International Journal of Research

# International Journal of Research (IJR)

e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

# An Overview of Network Security Challenges in Nigeria

[1]Amadi E.C; [2]Eze F.U & [3]Oluigbo I.

[1-3]Department of Information Management Technology, Federal University of Technology Owerri, Imo State, Nigeria.
ec.amadi@gmail.com

***Abstract:***

*Despite the gains offered by network systems, developing nations like Nigeria have been facing some stringent challenges in the security of networks. Although Nigeria has experienced continuous growth and rapid progress in policy and technological development, thus resulting in an increasing lycompetitive and networked world, it has however been encumbered with many security challenges. This study looks into network security challenges in Nigeria and proffered solutions that can aid in combating them. Secondary data where used to come up with the position in this report. Information technology has been acknowledged as the life wire of industries as it promotes and facilitates their performances in various countries. There is a variation in the level of trust that persons have in their organizations when it comes to network securities. A general lack of trust on networks is observed from the data gotten, which shows a great need to address network security issues in Nigeria to build confidence in network users. They noted that security is the major challenge to networks in Nigeria.*

**Keywords:** Network; Security; Information Technology; Nigeria; accidental sampling

## 1.0 Introduction

Over the past twenty years, unscrupulous network users have continued to use the computer to commit crimes; this has greatly fascinated people and evoked a mixed feeling of admiration and fear. This phenomenon has seen sophisticated and unprecedented increase recently and has called for quick response in providing laws that would protect the networks and its users. “The level of sophistication has gone high to the point of using network system to commit murder and other havoc” (Barnes, 2004).

Network security is more challenging than ever as today’s corporate networks become increasingly complex. With endpoints multiplying daily, and cloud computing leading to a far more dispersed application environment, the tidy north-south traffic of yesteryear is fast giving way to an east-west swamp.That’s placing a lot of pressure on IT security teams to secure the network or, more accurately, the traffic moving through it, above everything else. Given that security and network teams have historically not worked closely together, and that many network security technologies are still in their infancy, a host of security challenges have arisen.

## 2.0 Network Security Overview

### 2.1 What is Network Security?

Network security is the protection of a computer network and its services from unauthorized modification, destruction, or disclosure. “Itconsists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources” (Wada & Odulaja, 2012). Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password

### 2.2 Network Security Concepts and Attacks

Network security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name, i.e. the password, this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g. a security token, an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g. a fingerprint or retinal scan).Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users.

Networks are subject to attacks from malicious sources. Attacks can be from two categories: "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation. Examples of network passive attack include wiretapping, Port scanner and idle scan. Examples of active attacks include: denial-of-service attack, spoofing, and man in the middle, buffer overflow, SQL injection and cyber attack

### 3.0 The Network Security Challenges in Nigeria

With the new era of technological revolution all over the world, countries are beginning to compete and fight over control of information rather than natural resources. Today, it is all about e-platform, this implies offering services through electronic media to various customers irrespective of place, time and distance. In response to the demands for quick, efficient and reliable services, players in the industries are increasingly deploying technology as a means of generating insights into customers and users' behavioral patterns and preferences. Well developed outsourcing support functions (technology and operations) are increasingly being used to provide services and manage costs e.g. Automated Teller Machine networks, Cards processing, Bill presentment and Payments, Software Development, Call centre operations and Network management (Oluwatolani, et al, 2011). Despite the positive impact of technology on society, it has on the other hand led to unintended use in criminal activities like cybercrime. It has therefore become easier to steal a penny from millions of bank account owners using the internet than through conventional bank robbery (Wada, et al, 2012).

Some of the network security challenges in Nigeria include:

1. Lack of understanding of what network security means is a major societal challenge. Most people online are unaware of the threats and the significance of the threats. It's strange but people still fall victim to recharge card and the "Bill Gates is giving away all his money" scams. Access and consumption is the main focus of many. This demand for digital access and inclusion is justified, as Nigeria cannot afford to be left behind in the digital revolution. But how many know that the same PC that helps you to get the job done faster can also be a welcoming mat for danger?
2. Lack of interest in education and training **-** Lack of understanding is compounded by lack of interest in security education. Security is a serious issue but there is very little demand for security education. Even for the corporate environment, the belief is that "crime happens to someone else". There is an "it can't happen to me" mentality. Security education is not regarded as a priority. Instead the interest and demand in the ICT education is for user and the core professional skills.
3. Direction of governments is unclear **-** Although several governments both past and present have developed security and ICT policies, implementation is a major challenge. "Paper policies"? There is a need for clearer policy direction. And how realistic are such policies? How much has been invested in terms of time, education, personnel, etc? What are the priorities? Is deployment effective? Is content relevant? How committed is leadership? How effectively are resources mobilized and deployed? Are the policies government "shows" or are other stakeholders involved? How well integrated and prioritized are the policies within national development programs?
4. Most measures taken on Information security are reactive in nature, e.g. going after the "Yahoo boys". Quality will take a back seat where issues such as planning, research, monitoring, human resource development and statistics are not given the right attention.

Haphazard half measures won't work. There is a need for a better focus and coordination of efforts rather than playing to the gallery.

5. Low confidence exhibited in e-business structures - The poor attention paid to Information security has affected the growth of e-business in Nigeria. It isn't enough for industries to churn out e-business products and services. Is the environment right? Does the environment breed confidence? In the deployment of e-banking for example, what have the banks and other stakeholders in the e-payment industry done to promote an environment of trust. It isn't enough to throw money at the problem. Investors and key stakeholders – local and foreign – will not take e-business serious in an insecure environment.
6. Law Enforcement/Security/Intelligence Agencies Gap -Network security is about crime. However, a major challenge is that of empowering law enforcement in the digital era. The ICT infrastructure of law enforcement requires massive improvement. The "analogue" days of law enforcement are over. And the crime fighters must be equipped with critical and relevant skills for knowledge economy security and intelligence. Security and intelligence activities today cover more than the physical and the tangible. Information security requires not just ICT knowledge but ICT enabled intelligence. There is a need for skills to deal with the threats associated with Information infrastructure, products and services enabled by ICT.
7. Porous Nature of the Internet - The Internet is free for all with no central control. Hence, the state of anarchy presently experienced.
8. Support for BYOD - With the bulk of enterprises now supporting bring your own device (BYOD) policies, the demands on corporate networks have become more complex than ever, and security teams are struggling to keep pace with the fast-changing, hard-to-control environment.

## 4.0 Findings

Some of the most salient findings are as follows:

1. Organizations are experiencing multiple successful attacks against their networks. Figure 1 shows 59 percent (32+18+9) of respondents say their organization's network security has been successfully breached at least twice over the past 12 months. Ten percent do not know and 90 percent of organizations in the study have had at least one breach.

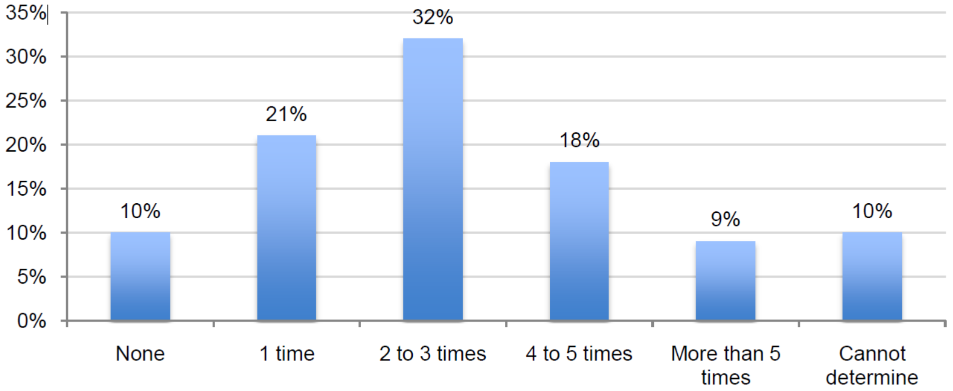

Figure 1 - The number of successful network security breaches over the past 12 months

2. Figure 2show perceptions about the security of the IT infrastructure. Thirty-four percent (11 + 23) of respondents say they have a low perception about their network security.

