionnaire survey. Analysis of result from both the Interviews conducted and the questionnaire survey indicated that numerous Cybersecurity risk Management practices are existing in the industry but there are Identified gaps that need to be closed. The study concludes that while Cybersecurity risk management practices have become entrenched in the Nigerian Financial Services Industry, there is need for more collaboration and coordination of efforts and the adoption of other measures to achieve enhanced Cybersecurity risk management in the industry.

Keywords: Cyberspace, Cyber Risk, Cyber Threat, Financial Services Industry, Cyber Attack, Cyber Threat, Vulnerability, ISO2700,Cybersecurity training

INTRODUCTION

Cyberspace has become a highly valued space for the conduct of many activities by individuals, organizations and nation state actors, these activities include politics, social activities as well as economic activities. The National Institute of Standards and Technology (NIST) of the US defines Cyberspace as a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace can also be defined as a virtual computer world, and more specifically, an electronic medium that is used to facilitate online communication which allows users to share information, interact, exchange ideas, play games, engage in discussions or social forums, conduct business and create intuitive media, among many other activities.

Cyberspace is increasingly becoming the space of choice for various human activities because of the unparallelled reach, ubiquity and instantaneous connectivity features which it provides among other benefits. These features and benefits have, however, brought with them some negative effects as well. Malevolent actors are increasingly using the space to perpetrate malicious cyber-attacks that have resulted in huge losses in lives and properties. According to a Report published by Statista the global cost of cybercrime will increase from $2.95 billion in 2020 to $13.82 billion by 2028.With the increasing spate of malicious cyber-attacks, it has become imperative for individuals. Organizations and nation states carrying out various activities in cyberspace to put in place measures to minimize their exposure to the associated risk factors.

One sector that is hugely impacted by the ongoing spate of malicious Cyber-attacks in cyberspace is the Financial services industry. As a result of Digital transformation, this industry currently leverages cyberspace heavily in the delivery of services and products to various categories of consumers. Cybersecurity risks to the financial system have grown in recent years, in part because the cyber threat landscape is worsening; in particular, state-sponsored cyberattacks targeting financial institutions are becoming more frequent, sophisticated, and destructive. In 2017, the G20 warned that cyberattacks could "undermine the security and confidence and endanger financial stability."

The Boston Consulting Group's 'Global Wealth 2019: Reigniting Radical Growth' report has stated that financial sector firms are 300 times more likely than other companies to be targeted by a cyber-attack. The report goes on to say that dealing with those attacks and their aftermath carries a higher cost for banks and wealth managers than for any other sector. A fact that is backed up by Fortunly's assessment that the cost of cyberattacks in the banking industry has reached $18.3 million annually per company - not only because of the financial losses but also because these breaches erode user trust. The IBM cost of data breach Report 2023 published by the Ponemon Institute stated that the global average cost of a data breach in 2023 was USD4.45 million, a 15% increase over three years.

Africa's rapid digital transformation since COVID-19 leaves critical infrastructure vulnerable to cybercrime, which cost the continent an estimated $4.12 billion last year. Banks and insurance companies are increasingly becoming prime targets within the continent. Across the continent, cybersecurity incidents result in losses estimated at between $3.5 billion and $4 billion every year. 97% of surveyed leaders of financial institutions in Africa rank cybercrime and regulatory constraints on cybersecurity as the leading threat to the financial services industry alongside worsening economic conditions. According to the report, the increase in the volume and sophistication of attacks explains why financial institutions consider cybersecurity a top concern.

Many countries across the continent including Nigeria are grappling with this menace as their financial services sector leverage digital transformation to enhance the delivery of their services and products to a growing population of customers.

The Nigerian digital financial ecosystem has witnessed remarkable growth in the past few years. According to McKinsey, Nigeria is home to over 200 fintech organizations, not counting fintech solutions provided by banks and mobile network operators.1 New service providers range from mobile money operators and payment service providers to fintech firms and other financial services providers, a trend that is increasing the need to ensure consumer security and trust. These services come with numerous important digital components, including mobile applications, digital tokens, Unstructured Supplementary Service Data, and digital ledgers, all of which involve potential vulnerabilities. It is increasingly important for the country's financial industry to prioritize cybersecurity as it is the most targeted sector for cyber-attacks.2

With the emergence and growth of internet banking in Nigeria, financial institutions have become ever more reliant on computer systems to perform their daily businesses (Lagazio et al., 2014). This, in turn, has provided a new opportunity that perpetrators of cybercrime may exploit (Raghavan and Parthiban, 2014). Cyber security breaches have, in fact, become one of the main threats affecting the Nigerian banking industry, generating considerable damage to this sector (Ojeka et al., 2017). Recent studies have shown that the emerging cyber security risk confronting the industry are not going to reduce but increase not just in frequency but sophistication. According to Kost (2024) in a paper titled The Six biggest Cyber threats for Financial services in 2024 while the major threat vectors in the industry have been phishing attacks and Distributed denial of service, Ransome ware attacks have become the dominant attack vector in recent times and will continue to be in the nearest future. in the first 6 months of 2021 Ransomware attacks increased by 151%.One huge motivation for attacks is the amount of money in the industry and the huge impact such attacks are likely to have when successfully carried out.

Against this background it has become highly imperative therefore to examine current Cybersecurity risk management practices put in place in the financial services industry to minimize its Cyber risk exposure with a view to ensuring that identified gaps are closed to minimize financial and non-financial losses due to cyber-attacks which are increasing likely to occur.

