# RESEARCH DESIGN, METHODOLOGY, QUESTIONNAIRE AND CASE STUDY, SYSTEM ANALYSIS.

## INTRODUCTION

Design has to do with the process whereby steps are been taking for the collection and analyzing of data that are necessary to solve some certain problem, such that the contrast of the various steps that are taken during the cost of obtaining accuracy and the expected valuable information in accordance to every level of such accuracy is magnified. This is divided into series of prior decisions which gives a strategic way of executing a research project.

### RESEARCH DESIGN

A research work was carried out in Access Bank Nigeria PLC which constitutes a number of population for study, as it is impossible to study the networking system of the entire bank, which is located in Ikorodu Lagos state branch in Nigeria. A survey technique was adopted by the researcher, an estimated of 100 population was targeted for this study.

## POPULATION AND SAMPLE SIZE

In this area of study, a population was used from different part of the bank which comprises of technical department, accounting department, networking department and financial department. A total number of 100 parastatals was taken for this research which are experience and professionals.

## SAMPLE TECHNIQUE

A sample was taken from the said bank in question in a wild view which involves the security implication of electronic banking. Based on this, an estimated population of 100 was taken. Using the population taken, a sample size was calculated.

Given the formular

n =

where N = population size

Z = Z-score

e = margin of error

n = sample size

at 95% confident level over Z = 1.96

e = 5%

n =

n =

n =

n = 79.346

n = 79

so out of 100 population at 5% margin error the sample size is 79

## RESEARCH METHODOLOGY

In defining research, is a systematic investigation taken by studying a source and material in a way to find out fact and additional information through data interpretation, analysis and planning.

When we talk about methodology is a system method which is structured approach in a specific area such as designs and analysis. In a nutshell research methodology is a specific technique which is use in identifying, processing, selecting and analyzing of information about a particular area or topic. It is also know as given a description details of what a researcher is planning and the necessary steps that is taken in gathering facts which is vital for this project. There are several methods which was use this include oral interviews, questionnaires and observation.

### ORAL INTERVIEW

This has to do with the obtaining of information from the respondent by the researcher and it also involve the recording of such first-class information. In this aspect a primary research and a secondary research was carried out

#### PRIMARY RESEARCH

This research was done in the process of interviewing some staff of the access bank from separate department by sharing questionnaires among them, but mostly from the computer department of the bank. A flexible question was asked by me to the information technologist on how data is been transmitted from their different branches and what problems that they experience in the transmission of data. Lastly, a computer operator was interviewed in other to acquire more information about the networking in computer security and firewall, it was successfully carried using these methods.

## SOURCES AND METHOD OF DATA COLLECTION

Data were collected in this project work in primary and secondary sources

### PRIMARY SOURCE

In this type of source data was collected through personal participating, visits, distribution of questionnaire to the said bank and observation, where the bank assistance regarding this project yielded a good result. This method was used personally to curtail any form of prejudice in the investigation of this object.

### SECONDARY SOURCE

This category has to do with the collection of data through relevant literature which are gotten from journals, books. Newspapers, magazines. Consequence, the internet was also among this category of collection as it is valuable.

### 

### **QUESTIONNAIRE FOR PRIMARY RESEARCH**

An adjustment of sampling method was selected for this project which is due to consistent and engagement of some staffs of the bank who most time engages in different activities. So, I shared questionnaires among the staff who shows interest. Designing of questionnaire by the researcher for the staffs who works in Access Bank Nigeria PLC in Ikorodu branch Lagos state, several staff was picked. A several short, structured question was constructed which are of course processed and typed, also a closed structure of combination was used, the use of an open type questionnaire was implemented so as to give the respondent the freedom of expression in their own views in their area of specification.

Please tick ▼ the appropriate answer

* What is your name?
* State your occupation?
* Gender

1. Male
2. Female

* Is it true that all the operations of this bank are computerize?

1. Yes
2. No

* The use of computer technology in performing bank services is this used by this bank.?

1. Yes
2. No

* Can you please indicate the range at which this bank uses computer technology in offering a computer-based system payment?

1. Large range
2. Small range
3. sometimes
4. No range

* please indicate the range of problem impacted in electronic payment system of your bank.?
* Lack of infrastructure in the aspect of communication links and power supply

1. Large range
2. Small range
3. Sometimes
4. No range

* The lack of provision of adequate security and fraud prevention

1. Large range
2. Small range
3. Sometimes
4. No range

* Lack of skilled workers and necessary equipment on end users coupled with the client system

1. Large range
2. Small range
3. Sometimes
4. No range

* Exorbitant cost of E-payment services.