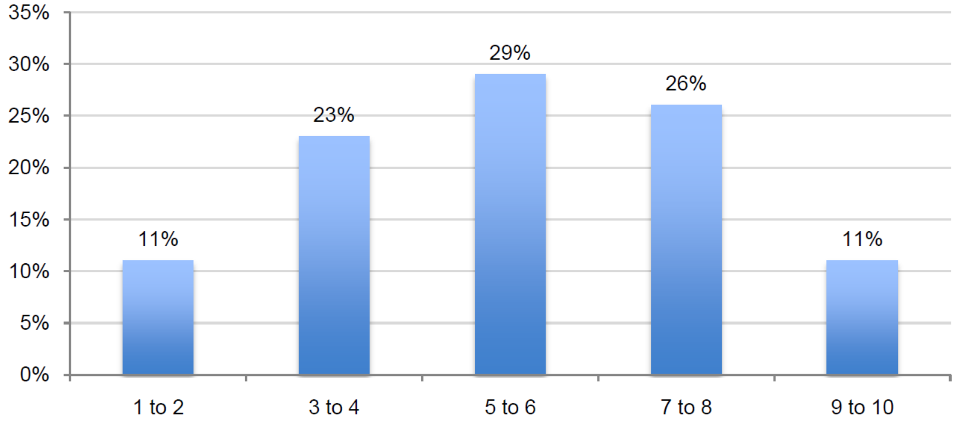

Figure 2 - Perceptions about the security of the IT infrastructure to prevent network security breaches using a 10-point scale from 1 = insecure to 10 = completely secure

3. Figure 3 shows the level of confidence in the ability to prevent network security breaches. Figure 3 reveals that 53 (23 + 30) percent of respondents have little confidence that they can avoid one or more cyber attacks in the next 12 months.

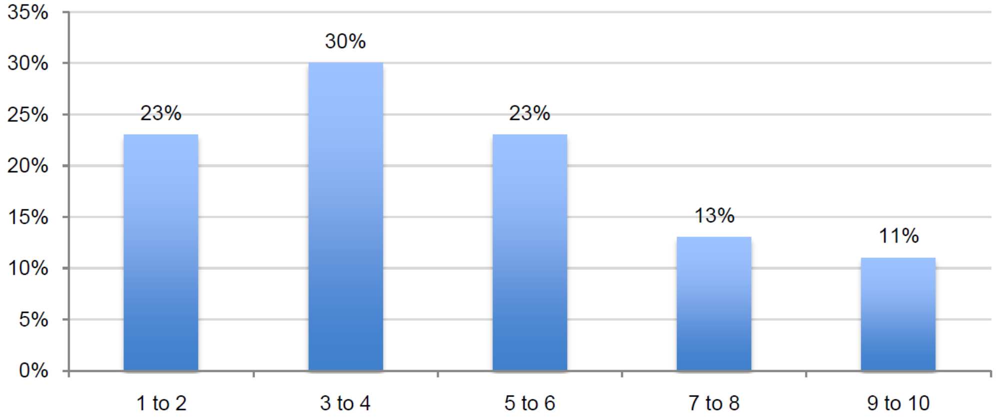

Figure 3 - Respondents' perceptions about the level of confidence that their organization will not experience one or more cyber attacks sometime over the next 12 months using a 10-point scale from 1 = no confidence to 10 = absolute confidence.

4. Security breaches most often occur at off-site locations but the origin is not often known. Mobile devices and outsourcing to third parties or business partners seem to be putting organizations at the most risk for a security breach. As shown in Figure 4, 28 percent say the breaches occurred remotely and 27 percent say it was at a third party or business partner location.

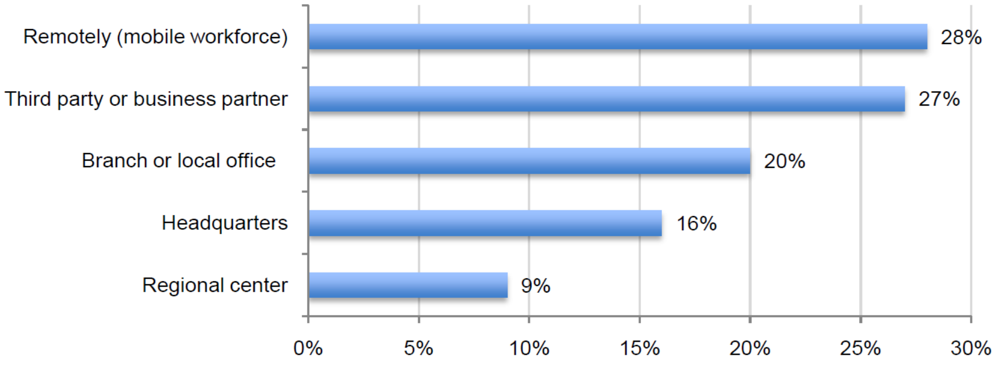

Figure 4 - Where did these security breaches occur?