Statement of the problem

The increasing embrace of Digital transformation by the financial services industry globally coupled with the increasing Cyber threat level in cyberspace has tremendously increased the exposure of the industry to Cyber risks. Ozarslan (2022) in his paper titled key threats and Cyber Risks facing financial services and Banking Firms in 2022 stated that although almost every business is a potential victim of cybercrime, cyber threat actors usually select their victims based on two criteria: maximum revenue and maximum impact. Financial institutions, such as banks and other financial services are prime target for cybercriminals since they fulfil these two criteria, as a result Cyber threat actors are targeting the financial sector excessively. He further stated that the cost of cybercrime for financial services is 40% higher than all other sectors. According to the latest World Bank report the financial services industry is more likely to be attacked now than ever before. In order to mitigate these risks, Cybersecurity risk management measures have been put in place across the industry. These is a need to evaluate these risks management measures/practices to determine if they are robust enough to provide the required level of cyber resilience against the increasing cybersecurity risks confronting the industry. The Cybersecurity posture of organizations is often undermined by gaps that are not exposed for closure which make them susceptible to cyber-attacks through various vectors. A critical assessment of these gaps and the implementation of recommended measures will help prevent the occurrence of these attacks and minimize their impact when they occur.

Research Questions

The questions addressed by this research are:

i. What are the Cybersecurity risk management practices currently prevalent in the Nigerian Financial services industry?

ii. How well are these cybersecurity risk management practices carried out in line with established standards/frameworks and how have the practices helped in improving the cybersecurity posture of the Nigerian financial services industry?

iii. What measures can be put in place to close identified gaps in the cybersecurity risk management practices in the financial services industry?

Objectives of the study

The aim of the study is to assess the Cybersecurity risk management practices in the Nigerian Financial services industry with a view to identifying gaps and proffering recommendations for the closure of such gaps which will help strengthen the cybersecurity posture of the industry.

The objectives are:

a) To assess and identify the Cybersecurity Risk management practices in the Nigerian financial services space against the backdrop of increasing cybersecurity threat level using questionnaires and interviews

b) To identify gaps in the Cybersecurity Risk management practices in the Financial services sector

c) To proffer recommendations on the closure of the identified gaps.

MATERIALS AND METHOD

This study adopted Descriptive Research design with mixed-method approach. This design combines quantitative and qualitative approaches in answering the research questions. The mixed method research approach used is the Convergent parallel mixed method approach. With this approach, Quantitative and qualitative data are collected at the same time and analyzed separately. After both analyses are completed the results are compared to draw overall conclusions Survey was used as part of the mixed-method approach which involved the deployment of questionnaires to targeted respondents. The questionnaire consisted of open-ended and close-ended questions.

A pilot of the Survey Questionnaire was conducted to verify its appropriateness and completeness as well as to gauge the meaning of the questions. The questionnaire instrument was piloted on 30th December 2024 to ten(10) different Cybersecurity subject matter experts who made comments and suggestions on the online questionnaire, which the researcher captured. This ensured that the questions were not ambiguous, difficult to answer or prone to many interpretations, which could lead to biased responses. Before the survey instrument was disseminated, some questions were edited to ensure clarity and answerability, while some were re-arranged to improve the flow of responses. Other changes involved altering some binary responses 'yes' or 'no' to the Likert scale type and providing options to other questions. The final questionnaire contained twenty seven questions with most of them providing response options based on a five-point Likert scale ranging from 1 = Strongly Agree to 5 = Disagree and the last question requires comments from respondents.

Population Sample and Sampling Techniques

The study targeted IT/Cybersecurity specialists in the employment of financial institutions and organizations in the Nigerian financial services industry comprising commercial banks, merchant banks, discount houses, building societies/Mortgage banks, Pension Fund Administrators, Insurance companies, Stock Exchanges and Finance houses. It also targeted Subject matter experts, Regulatory Supervisors and Chief Information Security Officers (CISOs) from Regulatory entities in the industry namely the Central Bank of Nigeria(CBN), Nigeria Deposit Insurance Corporation(NDIC), Securities and Exchange Commission (SEC), National Insurance Commission(NAICOM) and Pension Commission(PENCOM) as well as ISO27001 Auditors and Cybersecurity Service providers to the industry. The survey questionnaire for the study was administered to respondents in the financial services sector to obtain their responses to various questions cutting across the focus of the Research.

The population sample for this study was drawn from IT/Cybersecurity specialists working in Financial institutions across the Nigerian financial services industry, Cybersecurity services providers and Subject matter experts, Regulatory supervisors and Chief Information Security Officers in the various regulatory entities in the industry.

A combination of Purposive and Convenience sampling techniques was used in this Research to recruit participants. Purposive sampling, also known as judgmental, selective or subjective sampling, is a form of non-probability sampling in which researchers rely on their own judgment when choosing members of the population to participate in surveys. This type of sampling is often used in qualitative research, allowing the researcher to focus on specific areas of interest and gather in-depth data based on study purpose with the expectation that each participant will provide unique and rich information of value to the study .. Purposive and Convenience sampling can be mixed together in data collection for mixed methods Research studies. According to Fraenkel et al (2015) and Etikan et al (2016), the most common sampling strategies used in Quantitative and Qualitative research are purposive sampling and convenience sampling. While the former allows the selection of objectives and specially qualified respondents or participants to collect the requisite data, the latter allows for focus on specific areas of interest and gather in-depth data on those topics, subjects are selected based on study purpose with the expectation that each participant will provide unique and rich information of value to the study.

Sample size

Since a mixed-mode approach was used in this study which also entailed the use of a combination of Purposive sampling and convenience sampling, the determination of Sample size was not necessary. According to Arragante (2022), It should be noted that it is generally not necessary to calculate the sample size in qualitative studies, since the main aim is to achieve information saturation, which occurs when the information collected becomes redundant, and no new information is collected from the study participants. Also, according to Zhi (2014), as sample size increases, the statistical power of the convenience sample also increases while in purposive sampling, Sample size is determined by data saturation not by statistical power analysis. However, a sample size of 180 participants is proposed for the targeted population. It is believed that this is a reasonable enough number of participants that is representative of the targeted population.

