International Journal of Multidisciplinary and Current Educational Research (IJMCER)
ISSN: 2581-7027 ||Volume|| 3 ||Issue|| 1 ||Pages 154-162 ||2021||

The Current State of Cybersecurity Readiness in Nigeria organizations

[1,]Adamu A. Garba, [2,]Aliyu M. Bade
[1,2,]*Department of Computer Science, Yobe State University Damaturu, Nigeria*

ABSTRACT : Cybersecurity knowledge has become essential in today's world as cyberattacks are growing exponentially. This attack comes in different forms. All sectors can be prime targets of any attack, therefore, measures must be in place to minimize the impact of any form of attack. This paper targets to identify the current state of cybersecurity preparedness in Nigeria organization, the preliminary results indicate, cybersecurity is at "maturing stage", The paper proposes an immediate solution to increase cybersecurity awareness through continuous cybersecurity education programs across all domains to serve as an initial phase for increasing the awareness of cybersecurity attacks.

KEYWORDS: cybersecurity, Awareness level, Nigeria, cyberattacks, cybersecurity index.

INTRODUCTION

The emergence of cybersecurity is mature as the transition of the computer, any information that is transmitted through the internet is at risk of getting compromised without the knowledge of the sender. The emergence of cybersecurity is subjected to the advancement of the cyber domain in the 1950s (Tikk-Ringas, 2015). Any information stored in cyber-space is subjected to intrusion, it includes financial, military, government, and individual. Security breaches occur as a result of the new development of either hardware or software. This new device results in new vulnerabilities. (Garba A.A. et al., 2020). Cybersecurity is a method of protecting organization assets, through the identification of threats that can compromise the critical information stored in the organization systems, it also involves the protection, identification, and responding to threats The use of cyber as cyber power as weapon has also been used by the Russian in 1980s when it attaches 400 military computers include the pentagon computers, this resulted to new demission being added to the research of cybersecurity (Dunn Cavelty 2012; Rueter 2011; Taylor et al., 2014). The field of cybersecurity emerged as a result of Robert Morris testing the worlds' network vulnerability in 1980 when he uses a virus he created to test the size of the internet. His work leaves or indicates major loopholes of cybersecurity in the world of the internet (Healy & Grindal, 2013).

The 21century is regarded as the saturation stage of cybersecurity because it provides solid premises for the development of new theories in cybersecurity as the world becomes more connected. Sometimes the world cyber is not only refers to as technology but also a political idea that is cantered in the numerous technologies. Cyberspace has been functioning as a financial marketplace, political background, and also as social scene by utilizing the potential of the sector (Moody et al, 2018: Weishaupl, et al., 2018). Today, the world is so connected that a person from one continent can see or video chat with another person in another continent, also people connect to the internet using their phones, computers, cars, etc., even employees come to connect with the outside world as their workplaces. Some organizational operations are performed remotely nowadays as contractors or stakeholders can communicate a thousand miles away from the location of the company. All these are possible and it makes life more easy and enjoyable but at the same time if there is no control over the devices the infrastructure of the workplace is in danger of any cyber-attacks. People now connect to public Wi-Fi to do their business anytime and a huge amount of personal data are being processed over the unprotected medium. The organization is most vulnerable to cybersecurity attacks because employees can compromise the network of the organization through the connection to the internet. According to Langer (2017). Stated that organizations are required to adopt an optimized security measure that works within and outside the network to protect their sensitive information. Also, the organization needs sophisticated machines to detect infrequent behaviors' from employees and security levels that protect all access points or control the access point (Taylor et al., 2014).

The existing communications channels or mediums mostly use are not that secure as well thought, therefore, extra measures are required by any organization to protects their information, and also employees' behavioral patterns bust be monitored as well. Cybersecurity has become a necessity for all to learn the basic tricks on how to protect their personal information (Garba et al., 2020). This paper aims to identify how readiness Nigeria is

when it comes to cybersecurity and the current world cybersecurity index. This paper is further subdivided into the following: section II as an evolution of cybersecurity, Section III Worldwide Index in Cybersecurity, Section IV as Existing Research in the field of Cybersecurity in Nigeria, Section V Commonly Cyber-Attacks on Organizations, section VI as Nigeria Main Cybersecurity Issue Reports and finally Section VII as Conclusion.

