Vol 8. No. 4, December, 2015
ISSN 2006-1781

African Journal of Computing & ICT

www.ajocict.net

Approaches to Increase Public Awareness on Cybersecurity

J. O. Odumesi
E-Learning Department
Civil Defence Academy
Abuja, Nigeria
olayemijohn@yahoo.com

ABSTRACT

With the technological advancements recorded in the information and communication technology sector, security of the internet remains a major source of concern for users of these services. With the growing volume of cyberattacks in Nigeria, cybersecurity is a necessary consideration for all stakeholders. In lieu of this, Nigeria has taken concrete steps towards ensuring a secure cyberspace with the publication of its National Cyber Security Policy, National Cyber Security Strategy, and the enactment of the Nigeria Cybercrime (Prohibition, Prevention, etc.) Act, 2015. However, it is obvious that, cybersecurity awareness is still at its embryonic stage. Thus, the purpose of this study is to provide approaches the Nigeria government should use to improve cybersecurity awareness. A mixed methodology was used to analysis the online survey that was conducted. Based on the findings of the study, recommendations are made to the Nigeria government on how to improve cybersecurity awareness.

Keywords: Cyberthreats, Cybercrime Act, National Cybersecurity Policy, National Cybersecurity Strategy, Public Awareness

African Journal of Computing & ICT Reference Format:
J.O. Odumesi (2015): Approaches to Increase Public Awareness on Cybersecurity
. Afr J Comp & ICTs. Vol 8, No. 3. Pp 143-152.

1. INTRODUCTION

The internet penetration policies of government have yielded unprecedented growth and leading to increased dependence on information and communication technology in Nigeria. The Nigeria population census of 2006 placed the total population at 140,431,790 [12]. As at July 2014, [13] (Real time world statistics) placed Nigeria population at 178,516,904.

Table 1 and Table 2 of internet subscriber data by the Nigerian Communications Commission (NCC) for September 2015 revealed that the demand for internet connectivity is on the increase [10].

The total active internet subscribers on both Global System for Mobile communications and Code Division Multiple Access in Nigeria are 97,212,364. The total internet subscribers represent 69% or 54% of population census of 2006 or worldometers of 2014 respectively.

The Nigerian government is aware of the increasing dependence on cyberspace and the threats associated with the domain. In this context, the government developed a National Cybersecurity Strategy 2014, National Cybersecurity Policy 2014 and enacted the Nigeria Cybercrime Act 2015. These are measures towards addressing the challenges of cyberthreats in the overall interest of national security and economy.

Table 1: Active Internet Subscriptions (Global System for Mobile communications)

GSM Networks	October 2012	October 2013	October 2014	September 2015
Airtel	4,807,124	9,650,631	13,831,804	17,730,955
Etisalat	4,800,683	5,640,789	5,800,277	15,598,070
Globacom	885,649	12,975,809	15,843,258	21,896,229
MTN	15,878,288	29,347,442	38,637,446	41,411,846
Total	**26,329,908**	**57,840,299**	**73,869,523**	**97,060,548**

Source: Nigerian Communications Commission, 2015.

Vol 8. No. 4, December, 2015
ISSN 2006-1781

Table 2: Active Internet Subscriptions (Code Division Multiple Access)

GSM Networks	October 2012	October 2013	October 2014	September 2015
Multilinks	43,833	11,592	1,717	286
Starcomms	91,539	15,859	N/A	N/A
Visafone	78,975	143,449	155,660	151530
Total	**228,237**	**169,149**	**157,377**	**151,816**

Source: Nigerian Communications Commission, 2015.

2. PROBLEM STATEMENT

Cyber risk is inevitable without proper precautions to protect Personally Identifiable Information (PII) on the cyberspace. [6] identified that, Nigeria online users are highly vulnerable to cyberattacks. The laboratory maintained that, Nigeria is the 64th most attacked nation in terms of malware and 128th in terms of cyberthreats. Nigeria incurred loss as a result of defacement of 2175 websites with 585 belonging to government agencies to the tune of N159 billion between 2000 to 2013 [5]. He further stated that, the nature of cyber attacks include extreme intrusion, copyright infringement, unethical information technology practices by trusted professional and insider threats.

