# Evaluation of Computer and Network Security Strategies: A Case study of Nigerian Banks

Ogunwobi, Z. O. (Ph.D.),
Olabisi Onabanjo University,
ogunwobizac@yahoo.com

Folorunso, S. O.
Olabisi Onabanjo University,
Ago-Iwoye, Nigeria.
bamidelekeke@gmail.com

Alebiosu, O. B.
Olabisi Onabanjo University,
Ogun State.
boladealeb@gmail.com

## ABSTRACT

It has been identified that financial institutions are one of the major users of Information Technology hence the need to evaluate effective use of the computer security strategies. This study aimed at evaluating the effectiveness of computer and network security strategies employed in Nigerian banks. This study was led by the following objectives; to determine and assess the security strategies that are put in place by Nigerian banks, to suggest solutions that would improve the effectiveness of the evaluated security strategies, to identify the effect of the various security strategies on the integrated banking system. This study employed the use of online questionnaires as a means of data collection. The study majorly focused on computer security strategies employed by the banks, and how effective the implemented security strategies have been. The strategies include passwords, antivirus, firewalls, encryption, intrusion detection systems and intrusion prevention systems, and it was mentioned that the integrated banking systems used by Nigerian banks has a certain security level thereby aiding the computer systems security in general, the study also revealed that Nigerian banks rarely experience malicious attacks of any form on their systems. The study findings revealed that Nigerian banks are implementing at least five computer security strategies

## CCS Concepts

**• General and reference → Cross-computing tools and techniques →Evaluation**

## Keywords

Computer Security, Computer Network, Intrusion Detection System, Information Technology, Intrusion Prevention System

## 1. INTRODUCTION

All over the world, the development and growth of the economy is majorly dependent on the financial systems, as they happen to be the major users of information and communication technology. The level of development of this financial systems and efficiency in performing their roles, depends largely on the introduction and effectiveness of new technological media, which would aid customer satisfaction and convenience. [1].

The introduction of information and communication technology in efficient service delivery in the banking and financial sector is known as electronic banking (e-banking). Information and communication technology is the mechanization of steps, processes, actions, and information gathering using the computer, telecommunication machines, special purpose software and supporting devices such as Point of Sales (POS) machines and credit cards.

The competitiveness and complexity of the banking sector environment in the 21st century, can be characterized by unpredictable, epileptic and changing economic climate of the world. [2] Established that, business competitiveness can only be sustained, when banks and financial systems change from the traditional and old modelled way of operation, which is likened to "bricks and mortar" or "paper and biro" into a more advanced and technological approach, likened to "clicks and portal" or "computers and internet" Information and communication technology (ICT) is at the middle of this grand turning point of banking and financial sector in the World and Nigeria today. Banks and financial systems at home and abroad have adopted electronic banking (e-banking) due to the progression in information and communication technology methods, and a means of remaining abreast in this information age which also aids efficient customer service. [3].

The banking sector all over the world and Nigeria banks are also adapting new innovations in information technology such as e-banking and e-banking puts an end to endless queue in the banking halls, and encourages electronic transfer of funds, this done one internet enable devices and e-banking activated accounts, this done between individuals and financial institutions, the exchange of cash and keeping of large sums of money at home has totally been discouraged, cheques and other negotiable items are also rarely encouraged. In the world today, Point of Sales Machines (POS), Automated Teller Machine (ATM), credit and debit cards, with passwords, biometric scanners and personal identification numbers (PIN) are now means of paying for goods and services or transfer of funds, whenever and wherever the need arises.

The new advancements in the Nigerian Banking sector cannot be done without the use of computers, networks and internet and hence the need to protect the organization's computer and network from unwanted users and malicious attacks becomes very important. Cybercrime and other unintended use which makes it easy to steal a kobo from millions of bank accounts than traditional or conventional bank robbery is becoming predominant despite the positive impact of the advancement in information and communication technology has on the society. [4]

Technology has progressed so much that it would be of no surprise if your computers are hacked and you are completely unaware of the reasons for it. Any organization should monitor its system for potential unauthorized access and several kinds of attacks, in other to safeguard sensitive information. [5].

*CoRI'16*, Sept 7–9, 2016, Ibadan, Nigeria.