1. Large range
2. Small range
3. Sometimes
4. No range

* At what range the government support in improving the E-banking system?

1. Large range
2. Small range
3. Sometimes
4. No range

* Do you agree that the computer services payment has yielded a good profit to your bank.?

1. Yes
2. No

* At what range in the introduction of electronic payment has improve in your bank.?

1. Large range
2. Small range
3. Sometimes
4. No range

* To what range has this bank correctly apply security pattern in application in the context of a model security?

1. Large range
2. Small range
3. Partially
4. No range

* In your bank, do all security mechanism have a quantitative resources consumption?

1. Yes
2. No

* Have your bank experience any attack from external source?

1. Yes
2. No

* Does your bank have the most effective tools for simulating cyber-attacks?

1. Yes
2. No

* To what range has your bank tried in the improvement of information security system collected in social media portal database?

1. Large range
2. Small range
3. Partially
4. No range

* To what range as your bank encounter challenges in cloud security?

1. Large range
2. Small range
3. Partially
4. No range

* To what range is you bank defense in depth?

1. Large range
2. Small range
3. Partially
4. No range

* Has your bank had any abuse of privilege?

1. Yes
2. No

* How well does your bank uses log retention?

1. Large range
2. Small range
3. Partially
4. No range

* To what range a layer 7 firewall block a web security threat of your bank?

1. Large range
2. Small range
3. Partially
4. No range

* The use of blockchain technology has it improve the security of information transfer on the internet of the bank?

1. Yes
2. No

* To what range has your bank inform the customers about cybercrime attacks on electronic online banking?

1. Large range
2. Small range
3. Partially
4. No range

* To what range has the development of data processing technology of big data of your bank improve the credit risk management process?

1. Large range
2. Small range
3. Partially
4. No range

* To what range as your bank establish policies to combat future attacks?

1. Large range
2. Small range
3. Partially
4. No range

## **RETURNED QUESTIONAIRES FOR THE PRIMARY RESEARCH**

in all for the primary research a total of 60 questionnaires were distributed to staffs of Access Bank Nigeria PLC where 50 were returned, these 50 questionnaires were use as the basis of our conclusion and data analysis.

## OBJECTIVES

* Is it true that all the operations of this bank are computerize?

1. Yes
2. No

|  |  |  |
| --- | --- | --- |
| VARAIBLES | FREQUENCY | PERCENTAGE % |
| YES | 35 | 65 |
| NO | 15 | 35 |
| TOTAL | 50 | 100 |

In this table it shows that 35 respondents of the bank representing 65% agreed that their bank is computerized fully. While 15 respondents representing 35% did not concur to this, so most Nigeria banks are well computerized.

* The use of computer technology in performing bank services is this used by this bank.?

1. Yes
2. No

|  |  |  |
| --- | --- | --- |
| VARAIBLES | FREQUENCY | PERCENTAGE % |
| YES | 50 | 100 |
| NO | - | - |
| TOTAL | 50 | 100 |

In total all the respondents agreed to this.

* Can you please indicate the range at which this bank uses computer technology in offering a computer-based system payment?

1. Large range
2. Small range
3. sometimes
4. No range

|  |  |  |
| --- | --- | --- |
| VARIABLES | FREQUENCY | PERCENTAGE % |
| LARGE RANGE | 40 | 88 |
| SMALL RANE | - | - |
| SOMETIMES | - | - |
| NO RANGE | 10 | 12 |
| TOTAL | 50 | 100 |

In this, 40 respondents which represent 88% says that the bank is placed at a large context in the use of computer technology in offering a computer-based system payment, while 10% disagreed to this.

* please indicate the range of problem impacted in electronic payment system of your bank.?

