# Building a Cyber Fitness and Resilience in Financial Institutions in Nigeria using Hack Ability Score Technique and Cyber Security Self-Assessment Tool

ABDULKAREEM Hakeem Agboola
Head, Security Technology & Engineering, Access Banking Group

**Abstract:- The research work discusses the importance of cyber fitness and how financial institutions in Nigeria can improve their resilience to cyber threats. Cyber resilience in financial institutions refers to the ability of a financial institution to detect, respond to, and recover from cyber threats and attacks (Dupont, 2019). In achieving that, an in-depth analysis of the current approaches will be reviewed and come up with a robust Cybersecurity and Cyber Resilience process that can be adopted by any financial institution in Nigeria.**

**Generally, financial institutions operate in an increasingly digital world of which technology underlines their many innovations hence exposed to greater cyber risks which must be carefully managed in an ever-challenging environment.Building resilience in a financial institution is providing an enabling capability for such organisation to withstand and quickly recover from cyber-attacks that put into state of disruption usual business activities. It is imperative that any financial institution in Nigeria should have in place a robust Cyber Fitness and Resilience framework to protect such bank together with its assets in an agile environment.**

**Interviewing method was adopted in information gathering especially in identifying the different category of digital assets (including connected systems) of some selected top banks, their network architecture, current cybersecurity framework and Cybersecurity Maturity Level.**

## I. INTRODUCTION

In this technology-driven world, every business, regardless of the size, makes dedicated efforts to protect their sensitive data. This data could be about the staff, clients, business partners, internal operations, and more. But with the rise of sophisticated and targeted cyber attacks, it has become challenging to secure the infrastructure with cybercriminals using more advanced hacking tools, security has become an even more difficult job (McGee, Prusak and Pyburn, 1993).

Nigeria's digital financial ecosystem has seen impressive growth in recent years. According to Ladagu (2021), there are over 200 fintech organizations in Nigeria, not including fintech solutions by banks and mobile network operators. New service providers, ranging from mobile operators and payment service providers to fintech companies and other financial service providers, are driving an increasing need to ensure consumer security and trust.These services include numerous critical digital components, including mobile applications, digital tokens, Unstructured Supplementary Service Data (USSD), and digital ledgers, all of which contain potential vulnerabilities.

Consequently, the financial industry is a targeted area for cyberattacks, making cyber security a priority. Therefore, considering the a fore mentioned, businesses constantly work to find reliable defensive strategies against cyber attacks in financial institutions in Nigeria.

## II. OBJECTIVES

The key objectives of this dissertation are to conduct systematic reviews of cyber resilience of a typical financial institution by considering the entire network assets. The review offers an overview of the various levels of cyber resilience as well as core values. It also discusses and provides the latest solutions, tools and technologies in order to improve cyber resilience in the financial ecosystem. This research work also illustrates the latest trends that are involved in the methods of protection and attacks on critical assets in financial institutions.

Therefore, the outcome of this research work will include a cyber resilience process that can be adopted by any financial institution in ensuring that business is not disrupted in case of any cyber-attack as it will focus more on the underlisted areas:

- ***Vulnerability management process:*** providing tactical security vulnerability service across a financial institution and patching/hardening information to ensure only relevant findings are addressed.
- ***Governance upgrade***: establishing a streamlined reportingwith key performance indices (KPIs) and risk acceptances, then skill-up Information Security Officers across the selected case study offices/annexes.
- ***Red Team Establishment:*** set continuous in-depth end-to-end manual and automated attack testing and ramp-up support for the selected case study.
- ***Network Architecture:*** defining changes to the network for preventing systemic attacks based on hacking results.
- ***Monitoring***: detects gaps in current monitoring and advise on closing gaps, extend coverage across a financial institution, roll out and implement in-depth monitoring for assets and advise on implementation of new use cases,

measure and verify effectiveness of the bank's centralized Security Operations Control (SOC).

## III. LITERATURE REVIEW

A study by Adetunji and Okunoye(2019) conducted a survey of 100 financial institutions in Nigeria and found that only 37% of them had a documented cybersecurity strategy. The study identified lack of funding, lack of expertise, and lack of awareness as the major barriers to cyber resilience in Nigerian financial institutions.

Another study by Adebowale, Odetunmibi and Oluwadare(2020) examined the impact of cyber resilience on the performance of Nigerian financial institutions. The study found that cyber resilience positively influenced the performance of financial institutions in Nigeria, with a strong positive correlation between cyber resilience and profitability.

A research work by Alawode, Olusola and Okuboyejo(2021) examined the impact of cyber threats on financial institutions in Nigeria. The study found that Nigerian financial institutions faced a range of cyber threats, including malware, phishing, and ransomware attacks. The study also identified the need for continuous employee training and awareness as a key factor in improving cyber resilience.