Banking sector is a trust-based institution, that requires an absolute trust from her customers, upon this the banking sector should take security issues as a special concern to continually earn the trust of their customers, The need to tighten-up security and proper management channels that could give opportunities for fraud and malicious attacks such as: breach of privacy of customer data, distributed denial of service attacks, and technological letdowns created on electronic banking platforms becomes expedient.

Insecurity has been a major concern in the world's most prominent sector (finance), bank accounts, transactions and funds transfer are tampered with as a result of this insecurity, which is constantly being faced by operators of the banking sector. These experiences have become totally unfavorable, which have made the total adoption of technologies in the banking sector difficult. The insecurity issue has been caused by the ripple effects malicious attacks and threats like State-sponsored espionage, Distributed denial of service (DDoS) attacks, password management, insider threat, privacy laws and viruses among others [6]. Thus, this research is aimed at evaluating the computer and network security strategies employed by Nigerian banks. The following objectives that were used to achieve the aim were: the determination and identification of the security strategies which are being implemented by banks in Nigeria, ascertaining the impact of various integrated banking system on the total security of the banking sector, to assess the security strategies employed by Nigerian banks and also evaluate its effectiveness.

An Important factor in an organization's computer and network system is security, because the computer connects to other networks through the internet. An attack on the organization's computer can be possible from outside of the organization. Therefore computer network security is important to prevent and protect the organization from internal and external attacks. [7]

Computer and Network security is generally handled by the system administrator or network administrator who implements some security policies, software and hardware needed to protect the entire computer system and its resources from any unauthorized or unwanted access and usage and the system administrator also ensure ensures accessibility to the resources for authorized usage. The security system is based on layers of protection and consist of multiple components consisting of monitoring, security software, hardware and appliances. The security is the quality of state, when a computer system is secure it means it is free from potential danger. [8].

The following are the security strategies being focused on and implemented by Nigerian banks;

A firewall is a defined as a perimeter fencing which serves a border or control mechanism. Blocking or stopping traffic from entering into a computer system is the main purpose of a firewall, traffic inside the computer could also be blocked by firewall as well. Firewall serves as the first form of mechanism set up to control intruder activity on the computer. Unauthorized or malicious access in a computer network system can be prevented by firewall. The implementation of firewalls is done on the hardware or the software, or on both. [9]

The need for antivirus software is prompted by the wide spread of malware on computer systems. [10] The presence of malware in a computer system is detected by an antivirus installed in the computer system, the purpose of the antivirus is to identify the nature of the malware, and also remove the malware, which is also a means of preventing the host from future infections from any or similar malware and also dis-harming the host from malware. The minimization of false positives (false alarms) and false negatives (missed malware) is encouraged during the stage of detecting malware in the system.

Malicious activities that are targeted at computer network systems can be identified and responded to by a process called Intrusion detection system (IDS). From this definition, intrusion detection can be seen as a process, which involves a system, individuals, and tools. [11] To reduce the risk of attacks precautionary measures needs to be put in place. Preventing all attacks seems practically impossible but could be achieved with the right measures put in place. Malicious activities can be easily identified and diagnosed with a process which works similar to a burglar alarm, Intrusion detection. Intrusion detection combines three activities majorly to monitor, analyze, and respond. [12].

Intrusion Prevention System (IPS) is a defense system that is primarily network based, it properly combines the proactive technique of IDS with that of firewall as a result of increasing global network. The proactive technique of the system is to prevent malicious attacks before they enter into the system, it verifies and examines various information records. The offending data is blocked and logged when an attack is identified on such data. [13].

Encryption scrambles data thereby making the data very hard to find useful by the intruder, the interpretation of a scrambled data is meaningless if the intruder does not know how the scrambling was done. Encryption or scrambling is indeed an essential tool in providing computer and network security [14]. Encryption clearly addresses the importance of data confidentiality. Additionally, encryption makes it difficult to easily alter or change data, because it has been scrambled this makes it generally hard to read or understand thereby ensuring data integrity. [14].

Passwords have become the only barrier between just any user and one's personal information and they most common and widely used form of authentication. Several programs are available for easy download, which makes it easier for attackers to "guess" or "crack" a password, a very good password and keeping the password confidential makes very difficult for an unauthorized person to gain access to your information. [15].