The lack of cybersecurity awareness had made it easy for fraudsters to operate leading to loss of finances, reputation and credibility [7]. She maintained that, there is a need for a sure way to combat cybercrime and other resources breaches. [4] stressed the need for cybersecurity awareness collaboration between the public and private sector in other to address the growing cybercrime menace in the society.

[2] reported that, defacement of Nigeria government websites has risen from 10% in 2010 to 60% as at 2012. The report shows an alarming increase in cyber attacks on official websites. Cyber security awareness is one major approach to winning the war against cybercrimes [3]. He further explained that, it is very unfortunate that majority of the Nigeria population that uses the Internet are unaware of the dangers associated with the Internet.

From the above, it is evident that, cybersecurity awareness in Nigeria is still at its infancy. The way forward is to sensitise the general public so that they can be able to easily recognise cyberthreats and act rightly. These observations motivated the researcher to carry out this study in order to provide awareness mechanism towards cyberthreats in Nigeria.

3. RESEARCH OBJECTIVES

The main objective of this study is to provide approaches the Nigeria government should use to improve public awareness on cyberthreats through the cybersecurity strategy.

The specific objectives are as follows:

1. To understand the level of awareness of Nigerians about cybersecurity strategy.
2. To provide guidance for the implementation of the cybersecurity policy awareness.

4. RESEARCH METHODOLOGY

To measure the level of cybersecurity awareness, a mixed methodology research of both qualitative and quantitative was used to design and analysis the data. The quantitative method made use of charts, tables and figures to graphically illustrate the data. The qualitative method made use of thematic analysis to categorise the data for analysis. Thematic analysis [1] is a qualitative analytic method for identifying, analysing and reporting patterns (themes) within data.

An online survey was conducted with twenty questions grouped into four respective sections. Section A measured the socio demographic variables of the participants which includes gender, age category, sector and level of education. Section B measured the level of cybersecurity awareness with reference to the Nigeria cyberlaw, cybersecurity strategy and cybersecurity policy. Section C measured the level of cyberthreats awareness in getting the participants perspective. Section D measured the level of public awareness drive with reference to the participant perspective. The link to the survey website (esurveycreator) was distributed via social networks (Facebook, Twitter, Whatsup and BBM).

5. NIGERIA CYBERSECURITY MECHANISM

The Nigeria government has put in place cohesive measures towards addressing the emerging cyberthreats effectively, which include:

1. Development of the Nigeria's National Cybersecurity Policy document.
2. Development of the Nigeria's National Cybersecurity Strategy document.
3. Enactment of the Nigeria's Cybercrime Act 2015.
4. Establishment of the Nigeria's National Computer Emergency Response Team (ngCERT) Operation Center

5.2 Nigeria National Cybersecurity Policy

The aim of this document [8] is to chart a course towards an assured and trusted presence in cyberspace. This policy therefore sets out the strategic intent of the government in mitigating the country cyber risk exposure by prioritising our needs while focusing on key areas, curtailing escalation of cyber threats that are inimical to the national security posture and the Nigerian economic wellbeing.

This policy is a vital response element for safeguarding the nation. It helps to enlighten the citizens on the components that are to be used to empower the nation to understand, respond and collectively deter cyber threat activities. The policy outlines the doctrinal framework and guiding principles for achieving our roadmaps through a coordinated effort of all stakeholders in the country.

The document is made up of eleven (11) parts, which are:

1. Introduction
2. The national doctrines
3. National security and cybersecurity
4. National cybersecurity roadmap
5. National priorities
6. Principles on incident management and CERT ecosystem
7. Principles on critical information infrastructures protection
8. Principles on assurance and monitoring
9. Principles on national commitment and governance
10. Principles on online child abuse and exploitations
11. Miscellaneous principles

5.3 Nigeria National Cybersecurity Strategy

This document [9] is the nation's readiness strategy to provide cohesive measures and strategic actions towards assuring security and protection of the country presence in cyberspace, safeguarding critical information infrastructure, building and nurturing trusted cyber-community.

