PROFESSIONAL ARTICLE DOI 10.52781/cmm.e017

The missing spice in cyber education in Nigeria: national security perspective

El condimento que faltaba en la educación cibernética en Nigeria: la perspectiva de la seguridad nacional

Abstract: Since the advent of the internet, cybercrime has become a recurring decimal in Nigeria. Many nations are battling to protect their cyber space from criminals, for national security and integration. As a result of this, efforts are being made by governments to protect their citizens and image from online crime. Some of these efforts include cybersecurity education which entails awareness raising programmes to the general public in order to sensitize them about cybercrime. Several awareness raising programmes have been conducted to universities and other educational institutions and public and private institutions. However, it was observed that such programmes have never been conducted to the clergy who are fundamental agent, perhaps one of the most important spice that tends to create influence in the life of most Nigerians. It is against this backdrop that this research seek to utilize quantitative data to reveal how the clergy in Nigeria have been left out in the propagation of cybersecurity awareness among the general public. The objective of the study was to analyze the role and influence the clergy have on their congregation and suggest ways such influence can be utilized to improve cybersecurity awareness in Nigeria for enhanced national security in the country.

Resumen: Desde el advenimiento de Internet, la cibercrimen se ha convertido en un diezmo periódico en Nigeria. Muchas naciones están luchando para proteger su ciberespacio de los delincuentes, para la seguridad nacional y la integración. Como resultado, los gobiernos están dirigiendo esfuerzos para proteger a sus ciudadanos y su imagen de la delincuencia en línea. Algunos de estos esfuerzos incluyen la educación en ciberseguridad, que implica programas de sensibilización del público en general con el fin de sensibilizarlo sobre el delito cibernético. Se llevaron a cabo varios programas de sensibilización en universidades y otras instituciones educativas e instituciones públicas y privadas. Sin embargo, se ha observado que tales programas nunca se han llevado a cabo al clero, que son agentes fundamentales y quizás uno de los condimentos más importantes que pueden influir en la vida de la mayoría de los nigerianos. Es en este contexto que esta investigación busca utilizar datos cuantitativos para revelar cómo el clero en Nigeria ha sido excluido en la difusión de la conciencia de ciberseguridad entre el público en general. El objetivo del estudio era analizar el papel y la influencia que el clero tiene en su congregación y sugerir formas de usar esta influencia para mejorar la conciencia de ciberseguridad en Nigeria con el fin de aumentar la seguridad nacional en el país.

Shehu Saidu Shehu
Nigerian Army.
Abuja, Nigeria.
saidisco@yahoo.com

Received: Apr. 04, 2020
Accepted: Jul. 12, 2020

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

1 Introduction

One of the most significant technological phenomenon that has positively affected the way of life of humans around the world is the emergence of cyberspace. Cyberspace is a virtual global domain that is increasingly impacting almost every aspect of daily life. The domain is fast shaping communication, learning as well as collaboration among individuals and organizations. It is also transforming nations by dismantling barriers to commerce and creating opportunities for innovations (OMODUNBI e colab., 2016). However, new risk and vulnerabilities that threaten national economies and security lie behind the growing dependence on cyberspace (TIIRMAA-KLAAR, 2016). Having the requisite knowledge of these existing threats which will lead to managing the risks and building appropriate prevention and recovery capabilities are the essential elements of cybersecurity. Nowadays, cybersecurity is crucial for nation's economic development and national security as cyber criminals are using the cyberspace to perpetuate nefarious acts (NELLY, 2016).

The term 'cybercrime' symbolizes online insecurity and risk and it is widely used today to describe the crimes or harms that are committed using networked technologies (OSHO e ONOJA, 2015). Conversely, cybersecurity is the protection of cyberspace systems and network from damage, unauthorized use or exploitation. It is also the method used to guard the reliability of networks and systems against fundamental cyber threats, like cyberterrorism and cybercrime. As nation states are dependent upon vast array of cyberspace networks and systems for economic development, the breach of these networks could have dire implications to national security (HILTS, 2018). Also, considering that national security is the foremost responsibility of every government, nations are developing their cybersecurity efforts in order to provide a safe and resilient cyberspace for economic development. More so, the increased cyber capabilities of cybercriminals to carry out cybercrime have certainly put the national security of states at risk (HARE, 2010).

In October 2008, U.S. intelligence officials revealed that European law-enforcement officials uncovered a highly sophisticated credit-card fraud ring that used an advanced high technology to funnels account data to Pakistan from hundreds of grocery-store card machines across Europe (SIOBHAN, 2018). Similarly, in early 2016, an attacker group named "Lazarus", traced to North Korea, stole a total of over US $100 million, mainly from the Bangladesh Bank by penetrating the Alliance Access software used by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) networks, which carries worldwide financial transactions in a (up to that point) secure and standardized way. In the same vein, an attack on Maersk by the NotPetya ransomware later in 2017 cost the shipping giant up to $300 million (KOCH e GOLLING, 2018).

Within Africa, South Africa have experienced the highest number of cyberattacks from cyber criminals. According to Dahir (2018), South Africa records high number of cyberattacks

annually as 67% of corporations have allegedly been attacked. These attacks were estimated to have cost South African economy $242 million thereby increasing unemployment rate in the country and affecting means of livelihood (VERMUELEN, 2016). Estimating the net loss generated by cybercrime is a challenging task. Official numbers published by government or non-government bodies are weak indicator as only those cases filed with them are included. However, the most recent report indicates that the global cost of cybercrime is about $600 Billion USD including gains to criminals and cost to companies for recovery and defence (LEWIS, 2018).

Nigeria has over 120 million Internet users representing 24 per cent of all Internet users in Africa (INTERNET WORLD STATS, 2019). This internet usage consist predominantly of mobile internet usage as against fixed broadband subscriptions. However, this growing dependence on internet usage comes with threat exposures and vulnerabilities especially in a country popularly known for "yahoo yahoo"[1] (TADE e ALIYU, 2011). Research has revealed that 80% of these yahoo yahoo boys are youths and sometimes students of various higher institutions (ARANSIOLA e ASINDEMADE, 2011). Government agencies down to the general public have all been victims of these group of people.

This group of criminals continue to thrive despite several hard and soft efforts emplaced by the Nigerian government to curb the ugly menace in the country. The hard effort employs utilizing the various cybercrime legislations to deal with the arrested offenders whereas the soft effort entails cybersecurity education, training and skills. At the invitation of the Office of the National Security Adviser (ONSA) in October 2018, Global Cyber Security Centre (GCSCC) undertook a review of the maturity of cybersecurity capacity in Nigeria using the Cybersecurity Maturity Model (CMM)[2] which is composed of 5 distinct dimensions of cybersecurity capacity. In the third dimension, GCSCC reviews the availability of cybersecurity awareness raising programme for both public and executives. However, it was observed that the Centre did not consider awareness raising programmes to the clergy who are an important spice[3] of the cultural fabric of communities and, as such, can influence decision making, ideologies, and moral and ethical behaviors of people (PINTER e colab., 2016).

The purpose of this research therefore is to reveal how the clergy in Nigeria have been left out in the propagation of cybersecurity awareness to the general public, the group worst hit by cybercrime. The objective of the study was to analyze the role and influence the religious leaders have on their congregation and suggest ways such influence can be utilized to improve cybersecurity awareness in Nigeria for enhanced national security in the country. The study is significant as the outcome would assist in policy improvement and would add to the existing body of knowledge in cybersecurity.

1 Yahoo Yahoo is a slogan used in Nigeria referring to cybercrime.

2 See Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition at; https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition. Access on: Sep 21, 2019.

3 Spice is used here to mean "an attribute that makes something appealing, interesting or engaging".

The research was an applied one that employed empirical data that were collected and analysed. Field method of data collection using interviews and Questionnaires was utilized and the collected data were analysed quantitatively. Additionally, the sample size of the study was calculated using Taro Yamane Sample Size Formula. The study adopted cluster random sampling and the generated data was presented using charts to illustrate the relationships between the variables in the study. The study is limited to the clergy as well as 6000 to 8000 words.

2 Literature review

2.1 Background

Internet usage and subscribers have grown exponentially in Nigeria within recent years. Consistent with Section 89 Subsection 3(d) of the Nigerian Communications Act 2003 (NCA 2003)[4], the Nigerian Communications Commission (NCC, 2019) report stated that the number of active mobile phone and internet subscribers in Nigeria is about 175 million and over 120 million respectively. The high number of internet subscribers are mostly youths seeking for productive employment, social engagement and increased global connectivity. However, with this growing prosperity and digitization comes threats, risks, vulnerabilities and cybercrimes that could undermine national security. Cybercrimes are essentially criminal activities where computers, network or electronic information technology devices are the source, tool, target or place of crime. Cybercrimes are effected by way of illegal access into another's data base, illegal interception, data interference, system interference, misuse of devices, forgery and electronic scams (BAIDEN, [S.d.]).