EVOLUTION OF CYBERSECURITY

Cybersecurity has undergone profound changes in recent years, huge investment has been putting in place to see how to strengthening security to ensure that the organization's sensitive information, data, and other assets are properly secured. Initially, in the 1980s and the beginning of the 1990s security is highly focused on protecting users' computers and operating systems, it focuses on protecting the devices against malicious code or viruses which can affect the working of the computer. After the emergence of the internet, organizations' enterprises started to work on how to secure network connectivity. The idea of being connected makes the emergence of many vulnerabilities that could be misused by an attacker. An attacker aims to access vital information via a site or system or channel where no one had thought of protecting to reach or infect a system through the use of malware or any other mechanisms. This attacker can attack individuals, organizations, state, and a nation just to get access to critical information using a sophisticated method or by buying a program on the deep web for the exploitation of vulnerabilities to obtain that information. Many organizations have tried to protect their information using technological approaches as Peppard &Ward (2016) states, those technologies are as follows:

- **Intrusion Detection System (IDS):** these systems are used to monitor and detect accesses that are not allowed in a network (Effendy et al., 2017)

- **Intrusion Prevention System (IPS):** these systems are used to monitor traffic to detect attack vectors in a network by blocking them. Honeypot is the best example, where venerable computers that do not have critical information are designed to attract and detect attackers (Jin et al., 2013)

- **Security Information in Event Management (SIEM):** this system is used for event correlation and alert generation, by integrating different devices, launching actions according to the set alerts, and keeping the record for further analysis.

There are always new attackers' vectors, therefore organizations must make a concept to protect their assets as information security evolves. Organizations must invest in information security so that to have security policies designed and integrated into the strategic plans of the organization's operations (Moody et al., 2018).
Organizations should always understand or know how much their critical assets worth, business processes, and the kind of likely security breaches that could lead to an attack. Threats cannot be stopped but rather be minimize, therefore the organization must know the state of all their security stand at all times to know how to minimize it to bring it to a residual level. Moreover, the organization must define and integrate security policies into strategic plans, a risk to critical assets must be quantified, and business continuity must be identified in the event of an attack as well as disaster recovery plans. Today, there are major four threats identified to cyberspace, According to Tagarev and Stoianov, (2017). Which are

- Threats to people's assets
- Threats to organization assets
- Threats to virtual goods
- Threats to infrastructures

Computer networks developed in the 1960s by the Agency of Research and Advanced Project (ARPA) and the evolution of the third generation of computers in 1965 made the computer more compatible and popular when the internet is developed during the ARPA project interconnecting large computers in the US, from there the knowledge of the internet get popular. In the 1980s, due to the complexity of the computer, the UK government created a best practice model for information management which is the Information Technology Infrastructure Library (ITIL), subsequently, HP company adopted the best practice and made it popular, in 1995, the term computer security become popular as the US release control of the internet act and by 1997 Charles Plefeer generated a classification of information security properties, which are Confidentiality, Integrity, and Availability (C.I.A). The beginning of policies and standard designs started from 2005 when the ISO/IEC 27000 family of the standard was created for the information security management system, followed by the International Telecommunication Union of the US generated the ITU-T X.1205 standard as Data Networks for Communication of Open System and Telecommunications Security in 2008 and many others follow like the ISO/IEC 27032 in 2012. These standards make it easy by providing an overview of cybersecurity defined as a

set of tools, policies, security concepts, security safeguards, guides, risk management, action, best practices, and technology that can be used to protect the assets of an organization and also the use of cyberspace. The growing recognition of the internet as one of the basic infrastructures for economic and social development in many organizations has made researchers focus on how to deals with this emerging technology. Cybersecurity is more technical perceptions that cover the challenges of securing the organizational infrastructures by offering a solution to the internet security problems, routing, system authentications, and DNS (Denardis & Raymond, 2013). According to Dunn, (2016), stated that most academic production in the discipline can be divided into the following groups' Formulation of policies, generally in the field of the "think- tanks". Studies focused on the relationship between information and power (Day, 2001) Production of insecurity on the internet on the internet based on surveillance practice and censorship (Deibert and Rohozinki, 2010) Studies on the creating of threats in cyberspace (Hansen & Nissenbaum 2009). Recently, attention has been given to the link between internet governance and cybersecurity, because cybersecurity problems have challenged internet governance institutions like jurisdictional conflicts (Mueller & Klein, 2014). Therefore, it is important to establish the link between cybersecurity and the level of awareness regarding it, firstly, are there any policies or strategies regarding cybersecurity and cyber law in Nigeria, this is a good starting point so that it will help the researcher to find out their such documents exist and are familiar to all organizations in the country.