Also, the Central Bank of Nigeria (CBN) has released guidelines on cybersecurity for financial institutions in Nigeria. The guidelines provide a framework for the management of cybersecurity risks and outline the roles and responsibilities of financial institutions, as well as providing guidance on incident response and reporting.Therefore, the CBN self-assessment framework will be used in addition to the vulnerability assessment to determine the bank's overall security posture (CBN, 2018).

Conclusively, the literature on cyber resilience in financial institutions in Nigeria highlights the need for increased investment in cybersecurity, improved employee training and awareness, and the adoption of a comprehensive cybersecurity strategy. By implementing these measures, financial institutions in Nigeria can improve their cyber resilience and protect themselves against the growing threat of cyber-attacks.

## IV. CYBERSECURITY LANDSCAPE OF A TYPICAL TIER -1 BANK IN NIGERIA

The arc below provides a summary of Cybersecurity Landscape of a typical tier-1 financial institution in Nigeria highlighting the different categories of security solutions identified during the review exercise. However, those highlighted in red color represent the missing solutions that are recommended to be put in place in order to be in line with defense-in-depth approach.

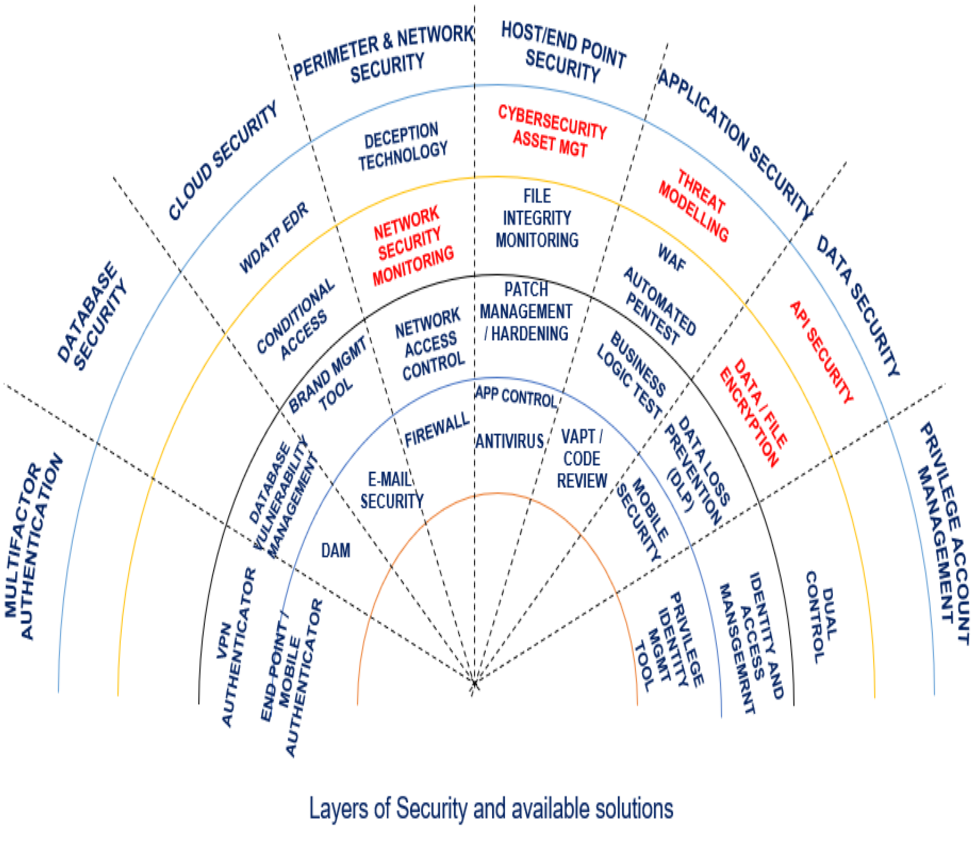

Fig. 1: Layers of Security and available Solutions

Cybersecurity refers to the measures taken to protect computer systems and networks from digital attacks, theft, and damage. While Cyber resilience is the ability of an organization to recover from a cyber-attack or other disruption to its online operations.

Cybersecurity and cyber resilience are important for banks as they handle sensitive financial information and process many online transactions, making them a prime target for cyber-attacks. A successful cyber-attack on a bank could result in the loss of customer data, financial losses, and damage to the bank's reputation.

In assessing the current security posture of a typical financial institution in Nigeria, one needs to identify and assess its current security posture including the types of assets, systems and networks that are in use, and the potential vulnerabilities and threats that they are exposed to.