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Problem | Large range | Small range | partially | No range | Percentage % |
| Infrastructure deficiency & erratic power supply | 15 | - | - | - | 28.5 |
| Non-provision of adequate security for fraud prevention | - | - | - | 13 | 26 |
| Inadequate skilled workers and necessary equipment on end users coupled with client system | - | - | - | - | - |
| Exorbitant cost of E-banking services | 7 | - | - | - | 16 |
| Lack of government support on improvement of E-banking | 15 | - | - | - | 28.5 |
| TOTAL | 50 |  |  |  | 100 |

Looking at this table, we found out that infrastructure deficiency and erratic power supply has a great impact in majority banks in Nigeria as 28.5% attest to this, while 13 respondents representing 26% attest that non-provision of adequate security in the banking sector is partially not always, as 15 respondents representing 28.5% attest to this that there is lack of support from government on the improvement of E-banking, more so, 16% respondents recertified that there are high range of exorbitant cost of E-banking services.

* Do you agree that the computer services payment has yielded a good profit to your bank.?

1. Yes
2. No

|  |  |  |
| --- | --- | --- |
| VARIABLES | FREQUENCY | PERCENTAGE % |
| YES | 40 | 89 |
| NO | 10 | 11 |
| TOATAL | 50 | 100 |

In this table, a total of 49 respondents representing 89% believed that the computer services payment has yielded a good profit to the bank while 11% of the respondent disagrees.

* At what range in the introduction of electronic payment has improve in your bank.?

1. Large range
2. Small range
3. Sometimes
4. No range

|  |  |  |
| --- | --- | --- |
| VARIABLE | FREQUENCY | PERCENTAGE % |
| LARGE RANGE | - | - |
| SMALL RANGE | 5 | 10 |
| PARTIALLY | 10 | 22 |
| NO RANGE | 35 | 68 |
| TOTAL | 50 | 100 |

In the table we see that 35 respondents representing 68% agreed that the introduction of electronic payment has not improve in the bank, as 22% says partially while 5 respondents representing 10% says that it has a small impact in their bank.

* To what range has this bank correctly apply security pattern in application in the context of a model security?

1. Large range
2. Small range
3. Partially
4. No range

|  |  |  |
| --- | --- | --- |
| VARIABLE | FREQUENCY | PERCENTAGE % |
| LARGE RANGE | - | - |
| SMALL RANGE | 30 | 70 |
| PARTIALLY | 10 | 15 |
| NO RANGE | 10 | 15 |
| TOTAL | 50 | 100 |

A number of 30 respondent agrees that the bank has a little correction of applying security pattern in application in the context of modern security while 15% says the bank has not correctly applying security pattern in application in the context of modern security, 10 respondents says the bank partially does.

* In your bank, do all security mechanism have a quantitative resources consumption?

1. Yes
2. No

|  |  |  |
| --- | --- | --- |
| VARIABLE | FREQUENCY | PERCENTAGE % |
| YES | 27 | 59 |
| NO | 23 | 41 |
| TOTAL | - | 100 |

This table above shows that 27 respondents representing 59% agrees that all security of the bank has quantitative resource consumption in all the security mechanism of the bank while 41% do not.

* Have your bank experience any attack from external source?

1. Yes
2. No

|  |  |  |
| --- | --- | --- |
| VARIABLE | FREQUENCY | PERCENTAGE % |
| YES | 50 | 100 |
| NO | - | - |
| TOTAL | 50 | 100 |

A whole number of respondents agreed that their bank have experience several attacks from external source. As this been said, it shows that most Nigeria banks do experience several attacks from intruders.

* Does your bank have the most effective tools for simulating cyber-attacks?

1. Yes
2. No

|  |  |  |
| --- | --- | --- |
| VARIABLE | FREQUENCY | PERCENTAGE % |
| YES | 35 | 60 |
| NO | 15 | 40 |
| TOTAL | 50 | 100 |

In this table, 35 respondents representing 60% recertified that their bank has the most effective tools for simulating cyber-attacks while 15 respondent representing 40% disagrees to this, well it shows that most banks in Nigeria have most effective tools for simulating cyber-attacks.

* To what range as your bank encounter challenges in cloud security?

1. Large range
2. Small range
3. Partially
4. No range

|  |  |  |
| --- | --- | --- |
| VARIABLE | FREQUENCY | PERCENTAGE % |
| LARGE RANGE | 30 | 60 |
| SMALL RANGE | 15 | 25.5 |
| PARTIALLY | 5 | 14.5 |
| NO RANGE | - | - |
| TOTAL | 50 | 100 |

In this table 30 respondents representing 60% agrees that their bank experience challenges in cloud security in a large context, while 15 respondents representing 25.5% says at a small context and 5 respondents says its partially.

* To what range is you bank defense in depth?