Banking applications generally known as Core Banking System (CBS) are believed to have a level of security incorporated in them, which helps militate against attacks on the applications and several servers attached, to this effect the need to review banking system application security becomes very important. [16] Application security helps put stringent measures and controls in place on an organization's applications, which reduce the risk from intruders using the application and the risk associated with the authorized user using it.
In a secure Core Banking System proper management of information security is required and this can only be delivered a vendor organization that manages information. Implementation of Information Security Management System (ISMS) on core banking systems makes the work easier for organization as specific areas and processes have been covered within the organization [16].

## 2. RESEARCH METHODOLOGY

The population of study is limited to computer security experts and information technology department staff in Nigerian banks. Eleven

(11) commercial banks and one (1) mortgage bank randomly filled the online questionnaire with a total of 30 respondents. The banks are: Ecobank, Guaranty Trust Bank, Skye Bank Nigeria PLC, Sterling Bank, Firstbank Bank, Fidelity Bank, Access Bank, Keystone Bank, Wema Bank, Zenith Bank, Diamond Bank and Haggai Mortgage Bank, while two (2) respondents did not provide the name of their banks.

Three factors were considered when choosing the sample. The first was that, the respondent must be an IT/ICT staff of a Nigerian bank, the second was to have an idea of the bank's computer security strategies and the third was the willingness of the respondents to cooperate, because some of the staff do not readily have interest in filling the online questionnaires.

An online questionnaire (http://bit.ly/1J6baWS) was administered for data collection which was designed for computer security experts and information technology department staff in Nigerian banks. An online questionnaire was preferred and chosen because the questionnaire was targeted at bank officials, who are very mobile and they always have access to the internet, and with the help of social media campaigns a wider number of respondents could be easily be reached.

Section A which contained the personal data of the staff, such as; age, bank type. It provided the background information needed in answering the research questions. It also contained questions based on the years of experience in the banking sector, years of experience with current bank and name of bank. Section B which contained achievement test items. The questions were twelve multiple choice items in computer security.

The criteria that were used to compare Avast, McAfee and Webroot antivirus were: **On-demand scan** refers to a manual scan which is being initiated by the user on the entire or certain segments of the computer system, here the user initiates the scan and decides what part of the system should be scanned or if the entire system should be scanned.

**On-access scan** refers to an automatically initiated scan which the product itself initiates without any external interference, it scans every file whenever it is created and/or whenever it is modified, and here the antivirus initiates a scan immediately a new file is created on the system.

**CloudAV** gives an efficient automatically initiated scan that is performed on the cloud storage, and this happens frequently. **Email Security** gives our emails the desired security from viruses and malware, thereby preventing penetration, through our email.

**Intrusion Detection System (IDS):** the process of identifying and responding to malicious activities targeted at computing and network resources**.**

**Intrusion Prevention System (IPS):** is a defense system that is primarily network based, it properly combines the proactive technique of IDS with that of firewall as a result of increasing global network.

**AntiSpam** gives us the needed efficient protection from malicious attacks such as: spam, scam and phishing attacks.

**Web protection** comes in when surfing the internet and protect the user from infected and malicious URLs, numerous phishing websites, this also protects us by giving us online banking protection and online identity protection (privacy).

# 3. RESULT AND DISCUSSION

This section is focused on the presentation and discussion of result obtained during the course of this research. The data was collected with particular reference to the questions raised earlier on. The purpose of this study was to evaluate how effective computer and network strategies put in place by Nigeria banks. This study strives to provide answers to the under-listed research questions:

i. What banks do the respondents work for?
ii. What are the years of experience of the respondents?
iii. What Computer security strategies are implemented?
iv. Why is a particular anti-virus preferred to other antivirus software?
v. How often has the bank suffered malicious attacks?
vi. Why is a particular integrated banking system (Core Banking System) preferred to other CBS software?

How effective are the computer strategies implemented?

## 3.1 Bank of the respondents

Figure 1 showed the number of respondents that filled the questionnaire from each bank. It was presented in Figure 1 showed that Ecobank and Wema Bank for a larger percentage of the banks of respondent, while other percentages were spread across ten different banks while three respondents did not mention the names of their banks. There are about nineteen (19) commercial banks in Nigeria as at November 2015, eleven (11) commercial banks participated in this survey, and this indicates that over 50% of Nigerian commercial banks was involved in this research.