## V. VULNERABILITY MANAGEMENT

Vulnerability Management is a crucial process for maintaining the security of a financial institution's systems and data. The general methodology for vulnerability management includes the following as related to a typical financial institution:

- ***Inventory:*** Identifies and inventory all hardware and software assets within the financial institution.
- ***Assessment:*** Perform regular vulnerability assessments of the bank's systems and applications to identify vulnerabilities that could be exploited by attackers. This includes using automated tools as well as manual testing.
- ***Prioritization:*** Prioritize vulnerabilities based on their potential impact on the bank's operations and data, as well as the likelihood of exploitation. This includes considering the potential financial impact of a successful attack.
- ***Remediation:*** Develop and implement a plan to remediate vulnerabilities in a timely manner. This includes patching systems and applications, updating software, and reconfiguring systems as needed.
- ***Verification:*** Verify that vulnerabilities have been successfully remediated through follow-up testing and validation.
- ***Continuous monitoring:*** Continuously monitor the institution 's systems and applications for new vulnerabilities and repeat the vulnerability management process on an ongoing basis.

## VI. BUSINESS CASES FOR CYBER RESILIENCE

Cyber resilience is essential to the success and reputation of any financial institution in Nigeria, and therefore, there are several arguments that can be made for the bank to investing in cyber resilience measures. These arguments including:

- ***Protection against cyber threats:*** Cyber threats such as hacking, malware, and phishing attacks can result in significant financial losses and reputational damage. Investing in cyber resilience measures can help protect the bank against these threats.
- ***Compliance with regulations:*** In Nigeria, just like in every part of the world, financial institutions are subject to numerous regulations related to data protection and cybersecurity. Failing to comply with these regulations can result in significant penalties and legal consequences. Therefore, investing in cyber resilience measures can help such financial institution to ensure compliance with the set regulations.
- ***Business continuity:*** A cyber-attack or breach can disrupt the bank's business operations, leading to financial losses and reputational damage. Investing in cyber resilience measures can help ensure business continuity and minimize the impact of a cyber incident at such institution.
- ***Protection of customer information:*** Financial institutions collect and store sensitive customer information, including personal and financial data. A breach of this information can result in significant harm to customers and damage to the bank's reputation. Investing in cyber resilience measures can help protect customer information and maintain their trust in the institution.
- ***Competitive advantage:*** In today's digital age, customers expect financial institutions to have robust cybersecurity measures in place. By investing in cyber resilience, you can differentiate your institution from competitors and gain a competitive advantage.

## VII. VALUATION OF CYBER RESILIENCE

The valuation of cyber resilience in a financial institution in Nigeria can be approached in several ways. One possible approach is to consider the potential costs of a cyber-attack and compare them to the cost of implementing cyber resilience measures.

Some potential costs of a cyber-attack on a financial institution could include:

- ***Financial losses from theft or fraud:*** Cyber-attacks can result in direct financial losses from stolen funds, fraudulent transactions, or ransom payments.
- ***Reputational damage:*** A cyber-attack on a financial institution can damage its reputation and erode customer trust, which can lead to lost of business and revenue.
- ***Legal and regulatory costs:*** A cyber-attack may trigger legal and regulatory action, resulting in fines, legal fees, and other costs.
- ***Operational disruption:*** A successful cyber-attack can disrupt operations, leading to downtime, lost productivity, and the need for remediation efforts.
- Therefore, to assess the value of cyber resilience measures, financial institutions in Nigeria could consider the potential benefits of implementing cybersecurity measures, such as:
- ***Enhanced protection against cyber threats:*** Cyber resilience measures such as firewalls, encryption, and multi-factor authentication can help protect against cyber threats.
- ***Increased customer trust:*** By implementing effective cybersecurity measures, financial institutions can demonstrate to customers that they take data protection seriously and can be trusted with sensitive information.

- ***Compliance with regulations:*** Cyber resilience measures can help financial institutions meet regulatory requirements for data protection and cybersecurity.
- ***Business continuity:*** Effective cyber resilience measures can help financial institutions maintain operations in the face of cyber threats, reducing the risk of downtime and lost productivity.

## VIII. METHODOLOGY

Developing a methodology for cyber resilience in a financial institution in Nigeria requires a comprehensive approach that involves different steps and considerations. Therefore, going by the literature review where the existing approach of vulnerability management and cybersecurity maturity level were comprehensively reviewed, below are some of the key elements that will form the fulcrum of the methodology to be adopted for this project:

- ***Risk Assessment:*** The first step in developing a cyber resilience methodology for a financial institution in Nigeriais to conduct a comprehensive risk assessment. This process involves identifying and analyzing the potential cyber threats and vulnerabilities that the institution faces, as well as the potential impact of these threats on its operations, finances, and reputation.
- ***Security Policy and Governance:*** The next step is to establish a strong security policy and governance framework that outlines the bank's security objectives, roles, and responsibilities of stakeholders, and the measures that will be taken to mitigate cyber risks.
- ***Technical Controls:*** A critical part of the methodology involves the implementation of technical controls that can help to detect, prevent, and respond to cyber threats. Examples of technical controls include firewalls, intrusion detection and prevention systems, anti-virus software, and encryption technologies.
- ***Incident Response Plan:*** A comprehensive incident response plan will be developed by deepening the existing plan, to guide the bank's response to cyber incidents. The plan would outline the roles and responsibilities of stakeholders, the procedures for reporting and escalating incidents, and the steps that will be taken to contain, investigate, and remediate incidents.
- ***Employee Training and Awareness:*** Employees are an important part of any financial institution's cyber resilience strategy, and the regular awareness and training programme will be deepened on security best practices, such as password management, phishing awareness, and incident reporting.
- ***Regular Testing and Evaluation:*** The effectiveness of the cyber resilience methodology will be regularly tested and evaluated to ensure that it remains relevant and effective in addressing the evolving cyber threats facing the institution. A clear and objective-based Key performance indeces (KPIs) will be prepared for the bank's Red Team to guidetheir continuously probing of the bank's environment.
- ***Compliance:*** Compliance with relevant regulatory frameworks, such as the Nigeria Data Protection Regulation (NDPR) and the Central Bank of Nigeria's Cybersecurity Guidelines, will also be considered in developing the new methodology.

Therefore, the new methodology recommended to improve the bank's maturity risk level is a combination of Hackability Scoretechnique and Cybersecurity Self-Assessment Tool by Federal Financial Institutions Examination Council (FFIEC) in United States. And the required information could be obtained through interview sessions of some selected stakeholders in a typical financial institution using the sample Questionnaire below:

- What security measures are in place to protect yourbank's computer systems and networks from cyber-attacks?
- Does your bank have a documented incident response plan for responding to cyber security incidents?
- How often are employees trained on cyber security awareness and best practices?
- Does your bank conduct regular vulnerability assessments and penetration testing on its computer systems and networks?
- What is the process for reporting and addressing cyber security incidents within your bank?
- What are the challenges of remediating identified vulnerabilities in your bank?
- What measures are in place to prevent unauthorized access to sensitive information?
- How does your bank ensure third-party vendors comply with its cyber security policies and procedures?
- Has your bank ever experienced a significant cyber security incident, and if so, what steps were taken to prevent a recurrence?
- Does your bank have a disaster recovery plan in place in case of a cyber security incident?

## IX. TECHNIQUES TO IMPROVE CYBER RESILIENCE – HACKABILITY SCORE

Hackability Score is a technique used to assess the vulnerability of a computer system or network to cyberattacks. It is a quantitative measure that considers various factors that can make a system susceptible to hacking (SRLabs, 2020). This approach entails an introduction of technical hacking Key Performance Indices (KPI) to guide the cyber resilience journey in an ever-dynamic financial institution summarises both the current posture of a typical financial institution and point to remediation with a well-prepared guide as well as handholding engagement to achieve result. Therefore, the Hackability Score is based on a set of criteria that includes:

- ***Vulnerability to known exploits:*** The score considers whether the bank is susceptible to known security vulnerabilities and exploits, such as malware or other types of attacks.
- ***Security configurations:*** The score considers whether the bank has appropriate security configurations in place, such as firewalls, intrusion detection and prevention systems, and antivirus software.
- ***Patching and updates:*** The score evaluates whether the bank is up-to-date with the latest security patches and updates.

- ***Access control:*** The score considers whether the bank has appropriate access controls in place, such as password policies, user permissions, and authentication mechanisms.
- ***Network segmentation:*** The score considers whether the bank is properly segmented and isolated from other networks, such as internal networks or the internet.
- ***Data protection:*** The score evaluates whether the bank has appropriate data protection measures in place, such as encryption or backup and recovery systems.
- ***Incident response:*** The score considers whether the system has an effective incident response plan in place to quickly detect, respond to, and recover from security incidents.

The Hackability Score is calculated based on these criteria, with higher scores indicating a higher likelihood of a successful cyberattack. The score can be used by the bank to assess their own systems and networks, or by third-party auditors to evaluate their security posture. See below the breakdown.

Table 1: Third-party auditors to evaluate their security posture

| **Severity** | **Rating for vulnerability findings** | **Hackability Score per finding (Base Score)** | **Hackability Score per organization** |
|---|---|---|---|
| 5 | Instantly exploitable issue | 15 | **Absolute Hackability Score = Base Score * sqrt(occurrences)**<br>Each additional finding of the same type counts less(hence the square root)<br>**Normalized Hackability Score = Absolute Hackability Score * 10 / sqrt(ports)** |
| 4 | Exploit fragment that can be used to craft successful attack | 5 | |
| 3 | Issues that may reveal sensitive information to enable further attackers. | 1 | E.g., Log4j issue with severity 5 occurs 4 times<br>→ Base score = 15<br>→Absolute Hackability Score = 15 *sqrt (4) = 30<br>The **Absolute Hackability Score** is a weighted score calculated over all vulnerabilities identified in the institution.<br>→Normalized Hackability Score = Absolute Hackability Score * 10/Sqrt(services)<br>Ports/services – 144 open ports<br>→ Normalized Hackability Score = 30 * 10/Sqrt (144)<br>→ Normalized Hackability Score = 300/12 =25<br>→ Normalized Hackability Score = 25<br>Services/ports – total number of open portse.g. https, smtp, ftp, ssh, http, ssl etc.<br>**Normalized Hackability Score compares** the level of security in the institution by putting the absolute Hackability in relation to their IT infrastructure size. |
| 2/1 | Best practice deviation | 0 | |