1. Large range
2. Small range
3. Partially
4. No range

|  |  |  |
| --- | --- | --- |
| VARIABLE | FREQUENCY | PERCENTAGE % |
| LARGE RANGE | 45 | 90 |
| SMALL RANGE | 5 | 10 |
| PARTIALLY | - | - |
| NO RANGE | - | - |
| TOTAL | - | 100 |

A couple of respondents representing 90% agrees at a large context that their bank uses defense in depth while 5 respondents representing 10% says at a small context.

* To what range a layer 7 firewall block a web security threat of your bank?

1. Large range
2. Small range
3. Partially
4. No range

|  |  |  |
| --- | --- | --- |
| VARIABLE | FREQUENCY | PERCENTAGE % |
| LARGE RANGE | 40 | 85 |
| SMALL RANGE | 10 | 15 |
| PARTIALLY | - | - |
| NO RANGE | - | - |
| TOTAL | 50 | 100 |

As this table implies 40 respondents representing 85% agrees at a large range that layer 7 firewall block a web security threat of their bank while 10 respondents representing 15% placed it at a small range.

* To what range has your bank inform the customers about cybercrime attacks on electronic online banking?

1. Large range
2. Small range
3. Partially
4. No range

|  |  |  |
| --- | --- | --- |
| VARIABLE | FREQUENCY | PERCENTAGE % |
| LARGE RANGE | 15 | 35 |
| SMALL RANGE | 30 | 50 |
| PARTIALLY | 5 | 15 |
| NO RANGE | - | - |
| TOTAL | 50 | 100 |

In this table 30 respondents representing 50% says that the bank is place at a small context in informing it customers about cybercrime attack on electronic online banking while 15 respondents representing 35% placed it at high range and 5 respondents places it partially. This shows that most banks in Nigeria is not doing enough in informing its customers about cybercrime attacks on electronic online banking.

* At what range has your bank detect an intrusion?

1. Large range
2. Small range
3. Partially
4. No range

|  |  |  |
| --- | --- | --- |
| VARIABLE | FREQUENCY | PERCENTAGE % |
| LARGE RANGE | 15 | 35 |
| SMALL RANGE | 30 | 50 |
| PARTIALLY | 5 | 15 |
| NO RANGE | - | - |
| TOTAL | 50 | 100 |

A total of 15 respondents representing 35% says that their bank has detect an intrusion in a large context while 30 respondents representing 50% says at a small context and 15% of the respondents says partially. This tend to show that there is high rate of bank intrusion in most Nigeria banks.

* To what range your bank put in policies to combat future attacks?

1. Large range
2. Small range
3. Partially
4. No range

|  |  |  |
| --- | --- | --- |
| VARIABLE | FREQUENCY | PERCENTAGE% |
| LARGE RANGE | 20 | 35 |
| SMALL RANGE | 25 | 45 |
| PARTIALLY | 5 | 10 |
| NO RANGE | - | - |
| TOTAL | 50 | 100 |

In this table 20 respondents representing 35% agrees that their bank policies is put at a large context when it comes to future attack while 25 respondents representing 45% says its placed at a small range, and 5 respondent representing 10% acknowledged that the bank is placed partially. This shows that the banks in Nigeria must do more in establishing strong policies to combat future attacks.

* Has your bank had any abuse of privilege?

|  |  |  |
| --- | --- | --- |
| VARIABLE | FREQUENCY | PERCENTAGE % |
| YES | 10 | 15 |
| NO | 40 | 85 |
| TOTAL | 50 | 100 |

Well the table says it all, as 40 respondents representing 85% says there is no abuse of privilege in their bank as 10 respondent disagrees to this. It really shows that most Nigeria banks have no abuse of privilege.

## **ORAL INTERVIEW QUESTIONS FOR PRIMARY RESEARCH**

well this was done by interviewing a staff who works in Access Bank Nigeria PLC, questions was asked by me so as to know how well banks in Nigeria are secured when it comes to their network compare to other banks here in Ireland.

* There is different element of cybercrime security which are networking security, information security, operational security, application security and business continuity planning which element of these cybercrime security you are stationed in your bank.
* Networking security
* We understand that Traceroute is use in the banking sector can you please state how this tools use in your bank?
* We use traceroute in our bank to check the breakage of connections and to identify the failure of that connection, we mostly use these tools when we see that packet does not reaches its destination.
* Brute force attack is a trial and error method to find out the right password which is been

use by hackers so can you please explain how your bank prevent this brute force attack?