2.2 Cybercrime

In Nigeria, cybercrime has become one of the main avenues for pilfering money and business espionage. Within the Nigerian cyberspace, Serianu (2017) revealed that the cost of cybercrime in Nigeria is about $649 million with 81% of cyber incidents caused by proliferation of fake news, ransomware and internet scams and the category most hit are the general public. In August 2019, the US authorities unearthed and charged 80 people, most of whom are Nigerian yahoo yahoo boys in $46 million internet scam (FARIVAR, 2019). The scammers were alleged to have victimized individuals and small and large businesses by using a tactics referred to as "business email compromise (BEC)"[5].

4 The act mandated NCC to monitor and report on the state of the Nigerian telecommunications industry, provide statistical analyses and identify industry trends with regards to services, tariffs, operators, technology, subscribers, issues of competition and dominance, etc, with a view to identifying areas where regulatory intervention would be needed.

5 A BEC is an exploit in which the attacker gains access to a corporate email account and spoofs the owner's identity to defraud the company or its employees, customers or partners of money.

The FBI and Nigeria's anti-graft agency, the EFCC[6], revealed that 167 people in Nigeria and 74 in the United States had been arrested, weeks after US officials released a list of Nigerians suspected of being behind the online scam. Such arrested cyber criminals and several others are usually prosecuted by EFCC in line with the extant laws so as to serve as deterrence to others. Therefore, aside the arrest and prosecution of the criminals, the government requires a robust cyber education initiative focusing on awareness raising programme on cybersecurity risks and threats as well as how to address them, for the general public, government stakeholders and private sector.

2.3 Cyber Education

It was envisioned that lack of security best practice awareness, user education and sensitization programmes could be the principal factors attributed to exposing most Nigerians to cyber threats. However, it was realized that there exist a lot of cybersecurity awareness initiatives organized by some organizations in collaboration with ONSA, National Information Technology Development Agency (NITDA), EFCC, Central Bank of Nigeria (CBN), and NCC among others aimed at raising awareness of executes and the general public about the importance of cybersecurity. Such initiatives include annual National Cyber Security Awareness Month (NCSAM) organized by International Centre for Leadership Development Nigeria (ICLDNG). The last NCSAM was held in October 2018 (ICLNG, [S.d.]). Others are the provision of specialized academic courses in cybersecurity at Nasarawa State University (CCS-NSUK, [S.d.]), First Technical University (TECH-U, [S.d.]), Federal University of Technology (SICT-FUTMINNA, [S.d.]) and Nigerian Defence Academy Kaduna (NDA, [S.d.]).

There equally exist an annual cybersecurity conference referred to as Cyber Secure Nigeria Conference organized by the Cybersecurity Experts Association of Nigeria (CSEAN). The association aims to bring together cybersecurity research from both industry and academic (CSEAN, [S.d.]). Additionally, service providers such as the E-Payment Providers Association of Nigeria (E-PPAN) were also said to participate in public awareness campaigns, particularly around the use of electronic payment platforms. Furthermore, an uptake of international security professional certification such as ISACA and International Organisation for Standardisation (ISO) 27000 series was observed (GCSCC 2018). Outside academic and official establishments, there exist some cybersecurity related community programmes for children. This programme is part of summer school offered to primary and high school pupils (DIGITAL PEERS INTERNATIONAL, 2019).

6 EFCC means Economic and Financial Crimes Commission.

The aforementioned awareness raising programmes appeared to have been all encompassing. However, GCSCC who was invited by ONSA to undertake a review of the maturity of cybersecurity capacity in Nigeria with a view to enabling Nigeria gain an understanding of its cybersecurity capacity in order to prioritize investment in cybersecurity capacities strategically observed that there is a need for greater partnership between academia and industry in cybersecurity research. The Centre further observed that adequate resources to facilitate cybersecurity education in the universities needed to be provided and membership of CSEAN is only open to IT students, graduates and professionals and those without IT training who work in organization where they make decisions that relate to IT. He further observed that rather than a complete month, NCSAM was only conducted for two days due to the constraints of other initiatives taking place. Following the review of the maturity of cybersecurity education, GCSCC made some recommendations aimed at providing advice and steps to be followed for the enhancement of existing cybersecurity capacity of Nigeria. A perusal of the review made by GCSCC revealed that there was no mention of any awareness campaign organized to the religious leaders in the mosque and churches among the list of all the places where cybersecurity awareness raising campaign was enumerated. It was also observed that the composition of stakeholder for the review by GSCSS did not include the clergy neither were they captured in the recommendations of the Centre.

2.4 Influence of the Clergy on the Nigerian Populace

Nigeria is a country divided roughly in half between Christians, who live mostly in the southern part of the country and Muslims in the northern part with a minority of the population practising religion indigenous to Nigeria. (NWAUBANI, 2014), a BCC writer and novelist, revealed that in Nigeria, a country that lays claim to a great percentage of Africa's most acclaimed entertainment celebrities and intellectuals, the Facebook and Twitter pages with the highest number of followers are those of the clergy. She further revealed that many religious leaders in Nigerian are regarded as superstars and play a positive role in the country. She added that should the leaders of Nigeria's five largest churches hint that no-one should have anything to do with the renowned novelist, Chinua Achebe, the author's fan base and book sales in Nigeria would instantly, unquestionably plummet and his works would be struck off the national curriculum, irrespective of how widely acclaimed he is around the world. In Nigeria, most who belong to one religion or the other perceive spirituality as a part of religion. On this issue, Aja (2019, Vol. 73(2) p. 82 – 87) stressed that:

> They tend to define spirituality in a variety of ways, including believing or having faith in the transcendent, having hope in the transcendent, having a relationship with the transcendent and being religious, opening one's heart to the transcendent, going to church, going to the mosque,appeasing the transcendent, doing all that the transcendent commands, observing religious tenets. Some may define spirituality using a combination of two or more of these definitions. The transcendent here could be God, Jesus, Allah, or gods, depending on the religious tradition. Adherents of the Islamic religion, as well as those of traditional religion, believe in the supremacy of God.

Passion for religion has crept deep into all facets of life of Nigerians and hardly can it be relegated to the background. The religious prohibition of family planning was attributed to be the main ingredient that inhibited the success of family planning programme in Nigeria (LAWANI e colab., 2015). Likewise, Nwaubani (2014) revealed that when Nigerians were convinced that their votes wouldn't count in 2007 general elections unless they get registered, people queued for hours simply because their pastors enjoined them to do so. The BBC reporter added that religious leaders also played key roles in battles against Polio, HIV and tackling the Ebola outbreak in Nigeria by passing on relevant information and stressing the urgency of the situation from their pulpits. Therefore, the clergy could turn out to be Nigeria's greatest assets in cyber awareness raising campaign if their immense influence was harnessed in more structured and focused ways.

3 Methodology

The method of data collection adopted in this study was field method. This method utilized a combination of interviews and questionnaire methods. The primary data for the study was collected from cybersecurity professionals who are deployed in agencies such as ONSA, NITDA, NCC, EFCC, Defence Space Administration (DSA) and Nigerian Army Cybersecurity Centre. Others are the clergy from the various places of worship. Since the greatest population of Nigerians are Muslims and Christians, the clergy studied were those in the mosque and churches. Two sets of questionnaires were sent out. One was to target the professional audience in order to unravel whether they had ever considered the clergy for their awareness raising programme. The second questionnaire was to the clergy in order to know their level of cyber awareness and whether they had ever received any form of awareness campaign. The Questionnaires whose reliability was α =0.94 and 0.73 for the clergy and the cybersecurity professions respectively as against Cronbach's Alpha recommended α = .70 (UNIVESITY OF CALIFORNIA, [201 -]) was used to generate data and the collected data were analysed quantitatively using Microsoft Excel. As the respondents were in Nigeria, the researcher sent the questionnaires through WhatsApp to Squadron Leader Ngulde and Flight Lieutenant Akintunde who assisted with the distribution, supervision and retrieval (BASSIC- RESEARCH, 2019)[7].

The secondary sources of data was obtained from relevant journals, seminars, conference papers as well as magazines. Others are online newspapers, unpublished researches and other relevant materials from the internet. Taro Yamane Sample Size Formula with a margin error of 5% and confidence level of 95% was used to calculate the sample size of the study (QUORA.COM, [S.d.]). This resulted in about 98 and 65 sample size of the study for the clergy and cybersecurity professionals respectively. The study adopted cluster random sampling as the clergy considered were only those who administer within the security services living area. Equally, the second respondents from the professional point of view considered were those

7 The questionnaires can be accessed at: https://drive.google.com/open?id=1LdXeL5f7iCNwCE2xXC9AeEc1HU4PREdR. Access on: Sep 21, 2019.

employed professionally to deal with cybersecurity. This is because all the organizations who plan and execute the awareness campaigns always do it in collaboration with the government agencies. The data generated was presented using charts to illustrate the relationships between the variables in the study.

The theoretical paradigm that would be used to analyze the use of the clergy in cybersecurity awareness by the cybersecurity professionals is the Theory of Planned Behaviour. The core claim of this theory is that it seeks to predict behavioral intention, or how likely a person would be performing a particular behavior. The researcher added that a person is more likely to perform a specific behavior if the behavior is deemed important and if he/she believes others would approve of the behavior (AJZEN, 2002; BLOOMFIELD, BOMMARITO, KUHL, 2015).