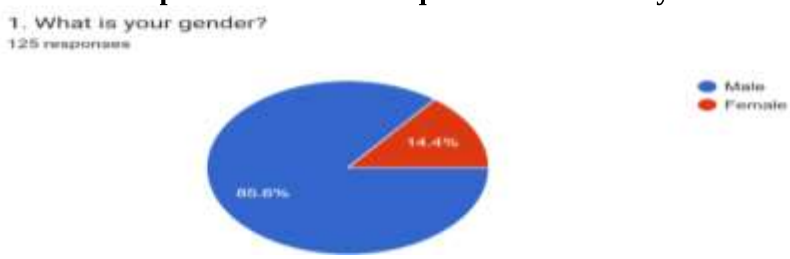
Validity and Reliability of data collection instrument

Reliability of the study was ensured by the consistent application of the data collection methods. This entails carrying out the same steps for each method. In conducting interviews or observations, a clear definition of how specific behaviors or responses will be counted was made, and questions were phrased the same way each time to avoid omitted variable bias or information bias. The validity of the study was ensured by choosing appropriate methods of measurement and ensuring the use of appropriate sampling methods to select subjects. - questionnaire questions were carefully and precisely worded. The study population was clearly defined and care was taken to ensure that enough participants that are representative of the population were used.

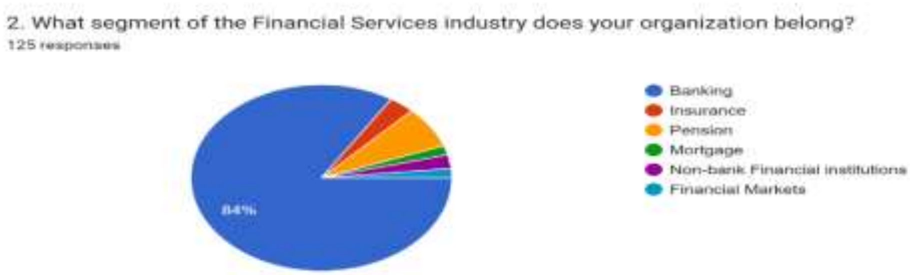
RESULTS

The online questionnaire survey was administered on IT/Cybersecurity specialists/staff of Banks, Pension Fund Administrators, Primary Mortgage Institutions, Finance Companies, Insurance companies and Financial Market operators. The administration of the Questionnaire commenced on 7th January 2025 and ended on 15th February 2025.It was administered on 180 respondents but 125 respondents provided response as at 15th February 2025. Secondary data for the research was obtained from relevant publications(including online publications/websites). The data from the interview sessions were transcribed and analysed using thematic analysis to identify the common themes among the interview responses:

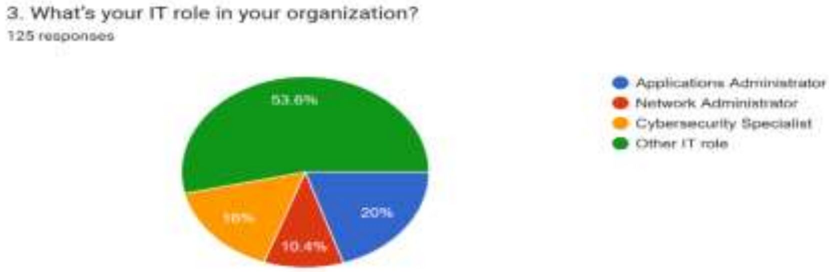
Details of Responses from Online questionnaire survey



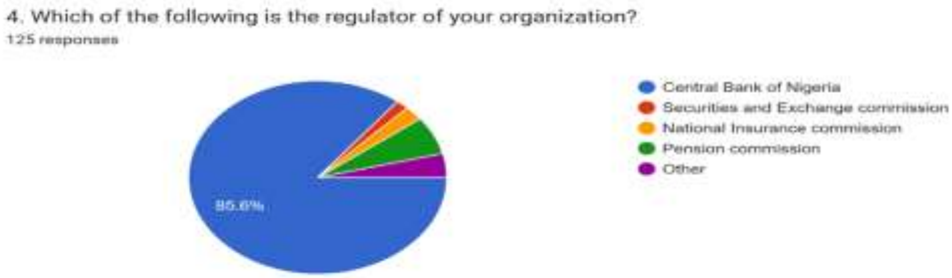
The gender categorization of respondents to the questionnaire survey indicates that 85.4% of respondents were males while 14.8% were females. This shows a significant level of gender diversity among respondents which also contributes to the richness of responses to the questionnaire survey.



84% of respondents were from the banking sector of the Nigerian financial services Industry, 7.2% respondents were from the pension sector, 3.2% from the Insurance sector, 2.4% from the Non-bank Financial institutions sector, 1.6% from the Mortgage sector and 1.6% from the Financial Markets sector.

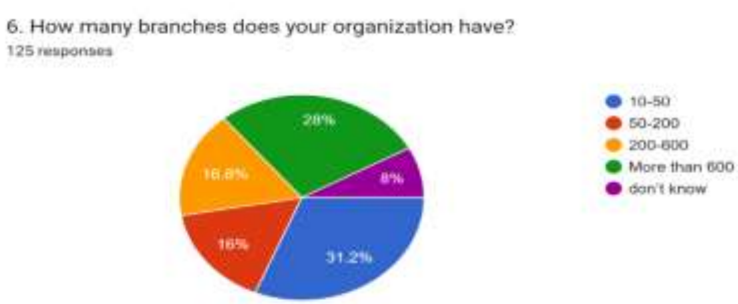


20% of respondents perform Applications administrator IT role in their organization, 10.4% perform Network Administrator IT role, 16% perform Cybersecurity specialist IT role, 53.6% perform another IT role.