* Well in our bank we set up a password length also increases the password complexity, lastly a limit is set on login failure that will now bar the access of such login.

.

* The term Man-In-The-Middle (MITM) attack is commonly used by hackers can you please explain why do they use it and how do you protect the customer against this?
* Well hackers uses Man-In-The-Middle attacks in other to access confidential information , this attack occurs in between two hosts that communicate with each other by listening to their conversations which act as main in the middle, and they uses some techniques in caring this act such as sniffing, packet injection and so on, and its sometimes difficult to detect such attack, that’s why a proper steps needs to be taking by always checking if the communication have been intercepted and checking of proper page authentication also the implementation of tamper detection is a good way to detect such attack. It is very important to take measures before such MITM occur, there are good ways we protect our customers from such attack, by having a very strong encrypted apparatus on our network to prevent unauthorize users from interfering such tools are public key pear based authentication.
* In my study of security in banking I found that some people are very good in hacking can you please explain to me how you classify these people?
* These are people who are very versatile in breaching network security, they can generate malwares for their own personal uses, they mostly breaks into networks in other to steal, modify and destroy all information or data so that such network will not be access by authorized users and this people are called black hat hackers

* How do you protect against potential vulnerability in your network security?
* As this case implies, we use a booster access control by using a strong password system. Which involve upper- and lower-case letters, characters and numbers inclusive. Also, we keep all software updated (automatic software update) and we use a standard software whereby users cannot just install any software into the system without approval
* During this pandemic we notice that most people are made to do their transaction online and as a means of this most hackers have derive various means as heaven for them to steal information and carry out their fraudulent activities so what tools do you think bank should put in place to combat such attacks?
* I will suggest the use of Risk-Based Authentication to prevent attackers to gain access into customers account by the use of security images and combination of challenging questions this will help the customer to identify any phishing site, well as phishing site will not be able to show the correct image for that customer this will enable the customer to know that it’s a phishing site and will not enter their credential. The use of a Multi-Factor Authentication is very important this also prevent attackers to intrude into customers account, these method include RSAs SecurID keyfob system, electronic keyfob which uses algorithm in generating complex pass code in every 60 seconds, and also the use of Real-Time Out-Of-Band Transaction Alert.
* The use of VPN is regarded as one of the major tools in network security can you please explain how important is this in banking security?
* VPN is use in our bank because is safer and all information are encrypted and secure from intruders, our VPN have a strict no-logs policy thereby keeping all data and browser history safe
* When it comes to security, authentication is very important so how do you implement the Two Factor Authentication (2FA) for a public website?
* Well we implement the 2FA the use of a unique code, this code is sent through our mobile application or text message, users are allowed to access the website when this code are entered cause the website will always prompt them to enter the secured code
* Accidental threat was one time use by a bank manager in a bank where I deposited money can you please explain the meaning of accidental threat to my understanding?
* oh yes, accidental threat are threat that are mistakenly carried out by the employees of the bank, they do this by mistakenly deleting files or by accidentally sharing confidential information or data with other business partners or outsiders without considering the policy of the bank. Well in our bank these things occur frequently. That is why a strict policy has now been put in place in dealing with such act.
* During my research I found the word Trojan virus which was commonly used by hackers in your own words can you explain this term?
* well the words Trojan Horse comes from the Greeks, is a type of virus that are also one of the non-physical threat hackers uses, it appears typically as a piece of malware that attaches to mails which comes from an untrusted source, it is a resemblance software that convince users to download it into their computer, once this is downloaded the hackers can then access the said computer.

### OBSERVATION

Most part the bank activities were computerized, and this method yielded a good result as the researcher was clever enough to observe and watch other part of activities that was done in the bank, direct observation was inquired by the researcher to understand those activities that were difficult. However, the researcher was notified on how security measure are been taken in ensuring that there is availability and integrity during sharing of information and how the flow of data is transmitted from one location of the bank to another. Using this method, it was very successful, where fresh certitude was obtained and taking from the said bank.

### NETWORK ANALYSIS

For it headquarter to communicate effectively within its branches, Access Bank Nigeria PLC sticks to three different class of network, such as Local Area Network (LAN), Metropolitan Network (MAN) and Wild Area Network (WAN). In the LAN, the ban uses this for inter-office data communication, while the MAN is use by the bank in the communication of intra-city between Lagos territories. The bank uses WAN to communicate among all Access Bank within the nation. As this may said the usage of WAN, Access Bank and its branches uses telecommunication facilities which include messages switching or packet, satellite transmission and optical fibre media.