4 Analysis and presentation of data

This chapter presented and analyzed the data collected from the respondents. The analyzed data was represented in numbers and percentages. Furthermore, each question from the set of questions on the questionnaire was analyzed in a chart form so as to show the details of the responses. Eighty-Nine questionnaires were administered to the clergy whereas sixty- five were issued to the cybersecurity professionals. All the questionnaires were returned and duly completed.

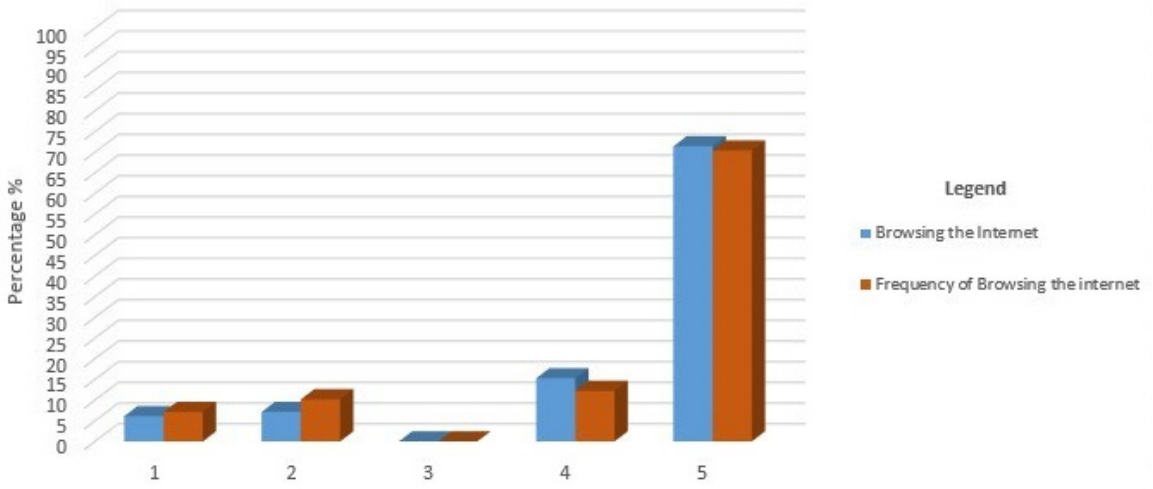
4.1 Analysis of Data Obtained from the Clergy

The data analyzed in this section is that of the clergy. The data was not analyzed in terms of those who administer in the mosque or church but as data from the religious centres. There were 16 questions in all and each question was given a rating of 1 to 5 with 1 being the feeblest and 5 the sturdiest.

4.1.1 Knowledge of the Internet

The researcher requested to know whether the respondents browse the internet and how often they do it. The responses from the respondents are as shown in Graph1 below.

Graph 1 – Chart of Respondents' View on Knowledge of theInternet



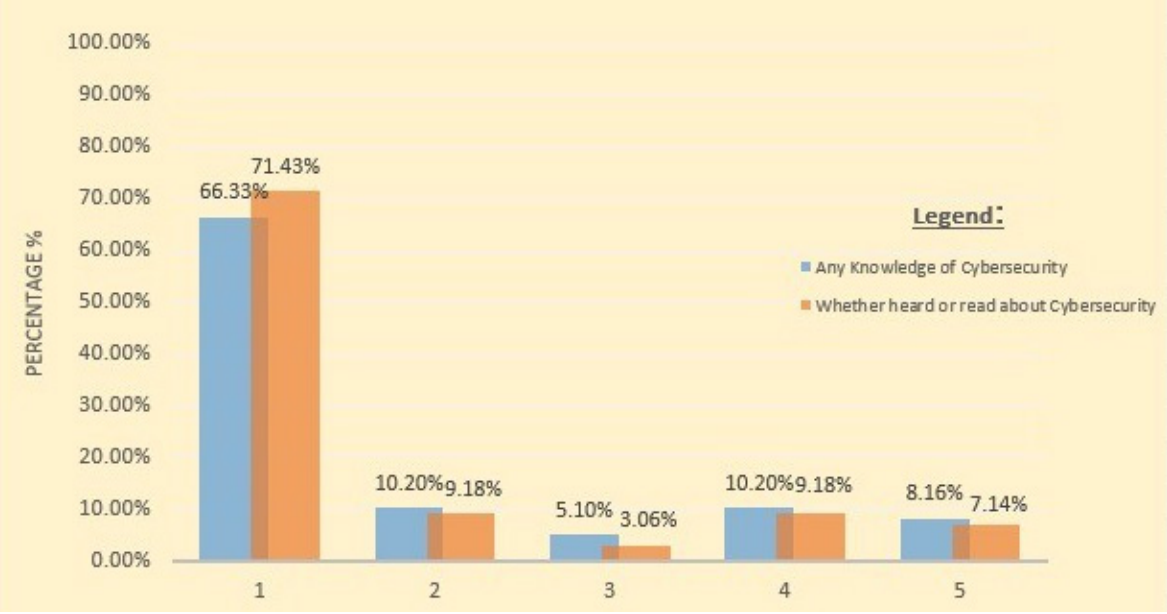
Source: Author (2019).

Graph 1 above shows that 71.43% of the respondents browse the internet very well where as 15.31% browse the internet well while 6.12% never browse the net. The high percentage of those who browse the internet as against the low percentage of those who do not correlates with the report of NCC which stated that there are 120 million internet subscribers as at 2019 (NIGERIAN COMMUNICATIONS COMMISSION, 2019). The figure equally revealed that 70.41% of the respondents visit the internet most frequently against 7.14% who do not visit the internet. The outcome of the survey on the two questions therefore proved the veracity of the NCC report.

4.1.2 Knowledge of Cybersecurity

The researcher requested to know whether the respondents have any knowledge of cybersecurity, read or heard about it. The survey result of the respondents' view on the questions are as shown in Graph 2 below.

Graph 2 – Chart Showing Respondents Knowledge of Cybersecurity



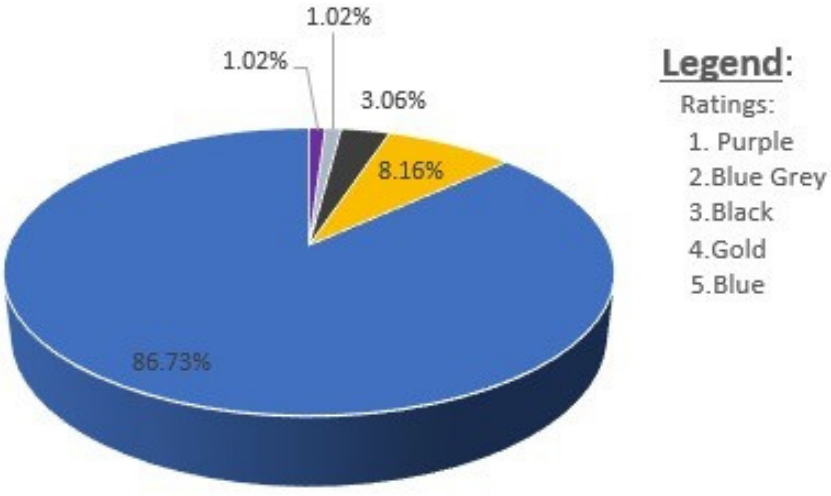
Source: Author (2019).

Graph 2 above revealed that 66.33% of the clergy claimed to have no knowledge about cybersecurity. The report further revealed that 71.43% of them had neither read or heard about it. The figure further revealed that 8.16% of the respondents claimed to have had a very good knowledge of cybersecurity whereas 10.20% opined having knowledge about it. On the other hand, 7.14% of the respondents indicated having a very good knowledge of cybersecurity through either reading or hearing about it from someone while 9.18% revealed good knowledge of reading or hearing about it as well. The sharp variance between the respondents who have no knowledge of cybersecurity to those who had known about it might indicated that those who have heard about it did so not necessary as a result of a cyber awareness campaign organized in the place of worship.

4.1.3 Knowledge of any Cybersecurity Awareness Campaign Organized in a Place of Worship

The researcher inquired whether any cybersecurity awareness campaign had been organized in the places of worship of the respondents and the result of field survey on their view is as shown in Graph 3 below:

Graph 3 – Chart Showing the Result of Knowledge of any Cybersecurity Awareness Campaign Organized in a Place of Worship



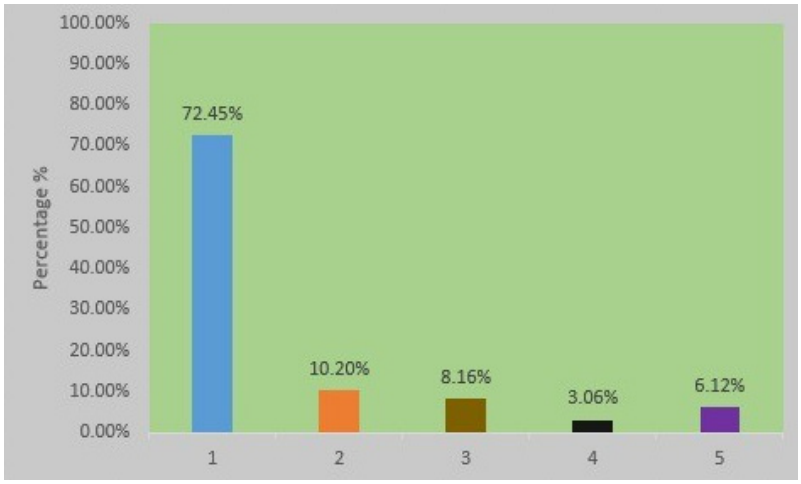
Source: Author (2019).