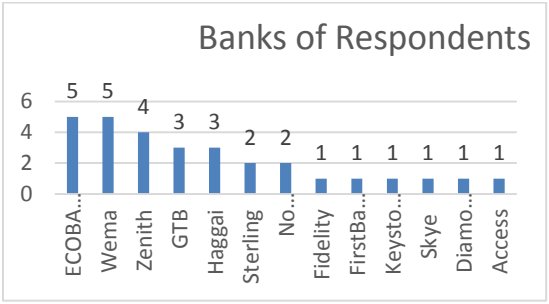


**Figure 1 Banks of Respondent**

## 3.2 Years of experience of the respondents?

Figure 2 summarizes the findings on years of experience of the respondents in the banking, and this ascertains that most of the respondents are either newly recruited staff or they have not stayed too long in the banking sector. This indicates that there level of knowledge of the bank's security strategies implemented could be limited as they have not spent so much time in that particular bank and this could also be a determinant of the level of management of the organization's implemented security strategies, this also shows that the respondents with not very long experience in a particular bank might not be aware of the malicious attacks experienced by the bank in the past.

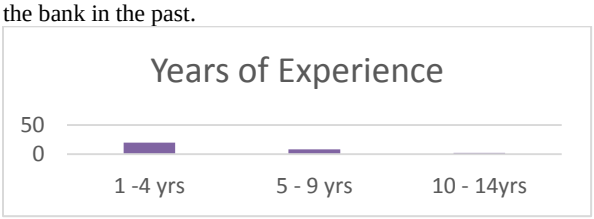


**Figure 2 Years of Experience of respondent**

## 3.3 What Computer security strategies are implemented?

Figure 3 shows that over 50% of the respondents implemented Intrusion Detection and Prevention in their company, 60%

implemented Encryption, 76.6% Firewall, while almost 100% were using Passwords and Antivirus. It can then be deduced that since all the percentages of yes of respondents on each of the five security strategies in Figure 3 are at an average of 75.33%, while average percentage of No and Not sure are 10 % and 14.67% respectively, we could then conclude that Nigerian banks implement all five security strategies.

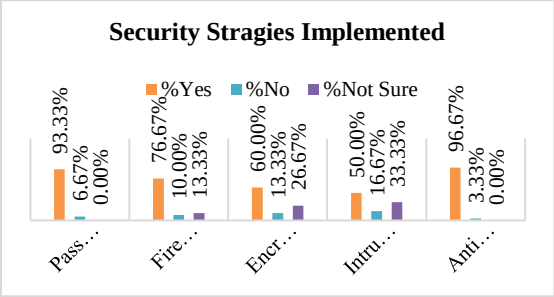


**Figure 3 Security Strategies Implemented**

## 3.4 Antivirus software preference

Figure 4 showed the type of antivirus each Nigerian bank uses and it revealed Avast and MacAfee antivirus are predominantly used while a small percentage of usage are spread sparsely across all other antivirus. Thus, the need to compare why Avast and MacAfee antivirus is preferred over the other and while some have less patronage, which would in turn answer our research question four that is; Why is a particular anti-virus preferred to other antivirus software?

The comparison of why Avast and McAfee are the most preferred and Webroot, the least patronized is showed in Table 2 from Figure 4. The comparison tools ranged from on-demand scan, CloudAV, on-access scan, boot-time scan, firewall, Email security, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Anti-spam and web protection.

It can then be deduced from the result presented in Table 2 that Avast and McAfee was chosen over the Webroot antivirus, seeing that the free versions of the Avast still has some security features already integrated in them and the Premier version of the Avast antivirus has almost all security features integrated in it except for the intrusion prevention system and the AntiSpam. McAfee on the other hand, for it McAfee Antivirus does not have CloudAV, firewalls, IDS, IPS, AntiSpam and web protection which still gives it a fair chance of usage but the McAfee Internet security has all security features integrated into them which might not even require user to install other security strategies.