The topology which the bank implemented is stapled at star topology, but in some cases the ring and hybrid topology are used in an exceptional situation. In this star topology the entire network is controlled by a communication program which is coming from the host computer also known as hub which is situated at the center of the star. Using this process, the bank has the ability in the aspect of accessing the company account also updating all information within its terminal connection present in the network which is usually routed within the center, one of the major aspect of this topology when using it, is that the network (star) cannot be hindered by any of the connected cables or devices facilities which is distinctly depending on the central hub, there are several device which are connected, they include keyboard, terminals, input/output device or microcomputers.









SCANNER

COMPUTER







FILE SERVER

PRINTER

COMPUTER

A STAR TOPOLOGY NETWORK DIAGRAM

There are two classes of physical equipment that is use in implementing the network. The specific communication equipment which is needed for the network and the other computer peripherals. The bank controls the network hub with the use of microcomputer and file server. The devices that helps in handling writing and reading of files to hard disk which provide access to the files is known as file server. The computer peripherals that is been used are IBM compatible. Some of these devices include keyboard, visual display unit (VDU), printers, magnetic ink character recognition (MICR) which are basically used to store, read and output information or data.

* visual display unit: as the name implies which display images that are been generated by the electronic device or computer.
* Keyboard: as this is not new to the ears, it uses for the transmission of data to the CPU for processing which do accept numeric and non-numeric data.
* Magnetic ink character recognition: this is known as the lines that appears at the bottom of checks.

Multiplexor and modern are special communication equipment which are obtained by the bank. Access Bank Nigeria PLC engages in the use of NOVELL operating system. Their operating system has different functions.

* Correction and detection of errors
* The provision of connection links is made.
* It allows the disconnection of link should there be a security breach.
* Act as a backup disk for the recovery of copied information.

### SYSTEM PROPOSAL

In this proposal, implementation that was used in this system was stated by the researcher, the system that was proposed is the security firewall system. To ensure adequate security of data, security program must be written. The use of firewall approach is very vital because some level of separation that exist between the internet and the internal network of the organization must be provided, most attacks on the information are perform by the means of illegal or legal hardware interface that are sticked to the network or the network communication system. The use of fibre optical system should be implemented in application where there is high security because of their lack of emission which makes them difficult should incase of making tapping impossible. An organization must define its security policies as firewall does not stand alone.

### OBJECTIVES OF THE SYSTEM

In an organization like banks, firewall is employed in checkmating the crime associated with the network, this is because there is various threat to the integrity and confidentiality of some important data. This is useful because is helps the organization to provide access to authorized users in the network and can also disconnect an unauthorized user from the network either inside or outside. More so, an organization security and policies measures must be taken in the implementation of firewall because most policies do dictate the protection of the data.

## **SECONDARY RESEARCH**

This was carried out in Ireland by interviewing a staff who works in Bank in America based in Ireland. Different questions were asked in the engineering sector how the bank operates in the protection of their data against intruders. Although it was same question that was asked by me to a staff of Access Bank Nigeria PLC, this is because to know how banks from different continent operate in the protection of their data again intruders. A full detailed information was taken as this method was successful.

### ORAL INTERVIEWED QUESTIONS ON SECONDARY RESEARCH

* State your occupation?
  + Software Engineer
* Gender

1. Female

* Is it true that all the operations of this bank are computerize?

We are a global bank and, have a digital bank offering. We have some operations that require human interaction. But wherever possible, we try to automate and computerize processes.

* The use of computer technology in performing bank services is this used by your bank.?

Yes

* At what range in the introduction of electronic payment has improve in your bank.?

1. Large range
2. Small range
3. Sometimes
4. No range

* How does your bank correctly apply security pattern in application in the context of a model security?

As a bank, we develop software with a security first approach. We have several security controls and measures in place to protect our systems.