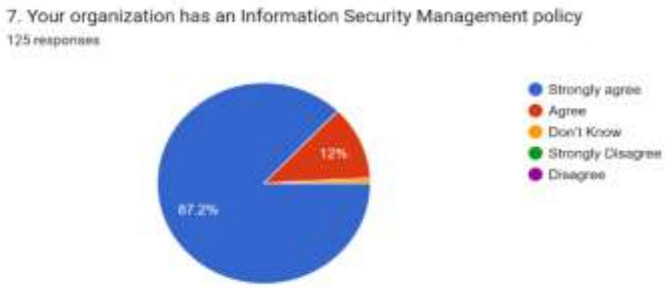


85.6% of respondents work in organizations that are under the regulatory purview of the Central Bank of Nigeria, 6.4% are under the regulatory purview of the Pension Commission, 2.4% are under the regulatory purview of the National Insurance commission,1.6% are under the regulatory purview of Securities and Exchange Commission and 4% are under other regulators within the industry.

34.4% of respondents work in organizations with staff strength of 10,000-20,000 staff, 26.4% work in organizations with staff strength of 1000-5000 staff, 8.8% work in organizations with 100-200 staff and 12.8% don't know the staff strength of their organization.

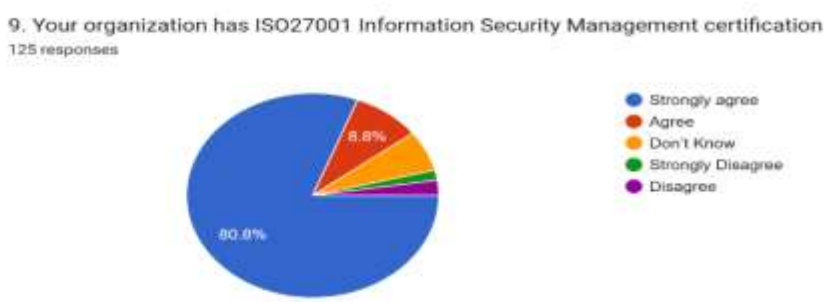


31.2% of respondents work in organizations that have 10-50 branches, 28% work in organizations that have more than 600 branches, 16.8% work in organizations that have 200-600 branches, 16% work in organizations that have 200-600 branches while 8% don't know the number of branches of their organization has.

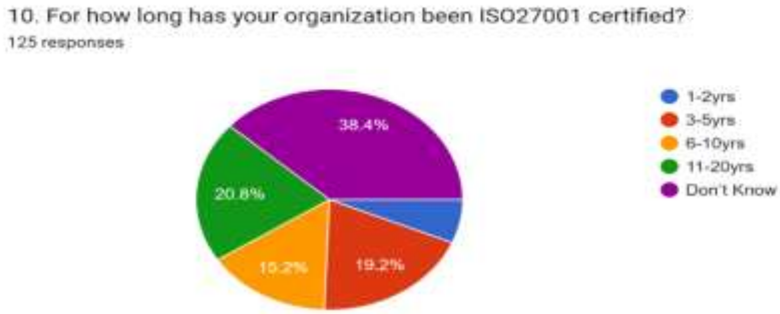


The existence and implementation of an information security management policy in an organization plays a very essential role in driving cybersecurity risk management in such organization. 87.2% strongly agree that their organization has an information security management policy, 12% agree that their organization has and 0.8% don't know and 0% strongly disagree and 0% disagree

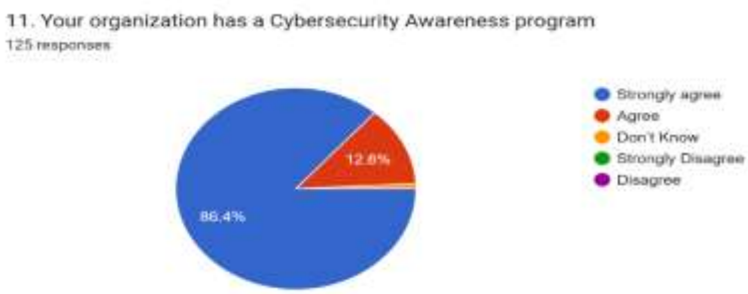
84.8% of respondents strongly agree that the information security management policy of their organization has adequate specifications for access control including multifactor authentication,12.8% agree, 1.6 % don't know and 0.8% strongly disagree, 0% disagree



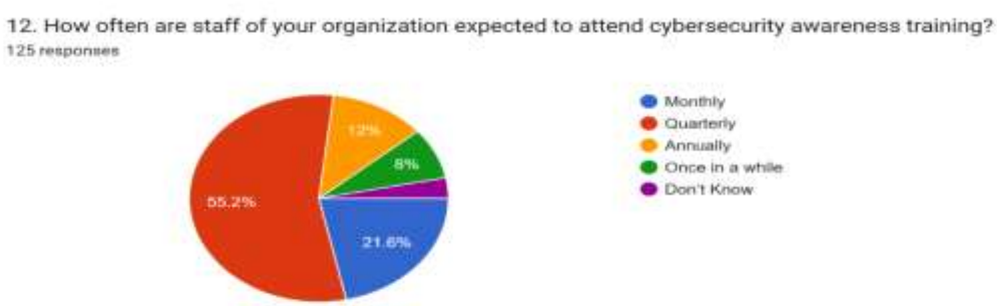
ISO27001 is a globally acclaimed Information security management standard that is very effective in driving corporate Cybersecurity risk management. It is a very comprehensive and robust standard for managing cybersecurity risk. Usually when an organization certifies to it, it undergoes rigorous re-certification Audit by the certification body every three years and rigorous surveillance Audit every other year. 80.8% of respondents strongly agree that their organization is ISO27001 certified, 8.8% agree, 6.4% don't know,1.6% strongly disagree and 2.4% disagree.