## X. SELF-ASSESSMENT CYBERSECURITY MATURITY LEVEL

In June 2015, the Federal Financial Institutions Examination Council (FFIEC) in United States released the Cybersecurity Assessment Tool to help institutions of all sizes identify their risks, assess their cybersecurity preparedness and help inform their risk management strategies. The content of the assessment tool is based on National Institute of Standards and Technology (NIST) cybersecurity framework and other industry accepted cyber security practices.

According to CBN (2018), Central Bank of Nigeria had adopted and mandated all the Deposit Money Banks (DMBs) in Nigeria to use the self-assessment tool to conduct a comprehensive assessment of their cybersecurity programmeto determine its current Cybersecurity Maturity Level (CML) with the sole aim and objective of improving it. Consequently, to establish a cyber fitness culture in a typical financial institution towards building a robust cyber resilience, the underlisted categories are considered during the assessment:

- Cyber Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cybersecurity Controls
- External Dependencies Management
- Cyber Incident Management and Resilience

Below is a typical summary report of assessment conducted using the CBN Self-Assessment tool.

Table 2: Typical summary report of assessment conducted using the CBN Self-Assessment tool

| S/No | Domain | Assessment Factor | Maturity Level | Observation | Recommendation |
|---|---|---|---|---|---|
| 1 | Cyber Risk Management and Oversight | Governance includes oversight, strategies, policies, and IT asset management to implement an effective governance of the cybersecurity program. | | | |
| | | Risk Management includes a risk management program, risk assessment process, and audit function to effectively manage risk and assess the effectiveness of key controls. | | | |
| | | Resources include staffing, tools, and budgeting processes to ensure the institution’s staff or external resources have knowledge and experience commensurate with the institution’s risk profile. | | | |
| | | Training and Culture includes the employee training and customer awareness programs contributing to an organizational culture that emphasizes the mitigation of cybersecurity threats. | | | |
| | | Threat Intelligence refers to the acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action to enhance decision making. | | | |
| | | Monitoring and Analyzing refers to how an institution monitors threat sources and what analysis may be performed to identify threats that are specific to the institution or to resolve conflicts in the different threat intelligence streams. | | | |
| | | Information Sharing encompasses establishing relationships with peers and information-sharing forums and how threat | | | |

| | | | | | |
|---|---|---|---|---|---|
| 2 | Threat Intelligence and Collaboration | information is<br>communicated to those groups as well as internal stakeholders. | | | |
| 3 | Cybersecurity Controls | Preventative Controls deter and prevent cyber-attacks and<br>include infrastructure management, access management, device and end-point security, and secure coding. | | | |
| | | Detective Controls include threat and vulnerability detection, anomalous activity detection, and event detection, may alert the institution to network and system irregularities that indicate an incident has or may occur. | | | |
| | | Corrective Controls are utilized to resolve system and software vulnerabilities through patch management and remediation of issues identified during vulnerability scans and penetration testing. | | | |
| 4 | External Dependency Management | Connections incorporate the identification, monitoring, and management of external connections and data flows to third parties. | | | |
| | | Relationship Management includes due diligence, contracts, and ongoing monitoring to help ensure controls complement the institution's cybersecurity program. | | | |
| 5 | Cyber Incident Management | Incident Resilience Planning & Strategy incorporates resilience planning and testing into existing business continuity and disaster recovery plans to minimize service disruptions and the destruction or corruption of data. | | | |
| | | Detection, Response, & Mitigation refers to the steps management takes to identify, prioritize, respond to, and mitigate the effects of internal and external threats and vulnerabilities. | | | |
| | | Escalation & Reporting ensures key stakeholders are informed about the impact of cyber incidents, and regulators, law enforcement, and customers are notified as | | | |

| | | | | | |
|---|---|---|---|---|---|
| | and Resilience | required. | | | |
| **Risk Rating Maturity Level:** | | | | | |
| **Recommendation:** | | | | | |

**Innovative:** Innovative maturity is characterized by driving innovation in people, processes and technology for the institution and the industry to manage cyber risks. This may entail developing new controls, new tools, or creating new information sharing groups. Real-time predictive analytics are tied to automated responses.

**Advanced:** Advanced maturity is characterized by cybersecurity practices and analytics that are integrated across lines of business. Majority or risk-management processes are automated and include continuous process improvement. Accountability for risk decision by frontline businesses is formally assigned.

**Intermediate:** Intermediate maturity is characterized by detailed formal processes. Controls are validated and consistent. Risk-management practices and analysis are integrated into business strategies.