WORLDWIDE INDEX IN CYBERSECURITY

Global cybersecurity index 2017 conducted a survey in Africa reign and 29 states responded out of 44 member states, the survey is meant to see how African states are in terms of controlling cyber Security in their states. Here only West African states are extracted from the survey, in the survey five aspects are involved; legal, technical, organizational, capacity building, and cooperation as a domain. Each domain has some criteria as shown below.

Table 1.1 Worldwide Cybersecurity Index Domain source (Global Cybersecurity Index, 2017).

S/N	Legal Measures	Technical Measures	Organizational Measures	Capacity Building	Cooperation
1	Cybercriminal legislation	National CERT/CIRT/ CSIRT	Strategy	Standardization bodies	Bilateral agreements
2	Cyber Security legislation	Government CERT/CIRT/ CSIRT	Responsible agency	Cybersecurity good practices	Multilateral agreements
3	Cyber Security training	Sectoral CERT/CIRT/ CSIRT	Cybersecurity metrics.	R&D programs	International participation
		Standards for organizations		Public awareness campaigns	Public-private partnerships
		Standards for professionals		Professional training courses	Interagency partnership
		Child online protection		Education programs	
				Incentive mechanisms	
				Home-grown industry	

Table 1.2: West African States Cybersecurity Criteria Measurement source (Global Cybersecurity Index, 2017)

West Africa	Cybercriminal Legislation	Cybersecurity Legislation	Cybersecurity Training	Legal Measures	National Cert/Cirt/Csirt	Government Cert/Cirt/Csirt	Sectoral Cert/Cirt/Csirt	Standards For Organizations	Standards For Professionals	Child Online Protection	Technical Measures	Strategy	Responsible Agency	Cybersecurity Metrics	Organizational Measures	Standardization Bodies	Cybersecurity Good Practices	R&D Programs	Public Awareness Campaigns	Professional Training Courses	Education Programs	Incentive Mechanisms	Home-Grown Industry	Capacity Building	Bilateral Agreements	Multilateral Agreements	International Participation	Public-Private Partnerships	Interagency Partnerships	Cooperation	Gc1
Benin	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	1
Burkina Faso	1	1	1	1	1	1	1	3	1	1	1	1	1	1	2	2	3	1	1	2	1	1	1	1	1	1	3	1	1	1	1
Cabo Verde	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	1
Côte d'Ivoire	2	3	3	3	1	3	1	1	1	3	2	1	3	1	2	2	3	1	3	3	2	1	2	2	2	1	3	1	1	2	2
Gambia	3	2	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	1
Ghana	3	2	1	2	3	3	3	1	1	3	2	3	2	1	2	1	1	1	2	1	1	1	1	1	1	1	3	1	1	1	2
Guinea	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	1
Guinea-Bissau	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	1
Liberia	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	3	2	1	2	1
Mali	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	1
Mauritania	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Niger	2	2	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	3	3	1	1	3	1
Nigeria	3	3	1	3	3	3	1	3	3	3	3	3	3	1	3	3	1	2	3	3	2	2	1	2	3	3	3	2	3	3	3
Togo	1	1	3	2	1	1	1	1	1	1	1	1	2	2	2	1	1	1	1	3	1	1	1	1	1	1	3	1	1	1	1
Senegal	2	3	2	2	1	1	1	1	3	1	1	1	1	1	1	1	1	1	2	3	2	2	1	1	3	3	3	1	1	3	2
Sierra Leone	1	1	1	1	1	1	3	3	1	2	2	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	1

The above criteria are used in table 2.2 is to measure how Africa is ready in dealing with cybercrimes, an average scoreline is formed were (3 = high, 2= medium, and 1 = low) in other to see in which part more action is needed. The above table 2.2 summarizes both strength and weakness of West African states in terms of cyber Security measure, according to the Global cybersecurity index 2017, only Nigeria scored the highest but with some components scoring low and medium as shown in the GCI column (3), also components like Cybercriminal legislation, Sectoral CERT/CIRT/CSIRT Cybersecurity metrics, Cybersecurity good practices, R&D programs, Education programs, Home-grown industry, Capacity Building, and Public-private partnerships need to be improved to compete with other countries that scored the highest across all components and domain like Europe. Lastly, Nigeria is placed fifth in Africa. Based on the report Nigeria's cyber-security programs and initiatives are in the ***"maturing stage***", which means that the GCI score of Nigeria is between the 50th and 89th percentage globally (Global Cybersecurity Index, 2017).