The duration of ISO27001 certification of an organization indicates the degree of how entrenchment of cybersecurity risk management in such organization.6.4% of respondents said the organization has been ISO27001 certified for between 1-2yrs,19.2% said 3-5yrs, 16.2% said 6-10yrs,20.8% said 11-20yrs and 38.4% don't know.

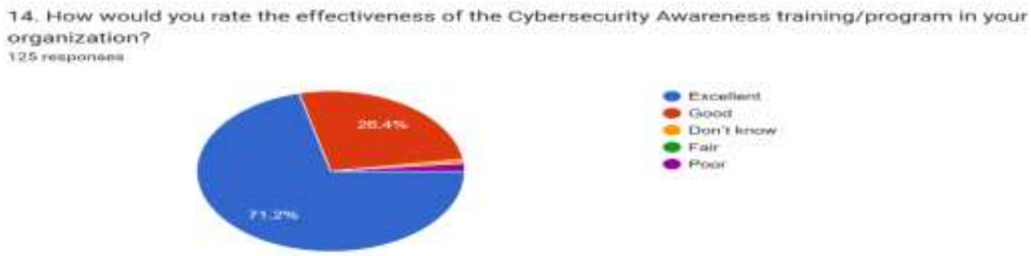


Cybersecurity Awareness program is a very essential means of managing cybersecurity risk in an organization. Cybersecurity risk management entails policies/processes, people and technology. From the people perspective, cybersecurity awareness program represents a very important component for risk management.86.7% of respondents strongly agree that their organization has a Cybersecurity Awareness program, 12.8% agree and 0.8% don't know.

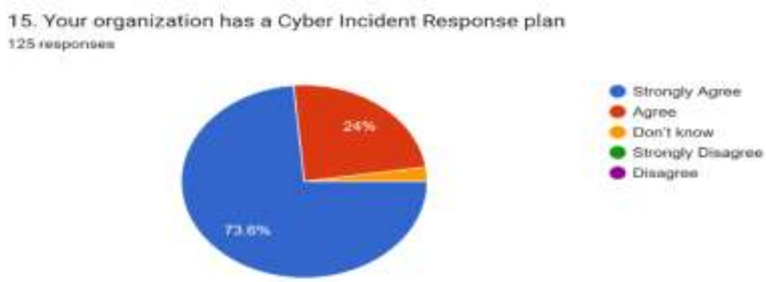


Regular Cybersecurity awareness training is very important in managing cybersecurity risk from the people perspective. 55.2% of respondents said staff are expected to attend Cybersecurity awareness training quarterly, 21.6% said monthly, 12% said annually,8% said once in a while 3.2% said they don't know.

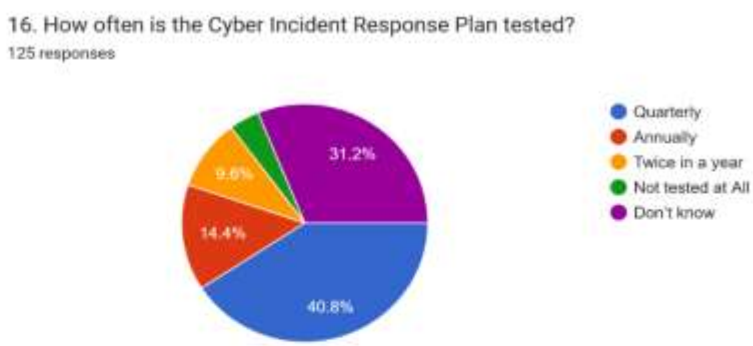
77.6% of respondents strongly agree to having attended a Cybersecurity Awareness training/program in their organization, 19.2% agreed,0% don't know, 0.8% strongly disagree while 2.4% disagree



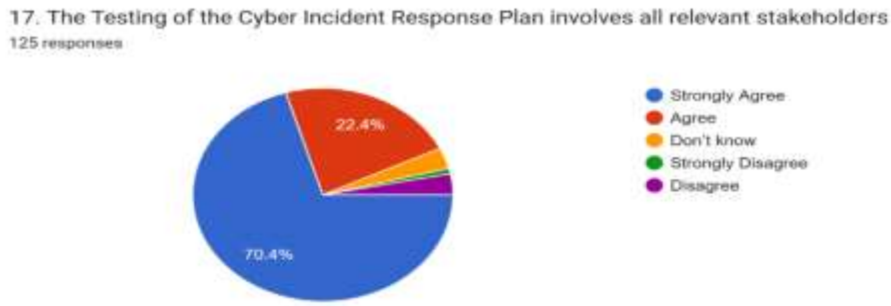
71.2% of respondents rate the effectiveness of the Cybersecurity Awareness training/program of their organization as being excellent, 26.4% rate it as being good 0.8% don't know,0% rate it as fair while 1.6% rate it as being poor.



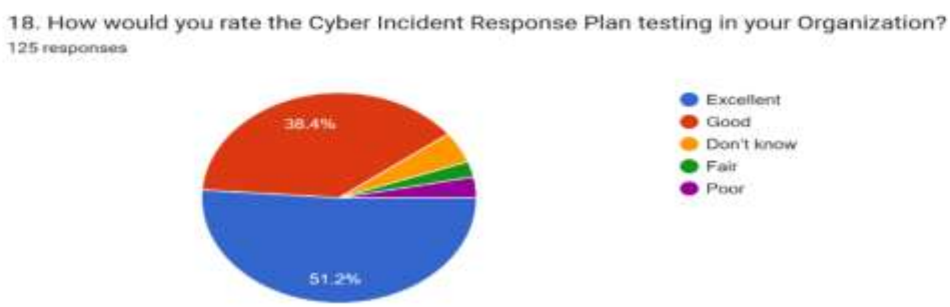
Cyber Incident Response plan testing is an essential cybersecurity risk management practice as it enables organizations to periodically assess their preparedness to manage Cyber incident when they happen. It also enables them to proactively identify gaps with a view to closing them.73.6% strongly agree that their organization has a Cyber Incident Response Plan, 24% agree and 2.4% don't know.