When developing and releasing a new feature, your code must be scanned. And the libraries used in your program must be complaint with the pre-determined measures set in place internal. There must be no known defect with the module. If there are any defects flagged by the security review, the code will not be permitted into production environment

* In your bank, do all security mechanism have a quantitative resources consumption?
  + No
* Have your bank experience any attack from external source?
  + Fortunately, as a bank, we have not experienced and major data breeches or security attacks. We have hired and built out departments specifically to detect, prevent and mitigate such attacks.
* Does your bank have the most effective tools for simulating cyber-attacks?
* Yes
* How often your bank encounter challenges in cloud security?
  + Yes, we have faced many challenges when it comes to adoption of public cloud. Many of these are due to the extra security measures that banks need to have in place. Many of these challenges will be addressed and resolved before we decide to use a cloud service.
* does your bank use its defense in depth?
* Yes
* Has your bank had any abuse of privilege?
  + No
* How does your bank use a layer 7 firewall block in web security threat?
  + We use layer 7 MTLS in some of our end-to-end components. Whenever we have traffic going over the internet, we use MTLS to ensure the integrity of the data being transmitted.
* To what range has your bank inform the customers about cybercrime attacks on electronic online banking?

1. Large range
2. Small range
3. Partially
4. No range

* What are the policies your bank has put in place to combat future attacks?
  + We have internal security protocols. For example, in AWS, we block all public access to our s3 buckets. We also use the principle of least privilege which means all access is denied by default and only explicitly allowed actions will be allowed.
  + We have incorporated several DdoS protection in our web applications.
  + We Ensure all staff complete mandatory Cybersecurity training quarterly.
  + We go through a rigorous onboarding process for new software and software components to ensure all software meet the minimum outlined requirements.
  + As a bank, We MUST adhere to strict banking regulations which means we must report all security and production incidents to the Banking regulators.
* At what range has your bank detect an intrusion?

1. Large range
2. Small range
3. Partially
4. No range

* At what range the government support in improving the E-banking system?

1. Large range
2. Small range
3. Sometimes
4. No range

* please can you tell the range of problem impacted in electronic payment system of your bank. Which am going to ask you?
* Lack of infrastructure in the aspect of communication links and power supply

1. Large range
2. Small range
3. Somethings
4. No range

* The lack of provision of adequate security and fraud prevention

1. Large range
2. Small range
3. Sometimes
4. No range

* Lack of skilled workers and necessary equipment on end users coupled with the client system

1. Large range
2. Small range
3. Sometimes
4. No range

* Exorbitant cost of E-payment services.

1. Large range
2. Small range
3. Sometimes
4. No range

* We understand that Traceroute is use in the banking sector can you please state how this tools use in your bank?

We use traceroute to test connectivity between a client and server, We use it to count the number of hops between a client and a server in other to determine at what point a connection might be dropped or how long it take to reach the server, We may also use it to pinpoint the arears were latency may occur.

* Brute force attack is a trial and error method to find out the right password which is been

use by hackers so can you please explain how your bank prevent this brute force attack?

We enforce the use of strong password (Numbers, Letters, and special characters) We encourage the use of MFA (Multi-factor authentication and enforce its use with our employees. We enforce a three times password retries and an account lockout upon the third failed login attempt.

* The term Man-In-The-Middle (MITM) attack is commonly used by hackers can you please explain why do they use it and how do you protect the customer against this?

An attacker might carry out a man in the middle attack to gain sensitive customer information while in transit to the bank. We protect the customer by transmitting data over HTTPS this encrypt the data while it is in transit when this data is acquired by an attacker it is useless to them because it is encrypted

* How do you protect against potential vulnerability in your network security?

We have set up guild lines and protocol for any new software onboarded unto our network, this guild lines include security vulnerability scanning, enforcing adherence to industry best practices source code scanning and approval from security teams.

* During this pandemic we notice that most people are made to do their transaction online and as a means of this most hackers have derive various means as heaven for them to steal information and carry out their fraudulent activities so what tools do you think bank should put in place to combat such attacks?

One of the most common ways to do this is to continuously educate our customers on the various phishing and social engineering methods used by hackers to obtain their sensitive information, We observe customer spending patterns and quickly alert and revise our customer from unusual spending. We continuously deploy updated security patches to our banking application.

* The use of VPN is regarded as one of the major tools in network security can you please explain how important is this in banking security?

We use VPN to enable our employees to connect securely and privately to the company network in other to access resources.

The uptake of the VPN technology has been greatly increased as most employees are now working from home. It is very important that all employees connect to the network using VPN this ensures that we maintain the Hight level of security in data transmitted over the network.

* When it comes to security, authentication is very important so how do you implement the Two Factor Authentication (2FA) for a public website?