This document provides strategies that will be used to implement the measures outlined in the new National Cybersecurity Policy.

The document is made up of eleven (11) chapters, which are:

1. An overview of national cybersecurity strategy
2. Understanding national cyber-risk exposure
3. National readiness strategy
4. Legal framework initiatives
5. National incident management strategy
6. Strategy on critical information infrastructures protection
7. Strategy on assurance and monitoring
8. National cybersecurity skill and manpower development
9. Strategy on online child abuse and exploitations
10. Strategy on public-private partnership
11. Strategy on national internet safety

The Nigeria Cybersecurity Policy and Strategy listed five main cyberthreats confronting Nigeria national growth and security [8] [9]. They are:

a. Cybercrime
b. Cyber-espionage
c. Cyber conflict
d. Cyberterrorism
e. Child online abuse and exploitation

The Nigeria Cybersecurity Strategy highlights the following as sources of cyberthreats [9]:

a. Foreign states
b. Organised criminal syndicates
c. Terrorists and extremist group
d. Hackctivists
e. Corporate insiders

5.4 Cybercrimes (Prohibition, Prevention, Etc) ACT, 2015

The Act [11] provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. This act also ensures the protection of critical national information infrastructure, and promotes cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

The Act is comprehensive in its coverage:

1. Critical Infrastructure Protection;
2. Computer related offences;
3. Content related offences;
4. Offences against integrity, functionality and confidentiality of systems and networks;
5. Procedural provisions – investigation, prosecution and general enforcement;
6. Jurisdiction and International Cooperation

Vol 8. No. 4, December, 2015
ISSN 2006-1781

The Cybercrime Act is made up of:

1. 59 Sections
2. 8 Parts
3. 2 Schedules.

Part I- Objects and Application

1. Section 1: Objectives
2. Section 2: Application

Part II-Protection of critical National Information Infrastructure

1. Section 3: Designation of certain computer systems or networks as Critical National Information Infrastructure.
2. Section 4: Audit and Inspection of Critical National Information Infrastructure.

Part III- Offences & Penalties

1. Section 5: Offences against Critical National Information Infrastructure
2. Section 6: Unlawful Access to computers
3. Section 7: Registration of Cybercafé
4. Section 8: System Interference.
5. Section 9: Intercepting Electronic Messages, Emails Electronic Money Transfers.
6. Section 10: Tampering with Critical Infrastructure
7. Section 11: Willful Misdirection of Electronic Messages.
8. Section 12: Unlawful interceptions.
9. Section 13: Computer Related Forgery.
10. Section 14: Computer Related Fraud.
11. Section 15: Theft of Electronic Devices.
12. Section 16: Unauthorized modification of computer systems, network data and System interference.
13. Section 17: Electronic Signatures.
14. Section 18: Cyber Terrorism.
15. Section 19: Exceptions to Financial Institutions Posting and authorized options.
16. Section 20: Fraudulent issuance of E- Instructions.
17. Section 21: Reporting of Cyber Threats.
18. Section 22: Identity theft and impersonation.
19. Section 23: Child pornography and related offences.
20. Section 24: Cyberstalking.
21. Section 25: Cybersquatting.
22. Section 26: Racist and xenophobic offences.
23. Section 27: Attempt, conspiracy, aiding and abetting.
24. Section 28: Importation and fabrication of E-Tools.
25. Section 29: Breach of Confidence by Service Providers
26. Section 30: Manipulation of ATM/POS Terminals.
27. Section 31: Employees Responsibility
28. Section 32: Phishing, Spamming, Spreading of Computer Virus.
29. Section 33: Electronic cards related fraud.
30. Section 34: Dealing in Card of Another.
31. Section 35: Purchase or Sale of Card of Another
32. Section 36: Use of Fraudulent Device or Attached E-mails and Websites.