Webroot, that happens to be the least on the chart in Figure 4 which was also compared alongside with Avast and McAfee, happens not to have not too many security features integrated into it secure anywhere antivirus other than on-demand scan and on-access scan, this shows the very reason why Webroot antivirus happened to be in the bottom section of Figure 4.

We would then conclude based on the comparison of different antivirus software on Table 2 it shows that Avast Antivirus software has a high level of in-built security, which could be the reason why it is the most preferred by Nigerian bank

**Table 2 Comparison of Avast, McAfee and Webroot Antivirus**

| | | Comparison Tools | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Company | Software | On-demand scan | On-access scan | Boot-time scans | CloudAV | Firewall | IDS | IPS | Email security | AntiSpam | Web protection |
| Avast | Avast Free Antivirus | Present | Present | Present | present | absent | present | absent | present | absent | present |
| Avast | Avast Pro Antivirus | Present | Present | Present | present | absent | present | absent | present | absent | present |
| Avast | Avast Internet Security | Present | Present | Present | present | present | present | absent | present | present | present |
| Avast | Avast Premier | Present | Present | Present | present | present | present | absent | present | absent | present |
| McAfee | McAfee Antivirus | Present | Present | Present | Absent | Absent | Absent | Absent | Present | Absent | Absent |
| McAfee | McAfee Internet Security | Present | Present | Present | Present | Present | Present | Present | Present | Present | Present |
| Webroot | SecureAnywhereAntiVirus | Present | Present | Absent | Absent | Absent | Absent | Absent | Absent | Absent | Absent |

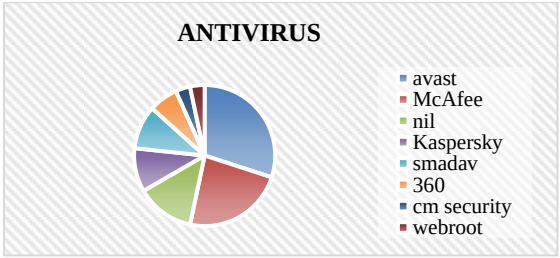


**Figure 4 Antivirus used in Nigerian banks**

## 3.5 How often has the bank suffered malicious attacks?

The result of how often the bank suffers from malicious attack was presented and analysed in Table 2. It showed that on the average, 47% of the respondents from Nigerian banks have never experienced any malicious attacks of any form on their equipment or personal accounts, and just 37% only experienced malicious attacks less often, while only about 15% say that their banks often experience malicious attacks on their equipment. This indicates that the security strategies implemented could be effective since malicious attacks where not very often.

**Table 3 Malicious Attacks on Nigerian Banks**

| Malicious Attacks | never | less often | often | very often |
|---|---|---|---|---|
| **How often have you been denied access to do legitimate work on your computer?** | 50.00% | 30% | 10.00% | 10.00% |
| **How often has a laid back employee caused a malicious attack through the information he/she has?** | 43.33% | 47% | 6.67% | 3.33% |
| **How often has the bank lost money due to malicious attack of any sort?** | 36.67% | 53.33% | 10.00% | 0.00% |
| **How often has your password been bye-passed?** | 70.00% | 20.00% | 6.67% | 3.33% |
| **How often do you experience virus attacks on your computer and network?** | 36.67% | 36.67% | 23.33% | 3.33% |
| **Average** | **47.33%** | **37.33%** | **11.33%** | **4.00%** |

## 3.6 Security strategy preference

Why is a particular integrated banking system (Core Banking System) preferred to other CBS software?

Core Banking Systems gives room from the implementation most or all security strategies on them and this could be found on any of the following Integrated Banking System application: AX, Finnacle, SAP, T24, Microsoft CRM, Phoenix, and Flexcube. As result of the resident security strategies on the core banking system this goes to show that a relationship exists between computer security strategies implemented by banks and the Integrated Banking System. Thus, there is a great impact from the Integrated Banking Systems on computer security strategies implemented in the banking sector.

Figure 5 displayed that Flexcube polled highest followed by some respondents who did not write the name of the integrated banking system used by their banks, while Finnacle polled one of the least results. So the need to review why Flexcube would be preferred becomes important.