The methods of MFA we use depends on if we are dealing with customer or an employee. with employees, we use a hardware MFA token to authenticate the login into their remote desktop. For customers we use 2fa soft tokens to authenticate login into bank account.

* There is a day I went to the bank and I heard the manager addressing his staff and talking about accidental threat so I was wondering was might that mean so I did some research on it and I found that is a threat that are accidental done by an employee of an organization, in your own words can you please explain in details the meaning of accidental threat and have your bank ever experience any accidental threat?

I cannot discuss the details of any particular security incident. However, we do educate and test employees periodically on social engineering and phishing attacks, We educate by the use of video learning and security courses and we test the employs by the via the use of quarterly fake phishing emails. These emails are sent quickly to employees. An employee has passed the test if they do not click the links in the email and if they report such emails to the security teams. If an employee’s fails this test first they are informed via email that they have failed, second time they and their manager are informed via email and an additional security training is assigned to them and for the third time an employee may face disciplinary action.

* During my research I found the word Trojan virus which was commonly used by hackers in your own words can you explain this term?

Trojan virus is presented to the victim as a legitimate software in other to trick the victim into downloading it. This download then infects the victim’s computer with a destructive virus.

## **COMPARISM BETWEEN PRIMARY RESEARCH AND SECONDARY RESEARCH**

Based on the data collected from the primary research from the interviewed questions, we found out that the staff was able to give answers to the questions that was asked by me, that’s to show that most staff of Nigeria banks are very conversant with the word networking security and firewalls and they also know what tricks hackers uses, and how well a bank should take its network security serious and protecting its customers against any vulnerability, we also see that Nigeria banks uses Traceroute tools, strong VPN, the usage od standardize software’s, also the usage of 2fa code, although it was stated by the staff that when it comes to accidental threat the bank do experience that a lot, which shows that this is a problem Nigeria banks have to contend with, then when we look at returned questionnaire from the staffs of Access Bank Nigeria PLC from the questions asked we found out that

* Most Nigeria banks are well computerized
* They offer a computer-based system payment which also yield a good profit to the bank.
* Infrastructure deficiency and erratic power supply has a great impact in most Nigeria banks
* The introducing of electronic payment has not improved in most Nigeria banks

The abuse of privilege is a thing they should really take serious and the establishing of a strong policy to fight against future attacks, it was also seen that the bank do experience intrusion most times, also they should try to do more by informing their customers about cyberattacks on electronic online banking and most especially the government should also try to assist the banks in E-banking system, as seen from the data collected epileptic power supply is a major issue that hinder most Nigeria banks, if the government can create an avenue why they can provide at least constant power supply during the peak period it will serve as an improvement to the banking sector. They should also improve in the aspect of electronic payment.

For the secondary research, same question was asked in the aspect of security in the banking sector, I found out that the said bank staff (Large Bank in America based in Ireland) is also very versatile when it comes to security network of the bank. during the time spent interviewing the staff who works in Large Bank in America based in Ireland, I have seen that the bank also operates on a well computerized platform In addition, human interaction is also involved, and they also offer computer-based payment, but when looking at the E-banking system I noticed that there is high support from the government as well as no range in power supply, it was also stated that the lack of adequate security and fraud prevention has no range, which means that there is enough security and fraud prevention in the banking sector, although as shown in the data collected the exorbitant cost of E-banking was place at a small range in the aspect of the bank. There are other goals are other goals that was stated

* There is high improvement in the introduction of electronic payment in the bank
* When the question was asked to what range has the bank correctly apply security pattern in application in the context of model security, it was recertified by the respondent that the bank is placed at a high level in applying security patterns.
* There is no quantitative resource consumption in all the security mechanism of the bank, this is one of the problem Access banks also faces as there are quantitative resource consumption in all the security of the bank
* Judging from the data collected, w can see that Large Bank in America based in Ireland has never had any attack from external source
* They also have the most effective tools for simulating cyber-attacks, although they do experience some challenges in cloud security
* They also make their customers aware of cyberattacks on electronic online banking

In conclusion, it shown that most Nigeria banks is aware of its network security has they faces attacks most times, but they should create more room for improvement. In terms of the Large Bank in America based in Ireland it shown that most banks in Ireland has established concrete measures in securing their network properly, although it was stated by the respondent that the bank has not experience any attack from external source which shows that the rate of attacks from external source in most bank in Ireland is put at its barest minimal.