Part IV- Duties of Financial Institutions

1. Section 37: Duties of Financial Institutions

Duties of Service Providers

1. Section 38: Records retention and protection of data.
2. Section 39: Interception of electronic communications
3. Section 40: Failure of service provider to perform certain duties.

Part V- Administration and Enforcement

1. Section 41: Co-ordination and enforcement.
2. Section 42: Establishment of the Cybercrime Advisory Council
3. Section 43: Functions and powers of the Council
4. Section 44: Establishment of National Cyber Security Fund

Part VI- Arrest, Search, Seizure and Prosecution

1. Section 45: Power of arrest, search and seizure.
2. Section 46: Obstruction and refusal to release information
3. Section 47: Prosecution of offences
4. Section 48: Order of forfeiture of assets.
5. Section 49: Order for payment of compensation or restitution.

Part VII- Jurisdiction and International Co-operation

1. Section 50: Jurisdiction
2. Section 51: Extradition.
3. Section 52: Request for mutual assistance
4. Section 53: Evidence pursuant to a request.
5. Section 54: Form of request from a foreign state.
6. Section 55: Expedited Preservation of computer data
7. Section 56: Designation of contact point.

Part VIII- Miscellaneous

1. Section 57: Regulations.
2. Section 58: Interpretation.
3. Section 59: Citation

First Schedule lists the Cybercrime Advisory Council. The Cybercrime Advisory Council shall comprise of a representative each of the following Ministries, Departments and Agencies-

(a) Federal Ministry of Justice;
(b) Federal Ministry of Finance;
(c) Federal Ministry of Foreign Affairs;
(d) Federal Ministry of Trade and Investment;
(e) Central Bank of Nigeria;
(f) Office of the National Security Adviser;
(g) Department of State Services;
(h) Nigeria Police Force;
(i) Economic and Financial Crimes Commission;

Vol 8. No. 4, December, 2015
ISSN 2006-1781
African Journal of Computing & ICT

www.ajocict.net

(j) Independent Corrupt Practices Commission;
(k) National Intelligence Agency;
(l) Nigeria Security and Civil Defence Corps;
(m) Defence Intelligence Agency;
(n) Defence Headquarters;
(o) National Agency for the Prohibition of Traffic in Persons;
(p) Nigeria Customs Service;
(q) Nigeria Immigration Service;
(r) National Space Management Agency;
(s) Nigeria Information Technology Development Agency;
(t) Nigerian Communications Commission;
(u) Galaxy backbone;
(v) National Identity Management Commission;
(w) Nigeria Prisons Service;
(x) One representative each from the following:
  (i) Association of Telecommunications Companies of Nigeria;
  (ii) Internet Service Providers Association of Nigeria;
  (iii) Nigeria Bankers Committee;
  (iv) Nigeria Insurance Association;
  (v) Nigerian Stock Exchange;
  (vi) Non-Governmental Organization with Focus on Cyber Security.

Second Schedule lists businesses to be levied for the purpose of the Cybersecurity Fund under Section 44 (2) (a):

1. GSM service providers and all telecom companies
2. Internet service providers
3. Banks and other financial institutions
4. Insurance companies
5. Nigerian Stock Exchange

6. DATA ANALYSIS AND FINDINGS

The study aimed at investigating the approaches the Nigeria government would use to increase public awareness on cybersecurity strategy.

6.2 Response Data

The study's sample size for analysis consisted of 691 responses drawn from the online survey from which a response rate was conducted below:

Usable response: 574 = 83%
Unusable response: 117 = 17%
Total response: 691 = 100%