FromGraph 3above,it can be seen that 86.73%oftherespondentshadnoknowledgeofany cybersecurity awareness campaign conducted in their place of worship. It could therefore be deduced that the high percentage obtained here has given credence to the analysis of the researcherinSection4.1.2thatthelittlepercentageoftherespondentswhohaveknowledgeof cybersecurity did that on their own accord and not as a result of cybersecurity awareness campaign organized forthem.

4.1.4 Knowledge of Cybercrime

The researcher asked whether the respondents are aware of cybercrime and the result of the survey is as shown in Graph 4 below.

Graph 4 – Chart Showing the Result of Knowledge ofCybercrime



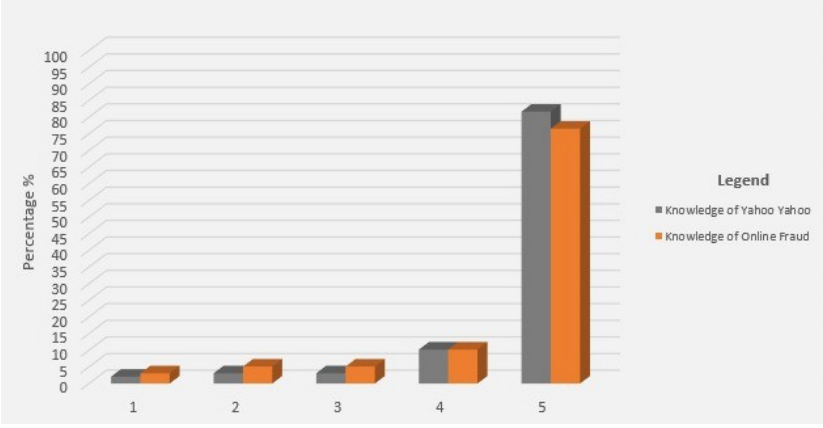
Source: Author (2019).

Graph 4 above revealed that 72.45% of the respondents have no knowledge of cybercrime. The revelation here is potentially worrisome if considered within the context of the result obtained in Section 4.1.1 and the revelation by Business Day (AKIYODE-LAWANSON, 2019) that Nigeria ranks third at 37.72% by share of users attacked by mobile malware.

4.1.5 Knowledge of Yahoo Yahooand 419[8]

The researcher enquired whether the respondents have knowledge of Yahoo Yahoo and 419 in Nigeria and the result of the survey is as shown in Graph 5 below.

Graph 5 – Chart Showing the Result of Knowledge of Yahoo Yahoo and 419



Source: Author (2019).

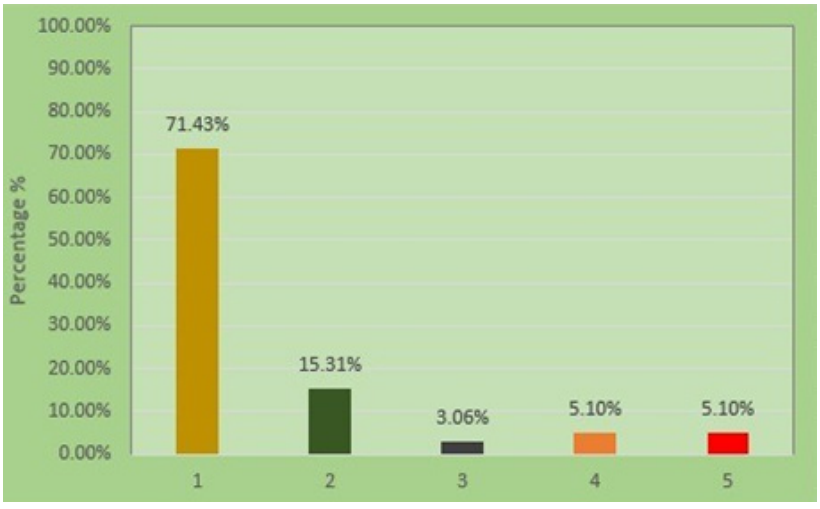
8 419 is generally used to describe fraudulent activities. It originated from Section 419 of the relevant extant laws of Nigeria which criminalizes financial fraud and internet scam or cyber-fraud in Nigeria.

From Graph5, it could be seen that 81.63% and 76.3% of the respondents are aware of Yahoo Yahoo and 419 respectively. The high percentage obtained here might be as a result of a popular antic of the Yahoo Yahoo of sending fraudulent messages to dupe GSM network subscribers. Tade and Aliyu (2011) revealed that the criminals having knowledge of the working of the telecommunication promotions, cloned it and exploited it to defraud Nigerians by sending fraudulent messages on their phones concerning a huge amount of money they have won. The researchers further revealed that the criminals then request the victim to send a certain amount of credit to a particular number before calling the number to negotiate how the prize would be picked up. Such acts therefore made Yahoo Yahoo and 419 very popular in Nigeria.

4.1.6 Knowledge of Correlation between Cybercrime, Yahoo Yahoo and OnlineFraud

The researcher requested to know whether the respondents are aware that cybercrime is the same as Yahoo Yahoo and 419. The result of the study is as shown in Graph 6 below.

Graph 6 – Chart on Respondents' view on any Knowledge of Correlation between Cybercrime Yahoo Yahoo and Online Fraud



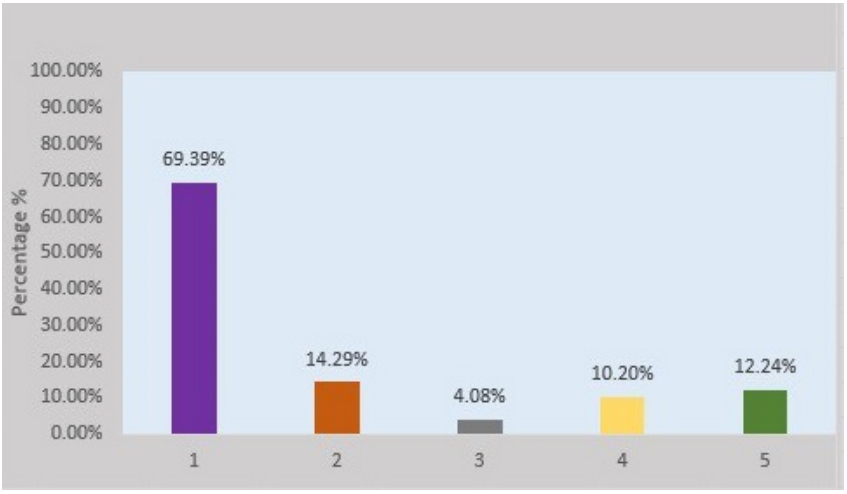
Source: Author (2019).

From Graph 6 above, it could be seen that 71.43% of the respondents are not aware of any correlation between cybercrime, Yahoo Yahoo and 419. From the results obtained in Section 4.1.4 and Section 4.1.5, it could be seen that the respondents have ample knowledge of Yahoo Yahoo and 419 but have no idea what cybercrime means. Therefore, the fact that they are not aware that Yahoo Yahoo, 419 and cybercrime means the same thing indicated that they see Yahoo Yahoo and 419 from the prism of duping an individual and having nothing to do with cyberspace.

4.1.7 Knowledge of any Action to be Taken when Hit byCybercrime

The researcher inquired whether the respondents have any knowledge of the actions to be take when hit by cybercrime. The result of the survey is as shown in Graph 7 below.

Graph 7 – Chart Showing the Result of Action to be Taken when Hit by Cybercrime



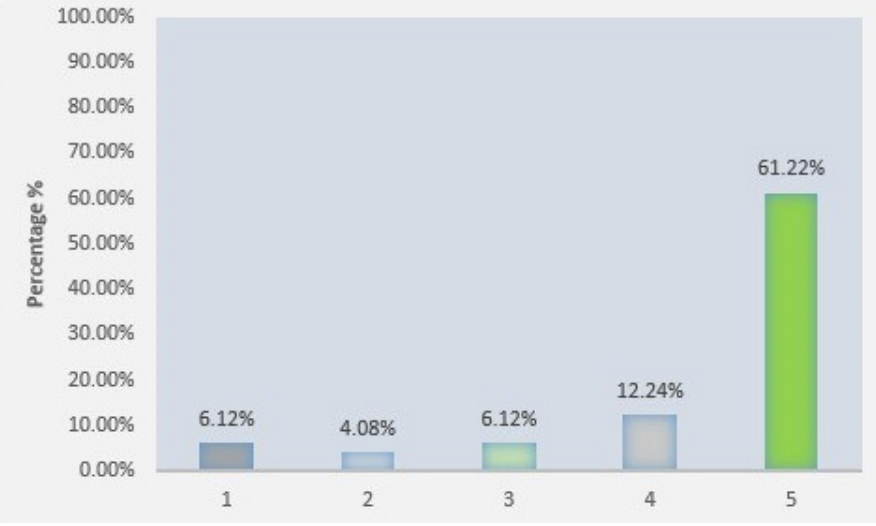
Source: Author (2019).