**Evolving:** Evolving maturity is characterized by additional formality of documented procedures and policies that are not already required. Risk-driven objectives are in place. Accountability for cybersecurity is formally assigned and broadened beyond protection of customer information to incorporate information assets and systems.

**Baseline:** Baseline maturity is characterized by minimum expectation required by law and regulations or recommended in supervisory guideline. This level includes compliance-driven objectives. Management has reviewed and evaluated guidance.

**Sub-Baseline:** Sub-Baseline maturity is characterized as operating below the FFIEC cybersecurity / resilience baseline.

Table 3: Cyber Fitness And Maturity Level Assessment Scope Of Work (Sow)

| Research Area | Sub Research Area | Cyber Fitness Deliverables | Description | Outcome of Cyber Resilience in Financial Institution | Duration (Week) |
|---|---|---|---|---|---|
| Measure Hacking Resilience | | Red Team security assessments | Setup Red Team Penetration Testing Tools. | Reliable cyber<br>baseline and Key Performance Indices (KPIs) (i.e., Hackability score – External and Internal Networks)<br>across the case study | 8 |
| | | | Conduct tactical end-to-end security assessments of the financial institution. | | |
| | | | Generate a list of highly likely hacking vectors that need to be addressed on priority. | | 4 |
| | | Broad continuous Hackability scans | Scan for security issues for both External (Internet) and internal network. | | |
| | | | Results in a maturity view that allows comparison between Case study and external peers. | Acquisition of International standard certifications like ISO 22301, ISO 27001, ISO 28000 etc. | |
| | Strengthen vulnerabil | Continuous cyber<br>fitness training of resource persons | Prepare improvement plan, remediation guide and structure it in easy-to implement cyber fitness units for different remediation teams in the Case | Vulnerability management measure to continuously "fix the basics" through | 6 |

| | | | | | |
|---|---|---|---|---|---|
| Improve hacking<br>resilience | ity<br>management | | study. | a cyber fitness plan. | |
| | | Cyber health alerts | Fast-track issues that are exploited in the wild for immediate remediation and additional monitoring. | An improved Mean Time To Detect (MTTD) and Mean Time To Recover (MTTR)<br>to intrusions | |
| | Ramp-up<br>security<br>monitoring | Continuous testing of identified attack vectors | Regularly send artificial attack vectors to measure detection coverage and agility of security operation center (SOC). | | |
| | | | Come up with improvement pack from each scan. | | |
| | | SOC ramp-up targeted training program | Conduct workshops and individual trainings for SOC analysts. | | |

## XI. RED TEAM SETUP AND ACTIVITIES

According to Amin, K., & Sharma, P. (2020) a Red Team is a group of ethical hackers that simulate attacks on an organization's systems, networks, and infrastructure to identify weaknesses and vulnerabilities. Therefore, as part of the cyber fitness exercise towards achieving a cyber resilience in a typical financial institution, see below some key steps that can be followed in setting up Red Teaming activities:

- ***Scope Definition:*** The scope of the entire cyber fitness activities should be well defined and based on the bank's risk profile and threat landscape. This will help to ensure that the Red Team's efforts are focused on areas that are most critical to the bank's operations. The entire engagement with the bank is set for 24weeks as contains in the statement of work (SOW).
- ***Train Red teamers:*** Ensure passionate cyber security professionals are trained to be highly skilledwith a strong background in cybersecurity, ethical hacking, and penetration testing so that they would be able to simulate attacks that replicate the tactics, techniques, and procedures used by real attackers.
- ***Establish rules of engagement:*** Rules of engagement that defined the scope, objectives, and limitations of the Red Team's activitiesshould be highlighted and same be discussed as part of the collaboration's efforts bythe bank's IT and cyber security teams with clear guidelines on how to report vulnerabilities and exploit them responsibly.
- ***Conduct regular assessments:*** Regular and continuous assessments should be conducted by Red team (to identify new vulnerabilities and assess the effectiveness of the bank's cybersecurity controls) as a necessity to ensure that the bank's systems and infrastructure remain secure over time.A comprehensive Red Teaming exercise should be carried out regularly and share report that contains the details of the vulnerabilities, the overall hackability score, prioritized vulnerabilities for urgent remediation and the related remediation guides andfollow up to ensure that the identified vulnerabilities are remediated promptly.
- ***Collaborate with the Blue Team:*** The Red Team should work closely with the bank's Blue Team (i.e., the defenders) to ensure that vulnerabilities are remediated promptly and that the bank's cybersecurity posture is continuously improving.
- ***Document findings and recommendations:*** The Red Teamshould document all findings and recommendations in a detailed report. The report should therefore include a prioritized list of vulnerabilities, recommendations for remediation, and a summary of the Red Team's activities.
- ***Continuously improve:*** The Red Team's activities are continuously evaluated and improved based on feedback from the bank's IT and cyber security teams as this helps in ensuring that the team's efforts remain relevant and effective over time.