5. However, as shown in Figure 5, there is uncertainty as to where the breaches originate. Forty percent of respondents do not know the source of the network security breaches. Of the 60 percent who say they know the source of all (11 percent), most (16 percent) or some of the attacks (33 percent).

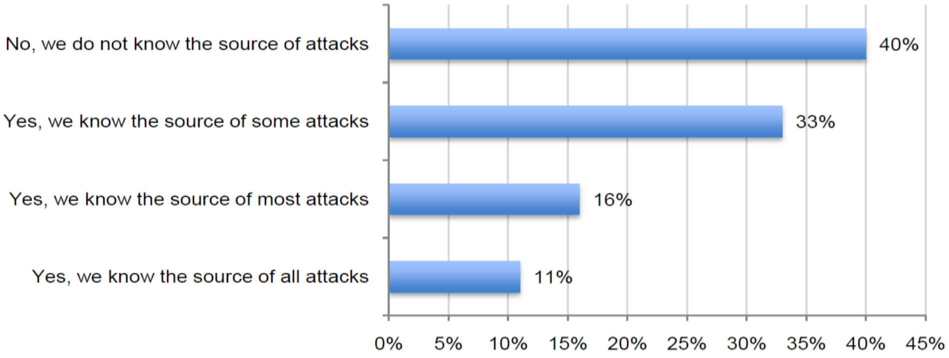

Figure 5 - What is the source of network security breaches experienced over the past 12 months?

6. Attacks are coming from external agents but insider abuse is prevalent. Figure 6 shows the person(s) most responsible for the attack. Both external agents and insiders (employees) are most often behind the security breaches according to 55 percent and 49 percent of respondents, respectively. Respondents also report that multiple sources can be blamed for the breaches.

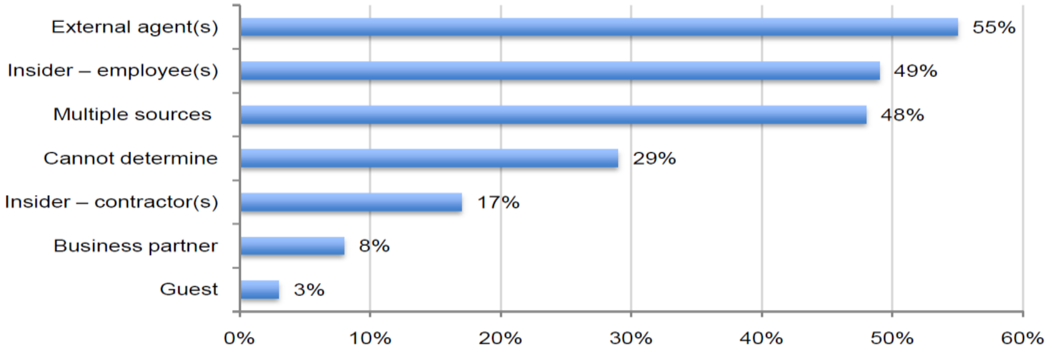

Figure 6 - Who was behind security breaches experienced over the past 12 months?

7. Fifty-two percent say the breaches were caused by insider abuse and 48 percent say it was malicious software download and 43 percent say it was malware from a website. Sixteen percent do not know the cause.