Graph 7 revealed that 69.39% of the respondents have no knowledge of the action to be taken when hit by cybercrime. The chart further revealed that only 12.24% were aware of the action to be taken. The high percentage of those who were not aware of the action to be taken is not surprising owing to the lack of knowledge of cybersecurity by the respondents. This lack of knowledge by the respondents can be said to be worrisome especially with the CBN (CBN, 2019) circular to all deposit money banks notify them of its policy to implement charges for withdrawals and lodgments on individuals and corporate bodies in order to enforce the government's drive to a cashless society. The circular stated the charges as 3% and 2% to be meted out on individuals for cash withdrawals and lodgments respectively while 5% and 3% apply to corporate organizations. The fact that the charges are effective 31 March 2020 means that all financial activities in the country will be online with effect from that date. There fore, the need for aggressive cybersecurity awareness campaign to mitigate the risk inherent in cyberspace.

4.1.8 Knowledge of being Affected by Yahoo YahooBoys

The researcher inquired whether the respondents had ever been hit by Yahoo Yahoo boys and the result of the field survey is as shown in Graph 8 below:

Graph 8 – Chart Showing Result for Knowledge of being Affected by YahooYahoo



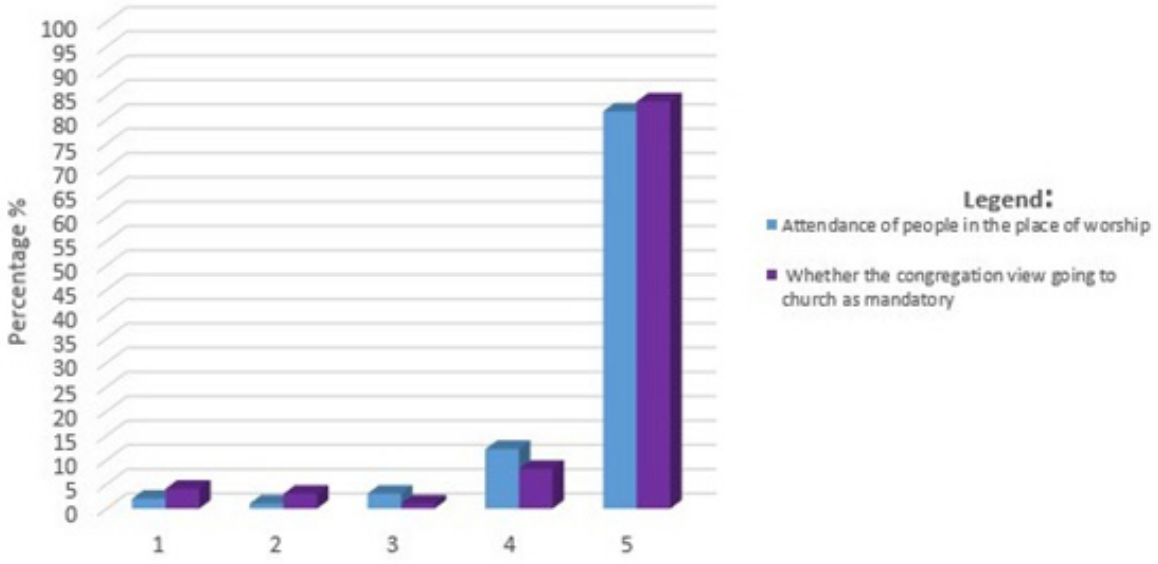
Source: Author (2019).

Graph 8 revealed that 61.22% of the respondents were well hit by Yahoo Yahoo boys while 12.24% were moderately hit. The high response observed here might be as a result of being hit by GSM scam or an encounter with the "distress traveler". The phenomena of a distress traveler is a scenario in Nigeria where a criminal, neatly dressed and looking responsible, paints a scenario of being stranded and short of bus fare and begs for assistance to reach his destination when in effect, he is only employing that tactics in order to defraud people of their money.

4.1.9 Knowledge About Religious Worship

The researcher requested to know the attendance of the congregation to the places of worship and whether they visualized their attendance as mandatory on them. The response of the respondents' is as shown in Graph 9:

Graph 9 – Charts Showing Result for Knowledge about Religious Worship



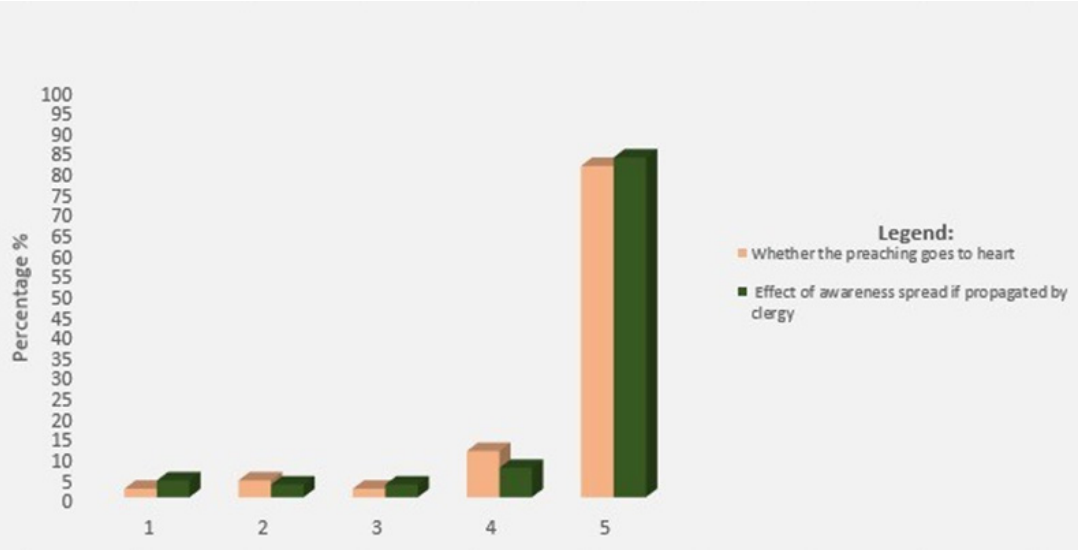
Source: Author (2019).

From Graph 9 above, it could be seen that 81.63% of the respondents believe that the populace attend the various worship very well. Equally, 83.61% of the respondents believe that the congregation visualize that coming to worship is mandatory on them. This therefore correlates with the revelation by Ajah (2019) that most people who belong to one religion or another in Nigeria perceive spiritually as part of the religion. The obtained result also correlated with a BBC 2010 survey which revealed that 87% of Nigerians said religion was very important to their lives. Another BBC report of 2014 also revealed how meetings of Nigeria's mega- churches pack football stadiums full.

4.1.10 Influence of the Word of the Clergy on the Congregation

The researcher requested to know the view of the respondents towards how their preaching's are taken to heart by their congregation and the resultant effect therein. The result of the survey is as shown in Graph 10 below.

Graph 10 – Chart Showing Result for Influence of the Word of the Clergy on the Congregation



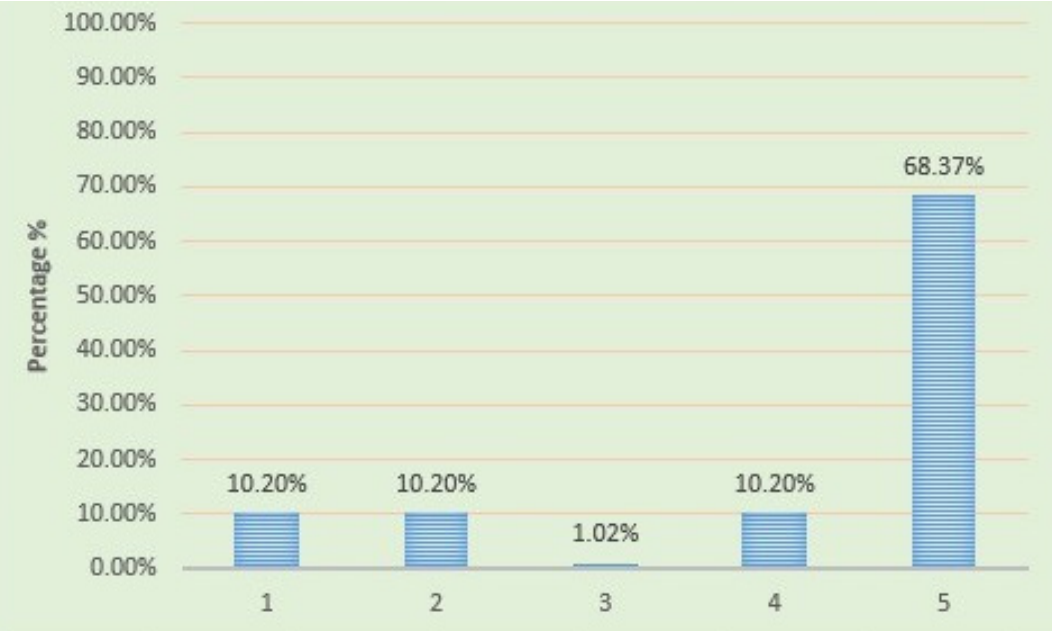
Source: Author (2019).