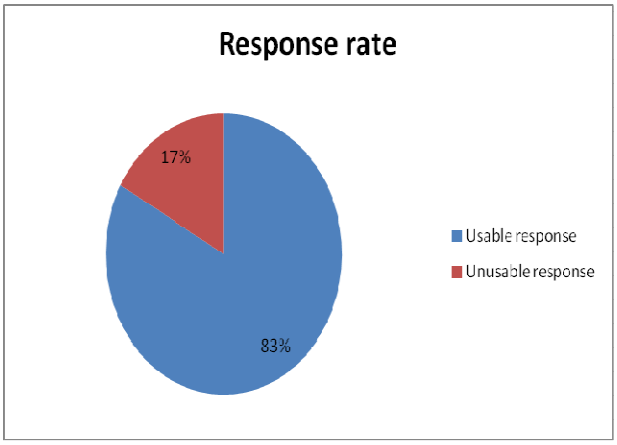


Figure 1: Response rate

The unusable responses of 117 represent 17% were removed from the data analysis because they were incomplete. The remaining 574 stratified responses represent 83% of the study's sample size with the highest participation coming from the Military/Para-Military/Security Agencies. Table 3 illustrated below:

Table 3: Stratified response

Strata	**Stratified Response**
Academia	88
Civil Service	19
Civil Society	9
Military/Para-Military/Security Agencies	295
Private Sector (Excluding ICT)	6
Private Sector (ICT)	164
Total stratified sample analysed	**574**

Source: Odumesi, 2015.

There were more male participants in the response of the sample with a 67% rate while females represented 33% as shown in Figure 2. The participants within the 30 - 35 age brackets were the highest as shown in Figure 3. University graduates were the highest participants compared to other levels of education as shown in Table 4.

Vol 8. No. 4, December, 2015
ISSN 2006-1781

www.ajocict.net

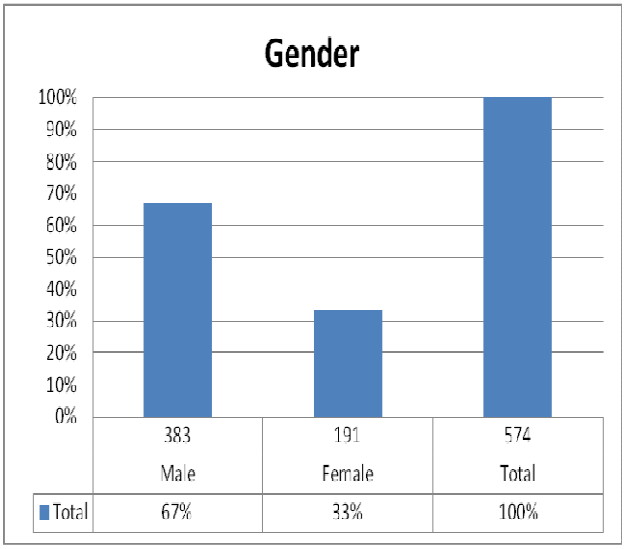


Figure 2: Gender distribution of usable response

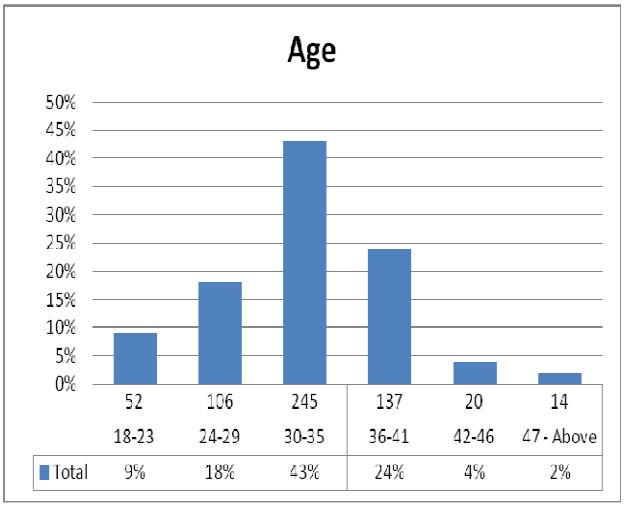


Figure 3: Age distribution of usable response

Table 4: Level of education of usable response

Level of education	**Stratified response**
Polytechnic graduate	70
University graduate	291
Postgraduate (Masters)	204
Postgraduate (Masters)	9
Total stratified sample analysed	**574**

Source: Odumesi, 2015.