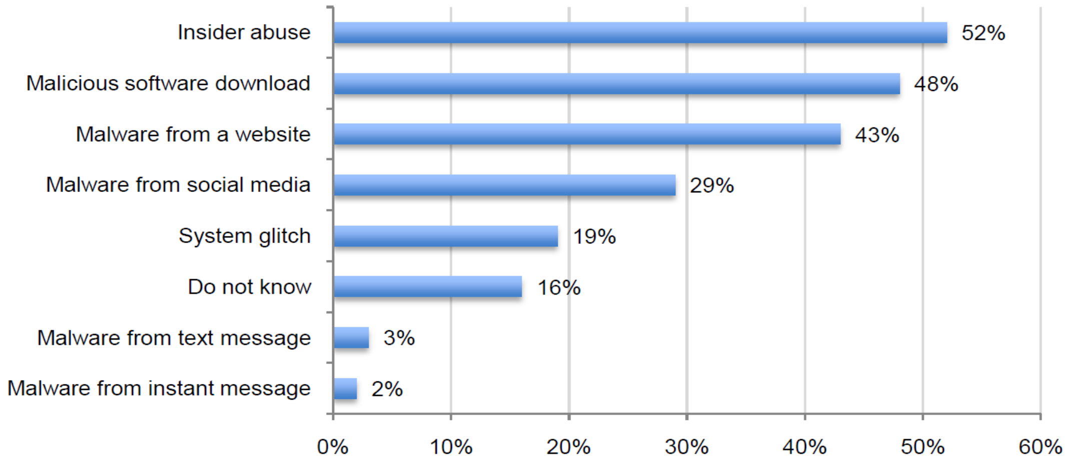

Figure 7 - How were these security breaches caused?

8. Employee mobile devices and laptops are seen as the most likely endpoint from which serious network attacks are unleashed against a company**.** Figure 8 shows that 34 percent of respondents say attacks occurred from infected laptops or remotely due to an employee's insecure mobile device. Further, the top two endpoints from which these breaches occurred are employees' laptop computers (34 percent) and employees' mobile devices (29 percent). Twenty-eight percent say it is employees' desktop computers.

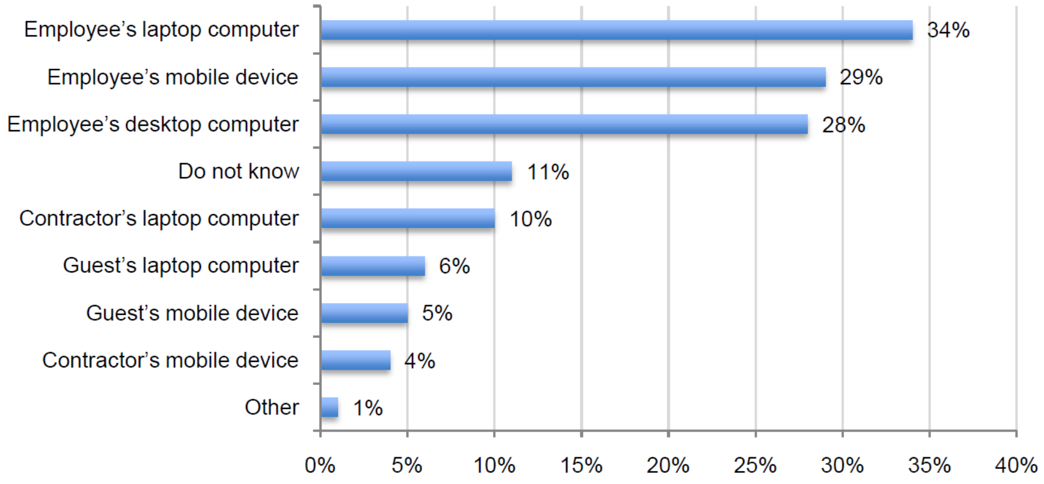

Figure 8 - What are the most likely endpoints from which serious cyber attacks are unleashed?

9. Despite knowing that mobile devices are putting organizations at risk, Figure 10 reveals that 60 percent of respondents say their organizations permit mobile devices such as smart-phones and tablets (including those personally owned by the employee) to access their company's network or enterprise systems.