Therefore, throughout this research work some Vulnerability Assessment and Penetration Testing (VAPT) tools like Kali Linux, Nessus, the CBN cybersecurity self-assessment tool and Blood Hound (Blood Hound is an Active Directory reconnaissance and attack path management tool that uses graph theory to identify hidden relationships, user permissions, sessions, and attack paths in a source Windows domain) were leveraged on.

## XII. BLUE TEAM SETUP AND ACTIVITIES

A Blue Team is a group of IT and cyber security professionals responsible for defending an organization's systems, networks, and infrastructure against cyber attacks (Seker and Ozbenli, 2018).). Therefore, below are some key steps to be taken in setting up a Blue Team for cyber resilience in a typical financial institution:

- ***Scope Definition:*** The scope of the Blue Team's activitiesshould be defined based on the bank's risk profile and threat landscape as that helps in ensuring that the Blue Team's efforts are focused on areas that are most critical to the bank's operations.
- ***Train and Hire Blue Teamers:*** Blue Team members are the administrators that are highly skilled in their respective IT and Cyber security departments with a

strong background in cybersecurity, incident response, and threat intelligence as they are able to detect and respond to cyberattacks quickly and effectively.

- ***Incident Response Procedures Establishment:*** Incident response procedures should be established to ensure that the Blue Team canrespond to security incidents in the entire institutionin a timely and effective manner. The procedures include clear guidelines on how to identify, contain, and remediate security incidents.
- ***Systems and Networks Monitoring:*** The Blue Team should continuously monitor the organization's systems and networks for signs of suspicious activity. This will help to detect security incidents early and minimize their impact.
- ***Security Controls Implementation:*** Security controls such as firewalls, Anti-DDoS solution, intrusion detection systems, Proxy solutions and antivirus software to mention a few should be thoroughly tested for effectiveness, checked to have been configured correctly and updated regularly toprevent and detect cyberattacks.
- ***Conduct regular vulnerability assessments:*** Leveraging on VAPT tools and with good collaboration with the Red Team, the Blue Team caries out regular vulnerability assessments to identify weaknesses in the bank's systems and infrastructure.
- ***Collaborate with the Red Team:*** The institution's Blue Team should work closely with the Red Team (i.e., the ethical hackers) to ensure that vulnerabilities are remediated promptly.
- ***Document incidents and lessons learned:*** As part of the cyber fitness, the Blue Team documents all security incidents and. The report usually includes a summary of the incident, the response actions taken, and recommendations for improving the bank's cybersecurity posture.
- ***Continuously improve:*** The Blue Team's activities are therefore advised to be continuously evaluated and improved based on feedback from the bank's IT and cyber security teamsgot through regular engagement as this helpsin ensuring that the Blue Team's efforts remain relevant and effective over time.

## XIII. DIGITAL FORENSIC AND INCIDENT RESPONSE (DFIR) LABORATORY

It is imperative to have a well functional, effective, skilled and responsive DFIR team that can always respond to any incident quickly with the main objective to curtail immediately, investigate and submit report whilst ensuring business continuity at all times in a typical financial institution. Consequently, a Digital Forensics and Incident Response (DFIR) team's core activities shouldfollow a well structed process as captured in the steps below:

- ***Incident Identification:*** The first step in the bank's DFIR process is to identify any incident or suspicious activity which could be a report of a security breach, unusual system behaviour, or any other indicator that suggests a security incident has occurred. The bank's central Security Operations Center (SOC) should be relied upon for this identification.
- ***Evidence Preservation:*** Once an incident has been identified, the next step is to preserve any potential evidence related to the incident. This includes making copies of affected systems, logs, network traffic, and other digital artifacts that may be relevant to the investigation.
- ***Analysis:*** With the evidence preserved, the next step is to analyze the data to determine the scope and nature of the incident. This involves reviewing logs and other data sources, identifying potential attack vectors, and attempting to trace the origins of the incident.
- ***Containment:*** Once the scope of the incident has been identified, the next step is to contain the incident and prevent any further damage or data loss. This may involve isolating affected systems, disabling user accounts, or other measures to prevent the attacker from further access or escalation within or outside the bank.
- ***Eradication:*** After the incident has been contained, the next step is to eradicate any malicious code or other artifacts associated with the incident. This may involve removing malware, patching vulnerabilities, or taking other measures to prevent the attacker from re-establishing access or connecting to any command and control on the internet.
- ***Recovery****:* Once the incident has been eradicated, the final step is to restore systems and data to their previous state. This involves verifying that all systems are secure and free from any residual malicious code and ensuring that any data that may have been lost or corrupted during the incident is recovered.

Finally, the ultimate goal of the DFIR process in a typical financial institutionis to minimize the impact of the incident on the bank's operations and reputation, while also preventing similar incidents from occurring in the future.