6.3 Cybersecurity Strategy Literacy Data Analysis

To investigate the participants' awareness of the cybersecurity strategy, the survey required them to state if they had accessed and read the Nigeria Cybercrime Act 2015, Nigeria National Cybersecurity Strategy 2014 and Nigeria National Cybersecurity Policy 2014 as shown in Figure 4, Figure 5 and Figure 6 respectively.

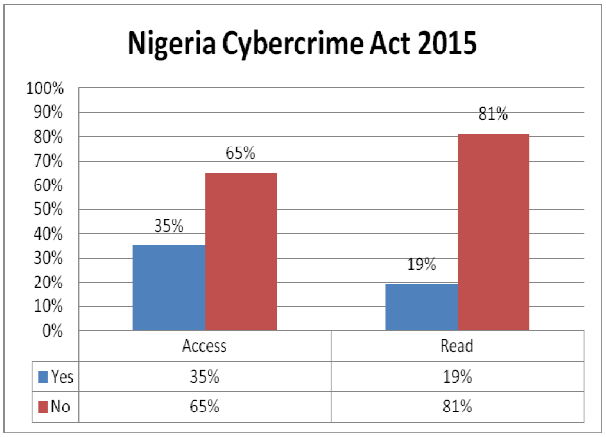


Figure 4: Participants who have access and have read the Nigeria Cybercrime Act 2015

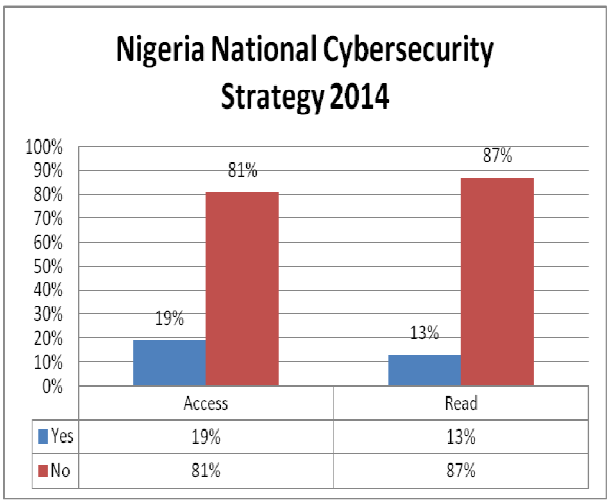


Figure 5: Participants who have access and have read the Nigeria National Cybersecurity Strategy 2014

Vol 8. No. 4, December, 2015
ISSN 2006-1781
African Journal of Computing & ICT

www.ajocict.net

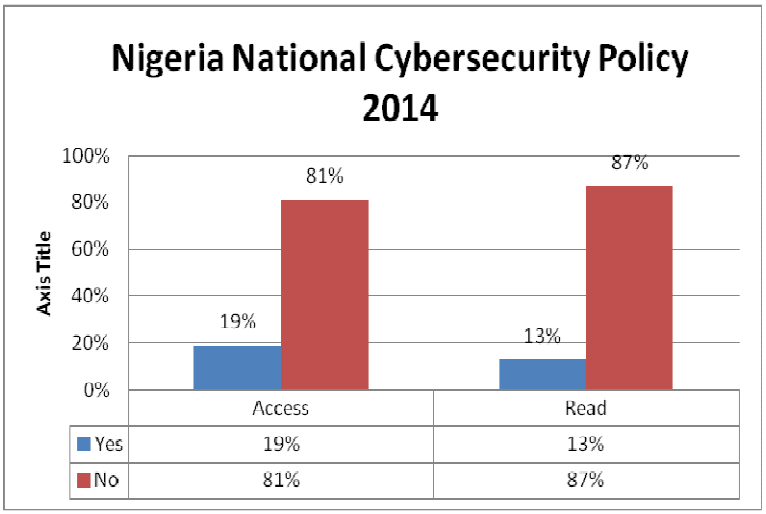


Figure 6: Participants who have access and have read the Nigeria National Cybersecurity Strategy 2014

From the survey data, 81% of the participants indicated that they have an internet enabled computer system of which 56% use it to access the internet very often as shown in Table 5. 100% of the participants indicated that they have an internet enabled phone of which 87% use it to access the internet very often as shown in table 6. 69% of the participants indicated that they have an internet enabled tablet of which 44% use it to access the internet very often as shown in Table 7.