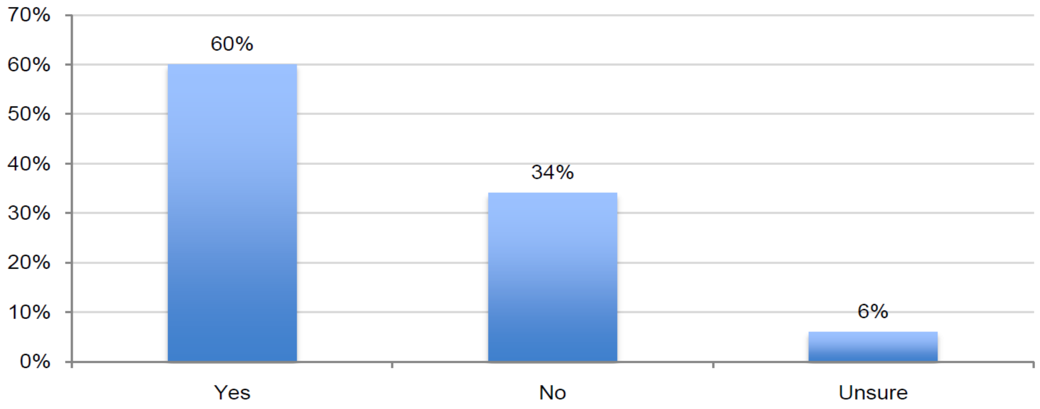

Figure - Do you allow mobile devices such as smart-phones and tablets (including those personally owned by the employee) to access your company's network or enterprise systems?

## 5.0 Recommendations

The author believesthat the research provides evidence that many organizations are lacking the right strategy to prevent attacks against networks and enterprise systems. This study suggests conventional network security methods need to improve in order to curtail internal and external threats. Organizations should consider incorporating the following recommendations in their network security strategy:

1. Understand the risk employees' mobile devices create in the workplace. In addition to problems created when inappropriately being connected to the network, breaches involving lost or stolen laptop computers or other mobile data-bearing devices remain a consistent and expensive threat**.**
2. **C**reate a comprehensive policy (including detailed guidelines) for all employees and contractors who use mobile devices in the workplace. The policy should address the risks associated with each device and the security procedures that should be followed. Guidelines can range from such topics as to what types of data should not be stored on these devices, how to determine if an application can be safely downloaded and how to report a lost or stolen device.
3. Improve ability through expertise and enabling technologies to detect and prevent breaches. Understanding the source of the breaches can help organizations strengthen their cyber security strategy.
4. Address the insider threat through the creation of an enterprise-wide security policy that includes the responsibilities of employees to help protect network security. The policy should be easily accessible. In addition, there should be a training and awareness program to ensure employees understand the various risks to the network and how they can contribute to preventing security breaches.
5. Complexity is recognized as a barrier to effective network security strategy. Organizations should assess their current procedures and technologies to understand how best to streamline their approach and have an end-to-end (holistic) approach to network security.
6. Reduce organization's vulnerability to attacks through the combination of proper staffing, enabling technologies and training programs. This can help prevent the pattern of multiple breaches experienced by many.

## 6.0 Conclusion

As the general population becomes increasingly refined in their understanding and use of computers and as the technologies associated with computing become more powerful, there is a strong possibility that network security challenges will become more common. “Nigeria is rated as one of the countries with the highest levels of e-crime activities. Network security must be addressed seriously as it is affecting the image of the country in the outside world” (Tunmibi & Falayi, 2013). A combination of sound technical measures in conjunction with legal deterrents will be a good start in the war against network security breaches. Information attacks can be launched by anyone, from anywhere. The attackers can operate without detection for years and can remain hidden from any counter measures. This indeed emphasizes the need for the government security agencies to note that there is need to keep up with technological and security advancements. It will always be a losing battle if security professionals are miles behind those involved in breaching network securities. There is need to create a security-aware culture involving the public, the ISPs, cybercafés, government, telecomm companies, security agencies and internet users. Also in terms of strategy, it is crucial to thoroughly address issues relating to enforcement. Mishandling of enforcement can backfire.

## REFERENCES

[1] Barnes D.A. (2004). “Deworming the Internet”. Texas. p279.

[2] F. Wada & Odulaja G.O. (2012). “Assessing Cyber Crime and its Impact on E-Banking in Nigeria Using SocialTheories”. African Journal of Computer& ICTs. Vol. 5. No. 1. p 69.

[3] Oluwagbemi Oluwatolani, Abah Joshua & Achimugu Philip (2011). The impact of information technology in Nigeria’s banking industries. Journal of computer science and engineering, volume 7, issue 2 p 2.

[4] Tunmibi S. & Falayi E. (2013). IT Security and E-Banking in Nigeria. Greener Journal of Internet, Information & Communication System. Vol. 1 (3), pp. 061-065.

[5] Wada F., Longe O. and Danquah P (2012). Action speaks louder than words – understanding cybercriminal behaviour using criminological theories. Journal of internet banking and commerce, vol.17, no.1 p.5.