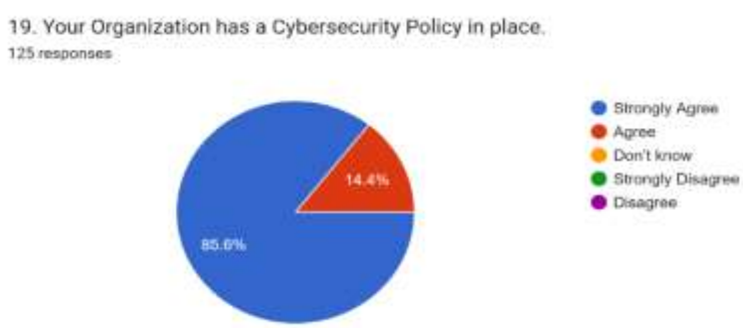
While it good for organizations to have a Cyber Incident Response Plan, it is also essential for such plan to be tested periodically to ensure effective cybersecurity risk management.40.8% of respondents said their organizations test their Cyber incident Plan quarterly, 31.2% don't know, 14.4% of respondents said annually9.6% said twice in a year and 4% said their organizations don't test their Cyber Incident Response plan at all.



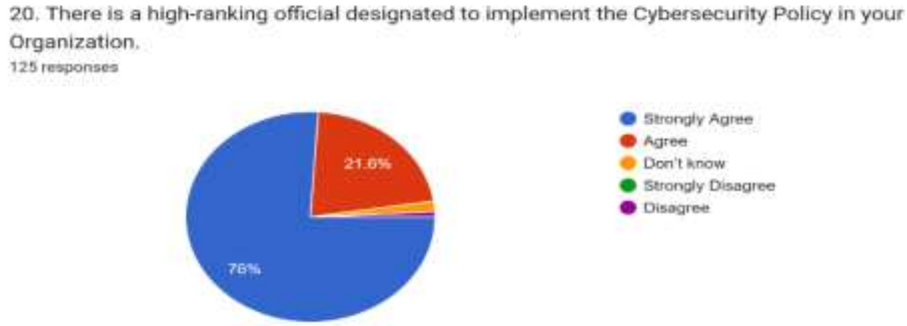
It is important that when Cyber Incident Response plan is tested in an organization all relevant stakeholders should be involved. This will enable the organization to properly assess the preparedness level of all stakeholders which in turn will help in ensuring the effectiveness of the plan.70.4% of respondents strongly agreed that the testing of the Cyber Incident Response Plan in their organization involves all stakeholders, 22.4% of respondents agree 3.2% don't know, 0.8% strongly disagree and 3.2% disagree



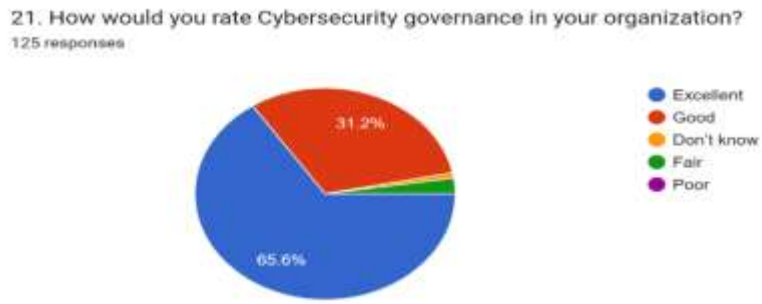
Cyber Incident Response plan testing is an essential cybersecurity risk management practice as such it essential that it is properly done by organizations.51.2% of respondents rated Cyber Incident Response plan testing in their organization as being excellent, 38.4% rated it as good 4.8% of respondents don't know, 2.4% rated as fair while 3.2% rated it as poor



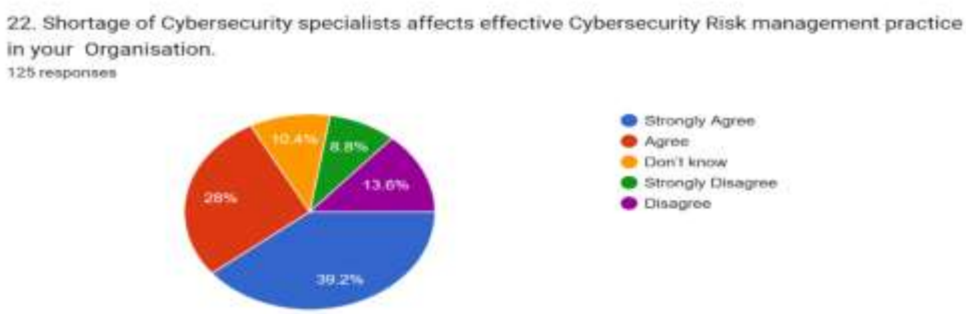
Cybersecurity Policy enables an organization to effectively and efficiently drive cybersecurity risk management practices. 85.6% of respondents strongly agreed that their organizations have a Cybersecurity policy in place and 14.4% of respondents agreed. This indicates a very high level of implementation of cybersecurity policy by organizations in the Nigerian Financial services industry.