From Graph 10 above, it could be seen that 80.61% of the respondents believe that the congregation are totally submissive to their preaching. Additionally, the survey revealed that 82.65% of the respondents are also of the view that the spread of the cybersecurity awareness will be wide if they use their pulpit to propagate it. The two results obtained in this research goes in tandem with the BBC 2010 survey as revealed by Nwaubani (LETTER..., 2014) that majority of people in Nigeria are deeply committed to the practices and major tenants of both Christianity and Islam. The obtained result from the survey may have equally emphasized Nwaubani's stance that the books published by the clerics are best sellers in a society that is frequently accused of having a poor reading culture. The report further revealed that text messages instructions from renowned clerics are usually taken seriously in Nigeria, and most often go viral.

4.1.11 Effect of Cybersecurity Awareness Campaign on Mitigating Cybercrime

The researcher requested to know whether the respondents believe that the activities of the cybercriminals could be drastically curtailed if there is great awareness of cybersecurity and criminality. The result of the survey is as shown in Graph 11below.

Graph 11 – Chart Showing the Effect of Cybersecurity Awareness Campaign on Mitigating Cybercrime



Source: Author (2019).

Graph 11 above revealed that 68.37% of the respondents are optimistic that great awareness of cybersecurity could help curtail the activities of cybercriminals. This revelation is supported by 10.20% who also believe that awareness campaign could have a militating effect on the activities of cybercriminals. The result obtained herein is akin to the revelation by Johnson e Bowers (2003) that publicity can tremendously improve the effectiveness of crime reduction. The researcher added that a carefully organized awareness campaign may represent a powerful cost effective tool in crime prevention.

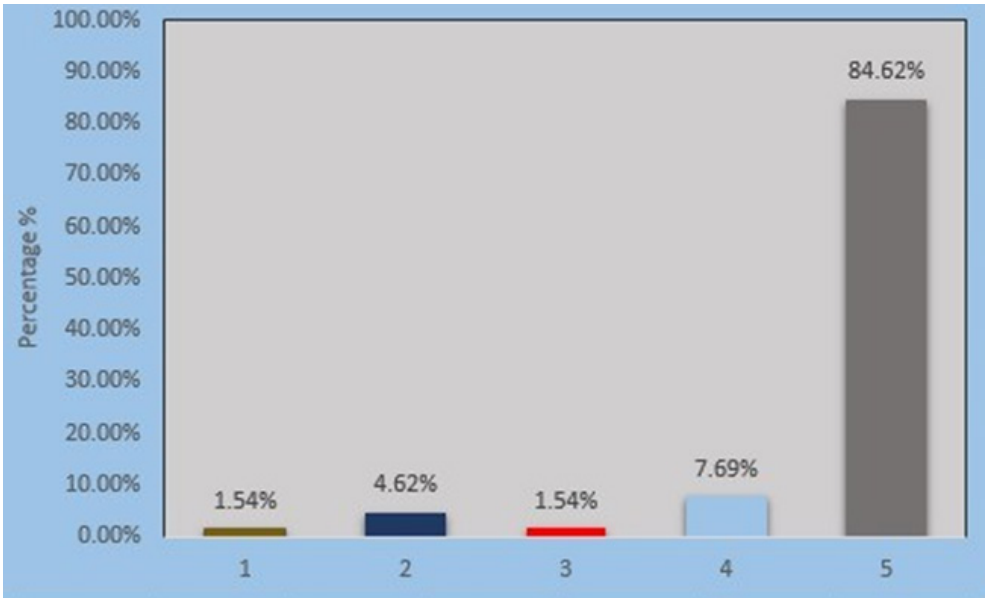
4.2 Analysis of Data Obtained from Cybersecurity Professionals

This section discussed the data obtained from respondents who are deployed in cybersecurity related fields within the various governmental agencies. Such agencies included ONSA, NITDA, EFCC, DSA and Army Space Command. Respondents from private organizations were not considered because they always organize cybersecurity awareness campaigns in collaboration with the government agencies. The data was not analyzed in terms of that obtained from each agency but as data from the professional agencies. There were 4 questions in all and each question in the questionnaire was given a rating of 1 to 5 with 1 being the feeblest and 5 the sturdiest.

4.2.1 Conduct of Cybersecurity AwarenessCampaign

The researcher requested to know whether the respondents had ever been engaged in the conduct of cyber awareness campaign and the result of the survey is as shown in Graph 12 below:

Graph 12 – Chart Showing Result for Conduct of Cybersecurity Awareness Campaign



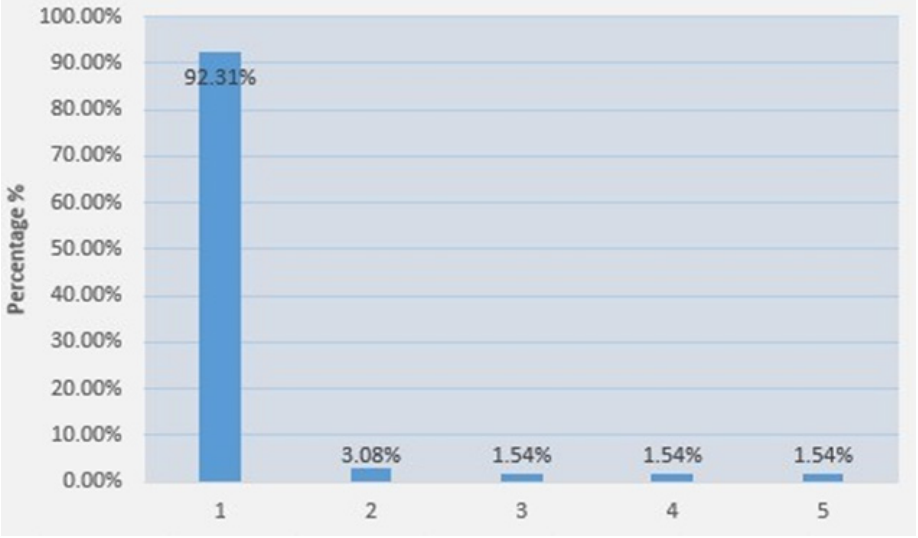
Source: Author (2019).

From Graph 12 above, it could be seen that 84.62% of the respondents strongly agreed to have taken part in cybersecurity awareness campaigns. The sharp contrast in the frequently of those who strongly agree to have taken part in awareness campaigns to 7.69% of the respondents who agreed to have taken part revealed that almost all the staff across the agencies had in one way or the other been engaged in cybersecurity awareness campaign. This revelation tallied with the finding of GCSCC's (2018) review of the maturity of cybersecurity capacity in Nigeria which revealed that national initiatives for cybersecurity awareness raising takes place in Nigeria. It further revealed that October 2018 was NCSAM additional to other pocket of awareness-raising activity that existed in the nation. The review further revealed that organization such as CSEAN, (E-PPAN) were said to participate in public awareness campaigns while a number of Nigerian universities offer cybersecurity courses along with some cybersecurity researches.

4.2.2 Conduct of Cybersecurity Awareness Campaign in any Place of Worship

The researcher requested to know whether the respondents had ever organized any cybersecurity awareness campaign in any place of worship and the result of the survey is as shown in Graph 13 below.

Graph 13 – Chart Showing Result for Conductof Cybersecurity Awareness Campaign in any Place of Worship



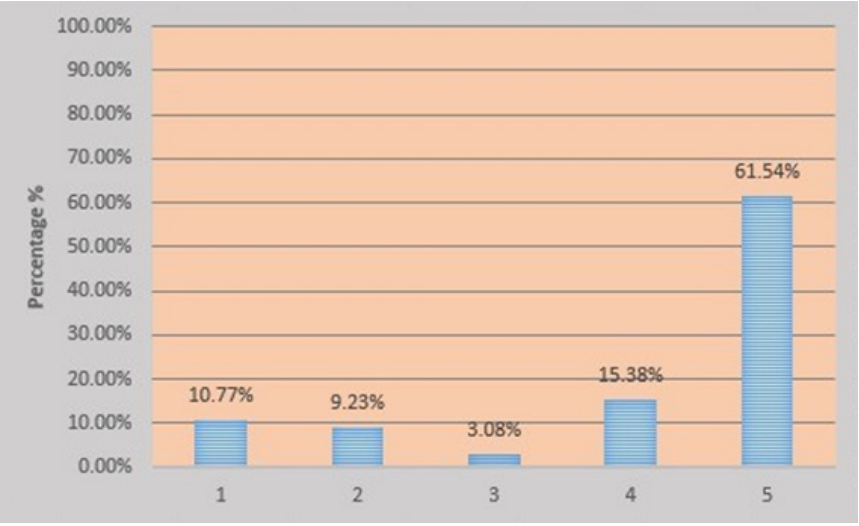
Source: Author (2019).