Table 5: Computer Internet Usage from usable response

Computer Internet Usage	Very often	Often	Not often	Not at all
Yes (81%)	56%	38%	0	6%
No (19%)	0	0	0	100%

Source: Odumesi, 2015.

Table 6: Mobile Phone Internet Usage from usable response

Mobile Phone Internet Usage	Very often	Often	Not often	Not at all
Yes (100%)	87%	13%	0%	0%
No (0%)	0%	0%	0%	0%

Source: Odumesi, 2015.

Table 7: Tablet Internet Usage from usable response

Tablet Internet Usage	Very often	Often	Not often	Not at all
Yes (69%)	44%	19%	6%	31%
No (31%)	0%	0%	0%	100%

Source: Odumesi, 2015.

The survey data from Table 5, Table 6 and Table 7 confirms the increase in internet proliferation among the Nigeria public and the urgent need for cybersecurity strategy awareness drives.

6.4 Cyberthreats Data Analysis

To justify the approaches suggested creating awareness on cyberthreats. In examining the survey results, Table 8 illustrates two major categories of cyberthreats which were identified as technical cyberthreats and non-technical cyberthreats:

Table 8: Cyberthreats Analysis

Cyberthreats Type	Number of Respondents	Percentage Response
Technical	350	61%
Non-Technical	224	39%
Total	**574**	**100%**

Source: Odumesi, 2015.

The findings suggest that technical type of cyberthreats are the most commonly known by participants at 61% which include hacking, yahoo yahoo, virus, phishing, malware, amongst others. The non-technical at 39% include government policies, illiteracy, lack of proper monitoring by security agencies, unemployment, amongst others. From the analysis, the result shows lack of public awareness on how to detect and prevent both technical and non-technical cyberthreats against themselves.

From the research question on how the government should address cyberthreats in Nigeria, the participants suggest that the government should address these cyberthreats through education curriculum at 25%, law enforcement agencies at 25% and public awareness at 25% as illustrated in Table 9:

Table 9: Medium to Address Cyberthreats

Medium	Number of Respondents	Percentage Response
Education curriculum	144	25%
Law enforcement agencies	144	25%
Mobile Network Providers	96	17%
Public awareness	144	25%
Technologically	46	8%
Total	**574**	**100%**

Source: Odumesi, 2015.

6.5 Public Awareness Drives

In examining the research question on what mechanism should the government use to create public awareness on cybersecurity. Table 10 illustrates the preferred public awareness mechanisms that government use, with educational institutions as the highest mechanism at 43% rate.

Table 10: Mechanism to Create Public Awareness

Mechanism	Number of Respondents	Percentage Response
Mass media	124	22%
Seminars/workshops	100	17%
Educational institutions	247	43%
Social media	103	18%
Total	**574**	**100%**

Source: Odumesi, 2015.

In exploring the research question what methods should the government put in place to help the public adopt the evolving nature of cyberthreats in Nigeria. Table 11 illustrates the preferred method that government should put in place, with strong policy and framework as the highest with 33%.

Table 11: Government support for the public

Method	Number of Respondents	Percentage Response
Strong policy/ framework	193	33%
Well trained security personnel	108	19%
Internet surveillance	91	16%
24/7 Cyberthreats complaint centre	182	32%
Total	**574**	**100%**

7. CONCLUSION

The cyberspace has become pertinent to address our collective capacity to respond to the inevitability of cyberthreats. The Nigeria government must urgently address cyberthreats issues tactically, strategically and operationally because cyberthreats is a national security issue.

Cybersecurity is a shared responsibility involving all spectra of the society from law enforcement/security agencies, academia, private sector and the general public at large. Thus, there is an urgent need to improved cybersecurity awareness by all stakeholders.