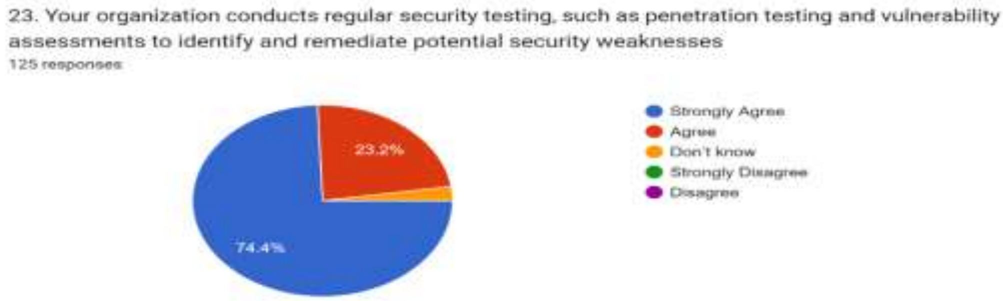
Effective Cybersecurity Risk management practice in an organization requires the active support and oversight of top management which implies that a senior management official should be designated to implement the Cybersecurity policy in the organization.76% of respondents strongly agreed that a high ranking officer is designated to drive implantation in their organization, 21.6% agreed, 1.6% don't know while 0,8% disagree.



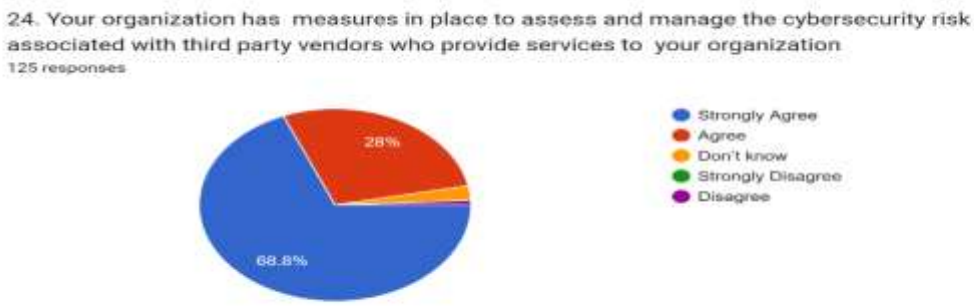
31.2% of respondents rated Cybersecurity governance in their organization as been excellent,31.2% rated it good,0.8% don't know,2.4% rated it fair while 0% rated it as being poor.



Cybersecurity risk management practice in organizations is largely driven by professions or specialists with the requisite know-how.39.2% of respondents strongly agreed that shortage of Cybersecurity experts affect effective cybersecurity risk management practice in their organization,28% agreed , 10.4% don't know 8.8% strongly disagreed while 13.6% disagreed.

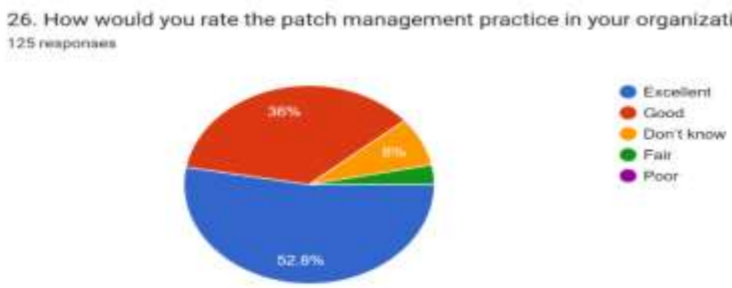


Regular Security Testing such as Penetration testing and vulnerability assessments is very essential Cybersecurity risk management measure as it enables organization to identify vulnerabilities and deploy remediation as quickly as possible.74.4% of respondents strongly agreed that their organization conduct regular Security testing, 23.2% agreed 2.4% don't know. This result indicates a significantly high level of Regular security testing in the industry.



Cybersecurity risk associated with Third party vendors is a significant risk factor in the industry as many organizations within the sector depend on third party vendor services.68.8% of respondents strongly agreed that their organizations have put measures in place to assess and manage third party risk, 28% agreed, 2.4% don't know 0% strongly disagreed while 0.8% disagreed. This indicates a high level of recognition of this risk factor by organizations in the industry.

A Patch management policy/process entails the application of patches or updates provided by OEMs(Original Equipment Manufacturers) on Applications and devices to remediate discovered vulnerabilities and improve functionality. This is an essential Cybersecurity Risk management practice.72.8% of respondents strongly agreed and 19.2% agreed that their organizations have a Patch management policy in place 6.4% of respondents didn't know if their organizations have it place while 1.6% disagreed that their organization have it in place.



52% of responders rated the patch management practice in their organization as excellent, 36% rated the practice as good in their organization, 8% didn't know the rating for their organization while 4% rated the practice poor in their organization. This indicates a significantly high patch management practice standard in the industry.

27. What additional steps do you think can be taken to improve Cybersecurity in your organization?

Responses include the following:

- Continuous learning and alignment with international best practices
- Mass sensitisation of staff
- Cyber Security Awareness Training of all cadre of staff.
- Never reuse passwords
- Operating a SOC (Security Operations Canter)
- More collaboration with external Vendors to Audit the existing process and identify gaps where applicable
- Use Encryption and Protect sensitive data both in transit and at rest
- SOC SIEM adoption
- Automate Manual process in our patch management procedures
- Improve endpoint compliance and patching cadence
- Carry out penetration test on application
- Industry Stakeholder Engagement, Third party risk reduction

DATA ANALYSIS AND RESULTS

In line with the research question 1 and objective 1, data obtained indicate that the following Cybersecurity Risk management practices are being practiced by most players in the Nigeria Financial Services industry

(i) Implementation of Information Security Policy

(ii) Designation of High ranking officers to oversight Corporate Cybersecurity programs

(iii) Implementation of Identity and Access Management to ensure that only authorized users access IT systems/services and roles are properly segregated

(iv) Implementation of Patch Management to ensure periodic Application of required patches/updates on IT Systems/services

(v) Certification to Cybersecurity Risk Management standards like ISO27001,PDCISS,etc

(vi) Implementation of Cyber Incident Plans/testing

(vii) Implementation of Cybersecurity training and Awareness for IT/Cybersecurity staff and other stakeholders

(viii) Mitigation of third-party cybersecurity risks

In line with Research question 2, the data revealed that the Cybersecurity risk management practices were more entrenched and better practiced in some sectors of the Industry than others. The banking sector is well ahead of the other sectors of the industry in terms of how well entrenched and robust Cybersecurity Risk Mangement practices are being carried out.