## XIV. FUTURE WORK

One potential future work for financial institutions to improve their cyber resilience is to conduct regular security assessments to identify vulnerabilities and assess the effectiveness of their cybersecurity measures. This can include penetration testing, vulnerability scanning, and security audits.

Another important future work for financial institutions is to implement a cybersecurity framework that aligns with industry best practices and regulatory requirements. The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a widely adopted framework that provides a comprehensive set of guidelines and practices for managing and reducing cybersecurity risks.

Financial institutions can also benefit from investing in advanced technologies such as artificial intelligence and machine learning to enhance their cybersecurity capabilities. These technologies can help identify potential threats and vulnerabilities, detect anomalies in user behavior, and automate certain aspects of incident response.

In addition to technological solutions, financial institutions must also prioritize employee training and awareness as a critical component of their cybersecurity strategy. This includes providing regular cybersecurity training to all employees, implementing strict access controls and authentication measures, and establishing clear policies and procedures for responding to cybersecurity incidents. Beyond training both the Red teamers and the Blue Teamers, the entire workforce should be trained regularly especially on social engineering techniques that adversaries can use to exploit to steal not only their confidential information but that of the bank.

Also, financial institutions must also prioritize the importance of third-party risk management. This involves assessing the cybersecurity posture of third-party vendors and partners who have access to the institution's systems and data. It's crucial to ensure that third-party vendors are also implementing appropriate cybersecurity measures to protect against cyber threats.However, the process can be improved upon by introducing an end-to-end Threat Modelling practice.

Finally, in the future, setting up an automated vulnerability scanner on ELK (Elasticsearch, Logstash, Kibana) can help any financial organisation to detect and remediate security vulnerabilities in your system such that there would also be at a glance dashboard that provide visualization real-time online of the status of every asset of the bank as well as the vulnerability status.

## XV. CONCLUSION

Overall, achieving cyber resilience in financial institutions is a complex and ongoing process that requires a holistic approach, involving people, processes, and technology, and continuous monitoring and improvement of the overall security posture.

Also, investing in cyber resilience measures is a critical business decision for financial institutions. It can help protect your organization against cyber threats, ensure compliance with regulations, maintain business continuity, protect customer information, and gain a competitive advantage.

Lastly, the value of cyber resilience in a financial institution in Nigeria will depend on factors such as the specific threats facing the institution, the potential costs of a cyber-attack, and the costs and benefits of implementing cybersecurity measures. It is important for financial institutions to conduct a thorough risk assessment and cost-benefit analysis to determine the most effective cyber resilience strategy for their specific needs.

In conclusion, cyber resilience is a critical issue for financial institutions, and there is a range of potential future work that can be undertaken to improve their cybersecurity posture. By prioritizing regular security assessments, adopting industry best practices and advanced technologies, investing in employee training and awareness, and managing third-party risk, financial institutions can enhance their cyber resilience and protect themselves against evolving cyber threats. I believe if financial institutions can reference this research work it would not only improve their exiting process but will project them on the right path towards achieving a cyber resilience financial industry that can support and grow the country’s economy.

## REFERENCES

[1.] Amin, K., & Sharma, P. (2020). Red Team Analysis of Information Security Measures and Response.

[2.] CBN (2018) *Risk-based cybersecurity framework and guidelines for deposit money banks and payment service providers* Available at : https://www.cbn.gov.ng/out/2018/bsd/risk%20based%20cybersecurity%20framework%20final.pdf (Accessed: 19 March 2023

[3.] Dupont, B. (2019) The cyber-resilience of financial institutions: significance and applicability. *Journal of cybersecurity*, *5*(1), tyz013.

[4.] ISA cybersecurity (2019) Cybersecurity for the Transportation Sector Available at :https://isacybersecurity.com/cybersecurity-for-the-transportation-sector/(Accessed: 08 August 2022).

[5.] Ladagu, N. D. (2021). *Factors for Sustainable Operations in the FinTech Industry. A Survey of Nigerian Users, Providers and Regulators*. University of Wales Trinity Saint David (United Kingdom).

[6.] McGee, J. V., Prusak, L., & Pyburn, P. J. (1993). *Managing information strategically: Increase your company's competitiveness and efficiency by using information as a strategic tool* (Vol. 1). John Wiley & Sons.

[7.] Prospero (2020) Cyber Security Threat Landscape and Challenges in the Transportation Sector Available at: https://www.virtual.prosperoevents.com/blog/cyber-security-transportation

[8.] (Accessed: 02 August 2022).

[9.] PWC (2019) *Building a Cyber Resilient Financial Institution* Asian Institute of Chattered Bankers Kuala Lumpur

[10.] SRLabs (2020) Cyber Fitness based on Proven Framework by Security Research Labs Available at: https://www.srlabs.de(Accessed: 10 August 2022).

[11.] Seker, E., &Ozbenli, H. H. (2018). The concept of cyber defence exercises (cdx): Planning, execution, evaluation. In *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-9). IEEE.