The following are some of the features the Oracle Flexcube possess:

i. Capability to process large transaction volumes, with high value of availability all day.
ii. A channel support of multiple delivery, which including branches, point-of-sale terminals, ATMs, mobile devices, call centers, and internet banking
iii. A Web-based user interface resident on XML with context-sensitive help
iv. Role-based access and application are covered by Security management.
v. Exception processing which is automated and online validations.
vi. Combination deployment which could either be centralized or decentralized.
vii. Existing systems are easily integrated using Enterprise Edition technology, flexible Java Platform.

Helps with collateral, and nonperforming assets which are Operational risk management controls.

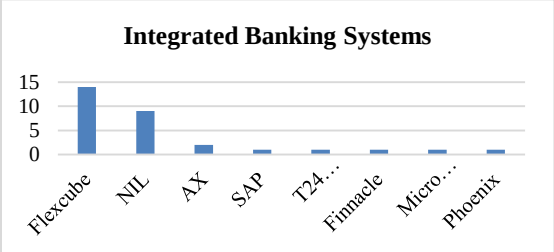


**Figure 5 Integrated Banking System Used in Nigeria**

## 4.7 How effective are the computer strategies implemented?

Figure 6 below depicts that computer and network security strategies which is currently deployed by Nigerian Banks are effective. Based on the facts there have been no instances of malicious activities and absolutely no cases of it in most banks of the respondents, it was cited by 65% of the valid responses that the security strategies have been effective, hence the highest response being on effective.

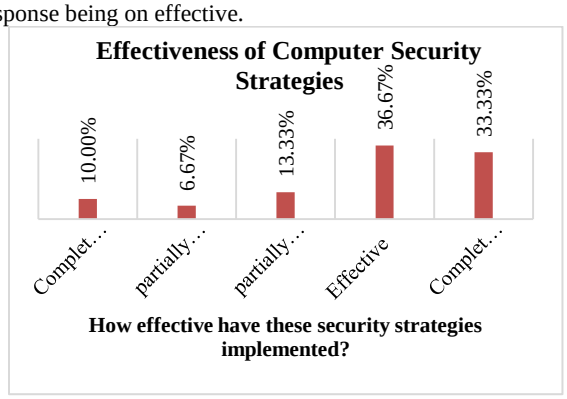


**Figure 6 Effectiveness of Implemented Computer Security Strategies**

# 4. DISCUSSION

[17] Stated that currently most financial institutions including banks employ security mechanisms such as Secure Socket Layers, digital certificates, data encryption which secures data transferred over the internet, etc. In protecting customer information stored within their servers, most financial institutions use firewalls, virus detection and prevention methods, efficient backup servers as a means of preventive measures. From this a strong base is gotten for the result that banks in Nigeria are implementing effective computer and network security strategies.

One of the research question was, what antivirus software are these banks using? And antivirus software is one of key computer security tools.

Analyzing the responses, the result shows that two types of antivirus were predominantly used in Nigerian banks, and these are McAfee Antivirus and Avast Antivirus and from a comparison of both antivirus from Wikipedia which was shown Table 2 showed why most Nigerian banks would opt for either of the two antivirus software, from Wikipedia both McAfee and Avast have the highest number of in-built security.

Another research question was, which integrated banking systems are Nigerian banks using? [6] Submitted that integrated

banking systems have in-built security tools, and all Nigerian banks need to implement an effective and reliable Integrated banking system which would enhance the computer security strategies. All Nigerian banks are using integrated banking system, and from our study it shows that a particular banking application is majorly used by Nigerian banks, which is Flexcube, which could mean that Flexcube is more reliable, efficient and secure.

The general research aim, which was to know how effective computer and network security strategies have been after implementation, and from the result of our research question seven, it shows that computer and network security strategies implemented in Nigerian banks are effective. This contradicted [18] who cited that the computer security strategies implemented are not effective due to several examples of banking related frauds that are still very rampant and [19] who also stated that e-fraud is a way Nigerian banks still keeps losing money which is due to ineffective computer and network security strategies. An effective mixture of computer and network security strategies are being implemented by Nigerian banks, examples of such strategies include passwords, encryption, intrusion detection and prevention systems, firewalls, integrated banking application.