8. RECOMMENDATIONS

1. Initiate the implementation of the enacted Nigeria Cybercrime Act 2015, the National Cybersecurity Policy 2014 and the National Cybersecurity Strategy 2014.
2. The need to encourage multi-stakeholder partnership to address cyberthreats in real time and at all levels of society.
3. The urgent need to include cybersecurity curriculum at all levels of formal education and the promotion of informal awareness courses and content.

9. FUTURE RESEARCH

Future research in this area is to be carried out to measure the effectiveness of the awareness mechanism. Thus, setting standard for countries developing or yet to develop their cybersecurity strategies.

REFERENCES

[1] Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3: 77-101.

[2] Centrex Ethical Lab (2013). Cyber Attacks At Nigerian Government Websites Increased By 60% In 2012 [REPORT]. Retrieved October 12th, 2015 fromhttp://techloy.com/2013/01/17/nigerian-government-websites-cyber-attack-report/

[3] Deji, E.O (2013). Government Should Invest in Cyber Security Enlightenment. Retrieved September 26th, 2015 from http://www.thisdaylive.com/articles/deji-government-should-invest-in-cyber-security-enlightenment/164895/

[4] Fashedemi, T (2014). Nigerian IT Company Introduces Security Awareness Resources. Retrieved October 15th, 2015 http://pulse.ng/tech/cybercrime-nigerian-it-company-introduces-security-awareness-resources-id3178208.html

[5] Jack, P (2015). Nigeria Loses N159 Billion to Cybercrime over 13 Years. Retrieved November 26th, 2015 from http://bizwatchnigeria.ng/176989-2/

[6] Kaspersky Laboratory Solution (2015). Nigeria internet users highly vulnerable to cyber-attacks. Retrieved November 11th, 2015from***http://www.premiumtimesng.com/news/more-news/192904-nigeria-internet-users-highly-vulnerable-to-cyber-attacks-kaspersky.html***

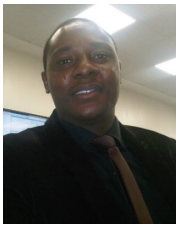
[7] Odunfa, A. (2014). Nigerian IT Company Introduces Security Awareness Resources. Retrieved October 14th, 2015 from http://pulse.ng/tech/cybercrime-nigerian-it-company-introduces-security-awareness-resources-id3178208.html

[8] National Cybersecurity Policy (2015). Retrieved September 20th, 2015 fromhttps://cert.gov.ng/images/uploads/NATIONAL_CYBESECURITY_POLICY.pdf September 16th, 2015.

[9] National Cybersecurity Srategy (2015). Retrieved September 20th, 2015 from https://cert.gov.ng/images/uploads/NATIONAL_CYBESECURITY_STRATEGY.pdf
[10] Nigerian Communications Commission (2015). Retrieved November 1st, 2015 from http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=68&Itemid=70
[11] Nigeria Cybercrime (Prohibition, Prevention, etc)Act, 2015. Retrieved September 20th, 2015 from https://cert.gov.ng/images/uploads/CyberCrime_(Prohibition,Prevention,etc)_Act,_2015.pdf
[12] National Population Commission (2006). Retrieved September 12th, 2015 from http://www.population.gov.ng/

[13] [13] Worldometers (2014).). Retrieved September 12th, 2015 from http://www.worldometers.info/world-population/nigeria-population/

Author's Brief



Odumesi John Olayemi lectures at the Civil Defence Academy, Abuja and presently on secondment to the Office of The National Security Adviser. He has a multi-disciplinary background with BSc Sociology from University of Abuja, BSc Computer and Information Systems from Achievers University, Owo and Masters degree in Information Science from University of Ibadan. He is a member of the Computer Professionals Registration Council of Nigeria (CPN), Nigeria Computer Society (NCS) and Nigerian Institute of Management (NIM). His research interests are cybercrime, cybersecurity, cloud computing, cyberforensics, critical information infrastructure and network security. He has published works in reputable peer refereed journals.