Graph13 above revealed that 92.31% of the respondents strongly agreed that they had never organized any form of awareness raising campaign in any religious worship centre. The high percentage gotten from the survey corroborated the view of Lieutenant Colonel M. B. Fakandu, Assistant Director, Critical Information Infrastructure Protection (CIIP), ONSA, when interviewed on phone that his office had never conducted any cybersecurity awareness campaign to a religious institution since his appointment into the office. He added that a perusal of the official archive equally revealed no evidence of an earlier activity of that nature. Furthermore, Mr. Sa'ad Abubakar, Head of Cybercrime Unit of EFCC shared the same view when he was interviewed on phone. The duo also professed having no knowledge of cybersecurity awareness campaign organized by other cybersecurity agencies because it had never been brought up at the National Cybersecurity Advisory Council neither was it brought up at the Nigerian Computer Emergency Response Team (ngCERT) routine meetings (BASSIC-RESEARCH, 2019).

4.2.3 Influence of Religion to theSociety

The respondents were asked the influence of religion on the society and their responses are given in Graph 14 below:

Graph 14 – Chart Showing Result for Influence of Religion on the Society



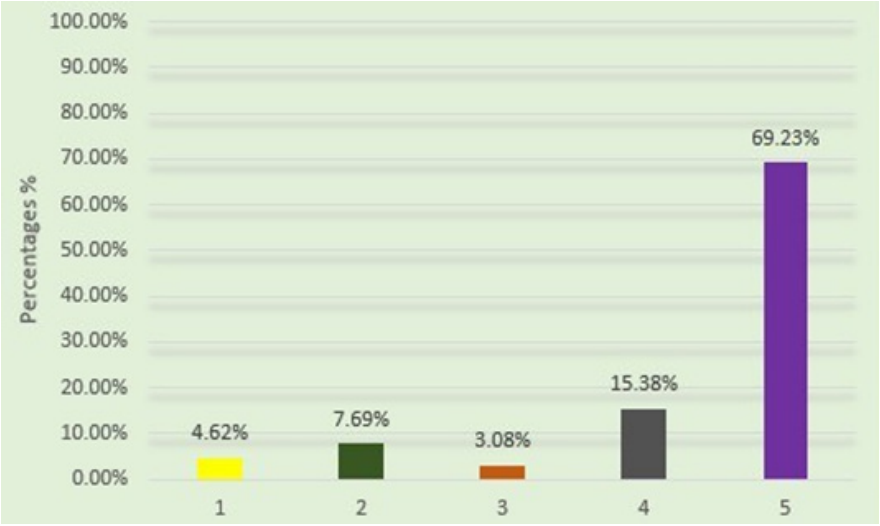
Source: Author (2019).

Graph 14 above revealed that 61.54% of the respondents believed that religion has a tremendous influence on the society in Nigeria. 15.38% also believed that religion does have an influence on the Nigerian populace. The result obtained in this investigation might be said to concur with Ojonemi e Colab., (2014) that religion in Nigeria and faith are critical aspects of everyday life and influences laws, thoughts and attitudes. The researchers further stated that religion plays a major role in the formulation of policies and major public projects owing to the importance ascribed to it.

4.2.4 Impact of Religious Leaders in Propagating Cybersecurity Awareness

The researcher requested to know the impact religious leaders can have in the propagation of cybersecurity awareness and the result obtained are as shown in Graph 15 below:

Graph 15 – Chart Showing Result for the Impact of Religious Leaders in Propagating Cybersecurity Awareness



Source: Author (2019).

From Graph 15 above revealed that 69.23% of the respondent believed that religious leaders can have a great impact on propagation of cybersecurity awareness. The figure further revealed that 15.38% of the respondent believed that the clergy can have an effect in the propagation of cybersecurity awareness. The revelation could be said to be true considering that the religious point of view on family planning had been inhibiting the success of all organized interventions aimed at increasing contraceptive uptake in Nigeria thereby leaving the country with one of the lowest Modern Contraceptive Prevalent Rate (mCPRP) estimated at 9.8% (NPC-ICF, 2014). However, having known that religious leaders in Nigeria can substantially influence and shape people's ideas and views about issue, Nigerian Urban Reproductive Health Initiative (NURHI) decided to partner with the religious leaders to promote awareness on the use of contraceptives. Adedini e colab (2018), who documented the research revealed that the decision of 66.4% of the women who agreed to family planning was influenced by continued inspiring statements in support of family planning in public gathering and through the media by the clergy.

5 Summary of findings

The study investigated the missing spice in cybersecurity education in Nigeria: National Security Perspective. To achieve that, sixteen and four research questions for the clergy and cybersecurity professionals respectively alongside interviews were generated for the study. The data obtained were quantitively analyzed and presented using charts to illustrate the relationships between the variables in the study. Consequently, the summaries of the findings are:

a. The clergy have ample knowledge of the internet and visit the internet frequently.

b. The clergy have no knowledge of cybersecurity.

c. The clergy never had any cybersecurity awareness campaign organized in their place of worship.

d. The clergy have no knowledge of cybercrime.

e. The clergy are aware of Yahoo Yahoo and 419 but have no idea that it is the same as cybercrime.

f. The clergy had in one time or the other been affected by cybercrime.

g. The clergy do not know the action to be taken in the event of a cyber-attack.

h. A great number of people always attend services in various places of worship.

i. Messages from the pulpit have great influence on the Nigerian masses.

j. Cybersecurity awareness campaign will have a great militating effect on cybercrime.

k. Cybersecurity professionals have conducted a lot cybersecurity awareness campaigns.

l. Cybersecurity professionals have never organized any cybersecurity awareness campaign to places of worship.

m. Religion has a tremendous effect on the Nigerian society.

n. Inclusion of the clergy in cybersecurity awareness campaign will have a great resultant effect in cyber education to the Nigerian society.

In line with the findings of the study, it is recommended that future cybersecurity awareness campaign should be organized to the clergy in order to drive the maximum benefit inherent in their influence on the Nigerian society.

6 Conclusion

Over the past decade, the internet has experienced an explosive growth with the number of hosts connected to it increasing daily at an exponential rate. As the internet grows to become more accessible and more services become reliant on it for their daily operation, so does the threat landscape. States gradually come to terms with the cyber perils and established guidelines, policies and institutions to deal with it. Despite that, internet fraud is definitely expected to rise as the amount of e-commerce increases on the internet and the current drive by the Nigerian government to press home its cashless policy. In view of this, various programmes were designed by the government to raise awareness of cybersecurity risk and threats as well as how to address them in order to serves as a veritable tool for mitigating the perils of cybercrime and enhancing national security. However, the drive by the government might not be felt owing to the fact that all the organized cybersecurity awareness campaign were around training institutions and official coffers whereas the greater population of the country are unemployed. Consequently, with religion being a fundamental agent and perhaps one of the most important factors that tend to create influence in the life of most Nigerians, utilization of the clergy could therefore turn out to be the governments greatest asset in its cybersecurity awareness campaign.

Acknowledgement

Glory be to Allah SWT, whose eternal mercy had enabled me to accomplish this project. I would like to express my profound gratitude to my distinguished supervisor, Col Marcelo Gomes. Beside my supervisor, I would like to extend my deepest gratitude to my country for giving the opportunity to be a part of BASSIC 2019. I also want to thank my family for the unending support, my instructors for their guidance and colleagues for their great assistance.

References

ADEDINI, S. A. et al. Role of religious leaders in promoting contraceptive use in Nigeria: Evidence from the Nigerian Urban reproductive health initiative. **Global Health Science and Practice**, [Baltimore], v. 6, n. 3, p. 500-514, 2018.

AJA, V. T. The relevance of patients' spiritual care in the Nigerian cultural context: a health care chaplain's perspective. **The Journal of Pastoral Care & Counseling:** JPCC, [Thousand Oaks], v. 73, n. 2, p. 82-87, 2019.

AJZEN, I. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. **Journal of Applied Social Psychology**, [S. l.], v. 32, n. 4, p. 665-683, Apr 2002.

AKIYODE-LAWANSON, J. Cybercrime: Nigeria ranks 3rd most attacked country in Africa. **BusinessDay**, Lagos, Nigeria, Mar 9, 2019. Available at: https://businessday.ng/technology/article/cybercrime-nigeria-ranks-3rd-most-attacked-country-in-africa/. Access on: Sep. 21, 2019.

ARANSIOLA, J. O.; ASINDEMADE, S. O. Understanding cybercrime perpetrators and the strategies they employ in Nigeria. **Cyberpsychology, Behavior, and Social Networking**, [New Rochelle, NY], v. 14, n. 12, p. 759-763, Dec 2011.

BAIDEN, J. **John Baiden, BSc., MBA., M.Sc., (distinction) JD, LL.M (distinction)** 1. [s. d.]. p. 1-14.

BASSIC-RESEARCH. **BrazilWarCollege - Google Drive**. [S. l.: s. n.], 2019. Available at: https://drive.google.com/drive/folders/1LdXeL5f7iCNwCE2xXC9AeEc1HU4PREdR. Access on: Sep. 21, 2019.

BLOOMFIELD, C.; BOMMARITO, R. K.; KUHL, M. **Supporting military families through research and outreach public awareness campaigns**. In: SEMANTIC SCHOLAR. [S. l.]: Allen Institute for Al, July 2015. Available at: https://pdfs.semanticscholar.org/7432/6da820ae48d452f08754e8b7d3cef0de969d.pdf. Access on: June 6, 2020.