## 5. CONCLUSION

This research evaluated the effectiveness of computer and network security strategies being used by banks in Nigeria. And the following conclusions were drawn, from the results presented earlier. First, computer and network security strategies implemented in Nigerian banks are; passwords, encryption, firewalls, intrusion detection system and intrusion prevention system and about half of the respondents were not sure if they use intrusion detection and prevention system. Secondly, from our research the evaluation, proved that almost all Nigerian banks are fully and effectively implementing the computer and network security strategies. However, only about 15.33% of the respondents from Nigerian banks experience malicious attacks of any form in the bank's system and about 84.66% asserts that they never or rarely experience malicious attacks of any form. Finally, from our presented results, we then conclude that Nigerian banks are using effective computer and network strategies after, implementing almost all security strategies and they rarely experience malicious attacks of any form.

## 6. REFRENCES


[1] Ofanson E. J. (Ph.D.), Aigbokhaevbolo O. M. (Ph.D.) and Enubulu G. O. (2010).The financial system in Nigeria: An overview of banking sector reforms. *AAU JMS Vol. 1, December*

[2] Chau P. and Lai V., (2003). An empirical investigation of the determinants of user acceptance of internet banking. *Journal of organizational Computing and electronic commerce, 13(2),* 123 -145

[3] Tunmibi S. and Falayi E. (2013), IT security and e-banking in Nigeria, *Greener journal of internet, information & communication system.* Vol 1 (3), pp 061 – 065, August.

[4] Wada F., Longe O. and Danquah (2012), actions speaks louder than words – understanding cybercriminals behaviour using criminological theories. *Journal of internet banking and commerce,* April, vol. 17, no 1

[5] Courtney H. (2014), Importance of network security for business organization, *avalan wireless blog,* May 7

[6] Zimucha T., Ngonidzashe Z., Kerina C., Elijah C., Petronella M. Tinovimbanashe M.,(2012), An evaluation of the effectiveness of e-banking security strategies in Zimbabwe: a case study of Zibabwean commercial banks. *Journal of internet banking and commerce,* December, vol. 17, no. 13.

[7] CholatipYawut and PhattarapongKeawpipop (2011) The Future of Organization's Computer Network security for the next five years (2011- 2015) by using the Delphi Technique. *International Conference on Information and Electronics Engineering, Volume 6*

[8] AartiRamehSonone, (2015), Security Techniques Used in Computer Networking, *Indian Streams Research Journal, Volume 5, Issue 9.*

[9] Adeyinka, O. (2008), "Internet Attack Methods and Internet Security Technology," *Modeling & Simulation, 2008.AICMS 08. Second Asia International Conference on*, vol., no., pp.77-82, 13-15 May

[10] Peter Szor, (2005), Art of Computer Virus Research and Defense, Addison-Wesley.

[11] Kruegel, C., Valeur, F., Vigna, G., Intrusion Detection and Correlation Challenges and Solution, *XIV, 118P*

[12] Richard B. (2005), Tao of Network Security Monitoring: Beyond Intrusion Detection, *Addison-Wesley.*

[13] Hu L., Wang W., and Zhao K. (2011), "The Design and Implementation of Trusted Communication Protocol for Intrustion Prevention System," *Journal of Convergence Information Technology*, vol. 6, pp. 55-62

[14] Charles P. Pfleeger, Shari Lawrence Pfleeger (2003) Security in Computing, *Chapter 1; Is There A Security Problem in Computing.*

[15] US-CERT (2013), Security Tips; Choosing and Protecting Passwords Retrieved August 13th, 2015 from, https://www.us-cert.gov/ncas/tips/ST04-002

[16] SEC Consult (2012), Application Security of Core Banking System, A first reality check.

[17] Hawkins, S.,Yen, D.C., & Chou, D.C. (2000). Awareness and challenges of internet security. *Information Management and computer security,8*(3),131-143

[18] Fatima A., (2011). E-banking security issues – Is there a solution in biometrics? *Journal of Internet Banking and Commerce, 16* (2).

[19] Umokoro O. (2013), Why Nigerian Banks will keep losing money to e-fraud, *ThisdayLive 21st November*, retrieved October 20, from http://thisdaylive.com/articles/why-nigerian-banks-will-keep-losing-money-to-e-fraud/164810/