In line with Research question 3 and Objective 2, the gaps observed are as follows:

1. Some Regulators in the industry such as SEC and NAICOM are not yet certified to the ISO27001 standard and other globally recognized standards which are very important drivers of robust Cybersecurity risk management in organizations. This is impeding the entrenchment of Cybersecurity risk management practices by entities within the purview of those regulators.
2. There are coordination and collaboration gaps in terms of Cybersecurity Risk management practices in the industry which is hampering adequate reporting of Cybersecurity incidents and threat intelligence sharing.
3. The supervisory framework in some sectors of the industry is not robust and stringent enough to ensure adequate compliance with prescribed Cybersecurity Risk management guidelines by supervised entities.
4. The overall Cybersecurity training/Awareness level in the industry among all stakeholders is not yet at the level it should be.

In line with Objective 3, recommendations are proffered in the next chapter with a view to closing the identified gaps.

DISCUSSION OF FINDINGS

The data from both the Interview sessions/engagement and the online questionnaire survey indicate the following:

(i) Cybersecurity Risk management practices are more entrenched in the Banking sector of the industry than in the other sectors. This could be as a result of the fact that it is a mandatory requirement in that sector and enforcement as well as rigorous supervision is carried out.

(ii) Some Regulatory entities (SEC & NAICOM) are yet to be certified to Cybersecurity Risk Management standards such as ISO27001 that help ensure more comprehensive and robust cybersecurity risk management practices. This gap has made it difficult for them to ensure implementation by the regulated entities under their purview.

(iii) More Cybersecurity training for IT/Cybersecurity specialists in the Industry and awareness creation among other staff is required to ensure that people-associated risks are mitigated.

(iv) There is inadequate inter-sectoral Cybersecurity coordination and collaboration in the industry. This has created room for a lot of silo Cybersecurity activities and initiatives in the industry which does not augur well for common beneficial outcomes for all stakeholders.

RECOMMENDATIONS

1. Cybersecurity Incident reporting and disclosure should be taken seriously by stakeholders in the industry with a view to ensuring that investigations are quickly done, lessons are quickly learnt and corrective measures put in place quickly to forestall recurrence. Heavy punitive measures where necessary should be meted out to defaulters to ensure compliance. To make this more effective the Cybersecurity portal of CBN and other Regulators should be put into effective use.
2. The Nigerian Financial Industry Cybersecurity Emergency Response Center (NFIC) which is yet to come on stream should be implemented immediately by relevant stakeholders. This is meant to provide a centralized Security Operations Center for the Banking sector of the Industry. Other Sectors of the industry could also key into this initiative.
3. Cybersecurity Threat Intelligence sharing should be strengthened among the Financial Services industry players. The Financial Services Regulation Coordination Committee (FSRCC) should place more emphasis on coordinating Cybersecurity risk management practices in the Financial Services industry in conjunction with the National Cybersecurity Center given the criticality of the sector. The Banking sector is well ahead of the

other players in the sector, the others should be encouraged to catch up as quickly as possible because the industry is as strong as its weakest link.

4. The Regulators in the Financial services industry should make it mandatory for all regulated entities to be certified to Cybersecurity Risk Management standards such as ISO27001, PDCISS, etc. to ensure that Cybersecurity Risk management practices become more entrenched in all sectors of the industry.

5. Cybersecurity Incident Response Plan/Testing should be regularly done by all stakeholders to ensure better incident management and recovery.

6. There should be a shift to the Zero-Trust Network framework in the industry by stakeholders as a way of proactively confronting evolving Cyber threats and Attack methods. This framework enforces strict authentication requirement on users and devices.

7.Automation of some Cybersecurity Risk Management practices such as Patch management, Vulnerability assessment and remediation as well as others should be implemented by stakeholders in the industry by leveraging Artificial Intelligence.

8. Stakeholders in the industry should ensure the comprehensive and effective use of deployed Cybersecurity Risk management tools and solutions with a view to achieving maximum benefit realization from the investment made on such tools and solutions.

9. Regulators in the industry should work with the National Insurance Commission (NAICOM) towards introducing Cyber security Insurance as a viable Cybersecurity Risk management approach for industry players. This has been adopted in other countries.

Conclusion

The study was able to provide in-depth insights into the Cybersecurity Risk management practices in the various sectors of the industry and also identify gaps which need to be closed. Recommendations have been provided with a view to closing them.

REFERENCES

Arrogante, O (2022). Sampling techniques and sample size calculation: How and how many participants should I select for my research? Enfermería Intensiva 33 (2022) 44---47

Boston Consulting Group (2019). Reigniting Radical Growth Global Wealth 2019 retrieved from https://web-assets.bcg.com/img-src/BCG-Reigniting-Radical- Growth-June-2019_tcm9-222638.pdf

Fraenkel, J, R., Wallen, N. E., & Hyun, H. H. (2015). How to design and evaluate research in education. 9th ed, Singapore, Mc Graw Hill

Hassan, A, O, Ewuga, S, K,Abdul, A, A, Abrahams, T, O,Oladeined, M,Dawodu, S, O(2024). Cybersecurity in Banking: A global perspective with a focus in Nigerian practices

Kost, E(2024). The 6 biggest Cyber Threats for Financial services in 2024 retrieved from https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services

Lagazio M,Sherif N,Cushman M(2014).A multilevel approach to understanding the impact of Cybercrime in the Financial Sector

Ozarslan, S (2022).Key Threats and Cyber risks facing Financial Services and Banking firms in 2022