CENTRAL BANK OF NIGERIA. **Cash-less Nigeria**. Abuja: Central Bank of Nigeria, 2019. Available at: https://www.cbn.gov.ng/cashless/#targetText=The Central Bank of Nigeria,N3%2C000%2C000 for Corporate bodies. Access on: Sep. 21, 2019.

CENTRE FOR CYBERSPACE STUDIES. **Keffi, Nigeria: CCS-NUSUK**, 2019. Available at: https://www.ccs-nsuk.net/. Access on: Sep. 21, 2019.

CYBER SECURITY EXPERTS ASSOCIATION OF NIGERIA. **Lagos, Nigeria: CSEAN**, 2019. Available at: https://csean.org.ng/. Access on: Sep. 21, 2019.

DAHIR, A. L. Cybercrime is costing Africa's business billions. **QuartzAfrica**, [S. l.], June 2018. Available at: https://qz.com/africa/1303532/cybercrime-costs-businesses-in-kenya-south-africa-nigeria-billions/. Access on: Sep. 21, 2019.

DIGITAL PEERS INTERNATIONAL. **Programs**. Abuja, Nigeria: Digital Peers International, 2019. Available at: http://www.digitalpeers.org/programs.html. Access on: Sep. 21, 2019.

FARIVAR, M. How dozens of nigerian scammers stole millions from people, businesses.**Voice of America**, [S. l.], Aug 24, 2019. Available at: https://www.voanews.com/usa/how-dozens-nigerian-scammers-stole-millions-people-businesses. Access on: Sep. 21, 2019.

HARE, F. The cyber threat to national security: why can't we agree?. In: CZOSSECK, C.; PODINS, K. (ed.). **Conference on cyber conflict:** proceedings 2010. Tallinn, Estonia: CCD COE Publications, 2010. Available at: https://ccdcoe.org/uploads/2018/10/1_Proceedings2010FullBook.pdf. Access on: June 10, 2020.

HILTS, S. A perspective on cyber security from the Canadian nuclear private sector. In: LEUPRECHT, C.; MACLELLAN, S. **Governing cyber security in Canada, Australia and the United States:** special report. Ontario, Canada: Centre for International Governance Innovation, 2018. p. 19-21.Available at: https://www.cigionline.org/sites/default/files/documents/SERENE-RISCweb.pdf. Access on: Sep. 21, 2019.

INTERNATIONAL CENTRE FOR LEADERSHIP DEVELOPMENT NIGERIA. **Cyber Security Awareness Month in Nigeria**. Abuja: ICLDNG, 2018. Available at: https://icldng.org/cyber- security-awareness-month-ng/. Access on: Sep. 21, 2019.

INTERNET WORLD STATES. **Africa Internet Users, 2019 Population and Facebook Statistics**. [MadiaPradexe]: Miniwatts Marketing Group, 2019. Available at: https://www.internetworldstats.com/stats1.htm. Access on: Sep. 21, 2019.

JOHNSON, S. D; BOWERS, K. J. Opportunity is in the eye of the beholder: the role of publicity in crime prevention. **Criminology Public Policy**, [S. l.], v. 2, n. 3, p. 497-524, July 2003.

KOCH, R.; GOLLING, M. **The cyber decade:** cyber defence at a X-ing point. In: MINÁRIK, T.; JAKSCHIS, R.; LINDSTRÖM, L. (ed.) **10th International Conference on Cyber Conflict:** CyCon X: maximizing effects. Tallinn, Estonia: NATO CCD COE Publications, 2018. p. 159-185, 2018. Available at: https://ccdcoe.org/uploads/2018/10/CyCon_2018_Full_Book.pdf. Access on: June 10, 2020.

LAWANI, L. O.; IYOKE, C. A.; EZEONU, P. O. Contraceptive practice after surgical repair of obstetric fistula in southeast Nigeria. **International Journal of Gynecology and Obstetrics**, [Malden, MA], v. 129, n. 3, p. 256-259, Feb 2015.

LETTER from Africa: the power of religion. **BBC News**, [London], Nov 7, 2014. Available at: https://www.bbc.com/news/world-africa-29692580. Access on: Sep. 21, 2019.

LEWIS, J. **Economic impact of cybercrime – no slowing down**. Washington: Center for Strategic and International Studies (CSIS), Feb 2018. Report. Available at: https://assets.website-files.com/5bd672d1924b9893a632c807/5c171d5e85ed62697a79e351_economic-impact-cybercrime.pdf. Access on: June 10, 2020.

NATIONAL POPULATION COMMISSION; ICF INTERNATIONAL. **Nigeria demographic and health survey 2013**. Abuja: NPC; Rockville, Maryland: ICF International, 2014. Available at: https://dhsprogram.com/pubs/pdf/FR293/FR293.pdf. Access on: June 10, 2020.

NIGERIAN COMMUNICATIONS COMMISSION. **Industry Statistics**. Abuja: NCC, 2019. Available at: https://www.ncc.gov.ng/stakeholder/statistics-reports/industry-overview#view-graphs-tables-6. Access on: Sep. 21, 2019.

NIGERIAN DEFENSE ACADEMY. **Intelligence and cyber security**: academic branch. Kaduna: NDA [201-]. Available at: https://academics.nda.edu.ng/faculties/military-science-and-interdisciplinary- studies/intelligence-and-cyber-security/. Access on: Sep. 21, 2019.

OJONEMI, S. et al. Deficit in religious practice in Nigeria: implications for national development. **Developing Country Studies**, [S. l.], v. 4, n. 4, p. 184-194, 2014. Available at: https://core.ac.uk/download/pdf/234681546.pdf. Access on: June 10, 2021.

OMODUNBI, B. et al. Cybercrimes in Nigeria: analysis, detection and prevention. **FUOYE:** Journal of Engineering and Technology, [Oye Ekiti], v. 1, n. 1, 2016. Available at: https://engineering.fuoye.edu.ng/journal/index.php/engineer/article/view/16. Access on: June 10, 2020.

OSHO, O.; ONOJA, A. D. National cyber security policy and strategy of Nigeria: a qualitative analysis. **International Journal of Cyber Criminology**, [Gujarat], v. 9, n. 1, p. 120-143, Aug 2015. Available at: https://www.cybercrimejournal.com/Osho&Onoja2015vol9issue1.pdf. Access on: June 10, 2021.

PINTER, B. et al. Religion and family planning. **European Journal of Contraception and Reproductive Health Care**, [London], v. 21, n. 6, p. 486-495, Dec 2016.

SERIANU. **Africa cybersecurity report2016**. Kenya: Serianu, 2016. Available at: http://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf. Access on: June 10, 2021.

SCHOOL OF INFORMATION AND COMMUNICATIONS TECHNOLOGY. **Minna, Niger State**: Federal University of Tecnology, c2016. Available at: https://sict.futminna.edu.ng/. Access on: Sep. 21, 2019.

SIOBHAN, G. Fraud ring funnels data from cards to Pakistan. **The Wall Street Journal**, New York, Oct 11, 2018. Available at: https://www.wsj.com/articles/SB122366999999723871. Access on: Sep. 20, 2019.

TADE, O.; ALIYU, I. Social Organization of Internet Fraud among University Undergraduates in Nigeria. **International Journal of Cyber Criminology**, [Gujarat], v. 5, n. 2, p. 860, 2011. Available at: https://www.cybercrimejournal.com/tadealiyui2011julyijcc.pdf. Access on: June 10, 2020

TECH-U. Faculty of natural and applied sciences. Ibadan, Oyo State: **First Technical University**, [201-]. Available at: https://tech-u.edu.ng/faculty-of-natural-and-applied- sciences/#. Access on: Sep. 21, 2019.

TIEMO, P. A.; NELLY, D. B. Efforts in combating cyber crime and criminality in Nigeria. **Information and Knowledge Management**, [S. l.], v. 6, n. 3, p. 23-28, 2016. Available at: https://www.iiste.org/Journals/index.php/IKM/article/view/29271/30060. Access on: June 10, 2020.

TIIRMAA-KLAAR, H. Building national cyber resilience and protecting critical information infrastructure. **Journal of Cyber Policy**, [London], v. 1, n. 1, p. 94-106, 2016.

UNIVESITY OF CALIFORNIA. Institute for Digital Research & Education Statistical Consulting. SPSS. Frequently asked questions. **What does Cronbach's alpha mean?**. Los Angeles: UCLA, [201-]. Available at: https://stats.oarc.ucla.edu/spss/faq/what-does-cronbachs-alpha-mean/. Access on: Sep. 21, 2019.

VERMUELEN, J. Anonymous hacks SA government database. **MyBroadband**, Olifantsfontein, South Africa, Feb 12, 2016. Available at: https://mybroadband.co.za/news/security/155030-anonymous-hacks-sa-government- database.html. Access on: Sep. 21, 2019.

WHAT is Yamane sample calculation?. In: QUORA. [S. l.: s. n., 2017?]. Available at: https://www.quora.com/What-is-Yamane-sample-calculation. Access on: Sep. 21, 2019.