EXISTING RESEARCH IN THE FIELD OF CYBERSECURITY IN NIGERIA

The growth of the internet has allowed for the development of technical structures, cyberspace has been part of everyday life and therefore information technology has become an essential factor for advancement. Cybersecurity is nowadays a concern to companies due to the continuous breaches which result in the theft of data and destroying critical assets (Johnson, 2016). These attacks can cripple the financial institution and the economy as well. Africa is growing in consumer credits, but lack of data protection serves as a major problem (Makulilo, 2016). Out of 54 or 55 countries as African Union recognizes 55 while the UN recognizes 54, only 16 countries have data protection and the most unfortunate Nigeria is not one of those countries and also Nigeria is part of the top 10 leading countries in the world leading in reported cybercrimes. Cybercrime refers to any unlawful activity by using the internet as means and additionally any illegal activity that uses a computer to gain improper benefits. Cybercrimes have long lowered the reputation of Nigerians worldwide (Ibikunle & Eweniyi, 2013) these threats have increased exponentially as the dramatic rise of mobile communication, the drive of the banks in the country to introduce careless economy, using internet technology in the government and online trade.

According to Andoh et al., (2014), they suggested that elected and state governments, the public organization well as privates all have parts to play through the enactment, the reception of international standards, creating awareness, and information and intrusion crusade in other to deal with cyber threats and ensure zero resilience in the misuse of the internet. Right now, the most used cybercrime that goes unchecked is electronic fraud where is equipped for taking all individual or cooperate bank account and sent a wrong flag against the monetarily related incorporate drive (Orji, 2012). The word "419" is associated with Nigerian Computer Advanced Fee Fraud. The CBD recent introducing of Bank Verification Number (BVN), to reduce the number of account individual or organization can manage, and the creation of the Nigerian Electronic Fraud Forum, Nigerian Interbank Settlement System (NBISS), and Deposit Money Banks(DBM) all in the name of protecting customers financial transactions, but scammers turn out to be faster in reaching their goals by defrauding the clueless customer of banks and other financial instruction in the country billions of naira. A critical part of cybersecurity is communication, which is lacking in Nigerian organizations. the power of cybercrime hacking networks depends on their need to share privileged data by exposing or selling to organizational rivals who restrict correspondence with their companies due to fear of rivalry. The next section will explain more on the issues reported regarding cybercrime activities and how much losses they cost to both government and organizations.

COMMONLY CYBER-ATTACKS ON ORGANIZATIONS

According to Korte, (2017), $500 billion was lost annually by cybercrime and the numbers keep on increasing as institutions continue to adopt the internet in carrying their business processes. The most wieldy attacks are the return of Ransomware, According to Wueest, (2017): Richardson and North, (2017), states that Ransomware is a style of cyber-attack that is known as information hijacking, where the attacker uses a code to get access to the organization's server and then demand a payment to give access back to the data if payment is not made the attacker destroyed the data or sell it online. Other attacks include Advanced Persistent threats. Nigerian financial organizations have used these chances to grow their e-business through the use of the internet and mobile applications, which has also lead to an increase in cybercrimes. The most recent cybercrime using mobile devices in Nigeria is the SMS sim splitting or swapping technique, where a hacker takes over users' identity after gaining access to their cell phones. The hacker then downloads financial applications and log in using stolen credentials through a social engineering approach.

The following attacks mostly are aimed at the customers especially those that have less knowledge of the cyber world or the financial institutions with sole to sell or distrust transactions.

- **Viruses**: A virus is a malicious program that is designed to infect other files on the system to change or make them useless, for this virus to work the user must activate it by clicking on the file, some of its purposes include: getting the password, deleting all computer files and denial of service attack.

- **Malware**: Malware is a malicious code designed, where it is installed and executes without the knowledge of the owner. The most common usage of this attack is to get personal data and electronic benefits, it can be operated automatically or remotely control.

- **Worm**: the worm is a malicious program that can replicate itself and can spread over a network. The worm has the same agenda as the virus

- **Trojan**: A Trojan is a small hidden program in another program. The program gets installed by the user without noticing it and it can perform various activities without the consent of the user (Aliyu, et al, 2014).

- **Browser Hijacker**: Browser Hijacker is a program that is designed to make changes to the configuration of the web browser e.g. changing the normal home page of a website to an advertising page

- **Dialer:** Dialer is a hidden program designed to connect to the internet through a modem thereby allowing the hacker to make calls to phones at a special rate.

- **Backdoor**: backdoor is a program whose main intention is to open computer access to the malware developer, ignoring the main or genuine process of authentication. The program makes it easier for the attacker to control the attacked device remotely

- **Spyware**: spyware is an application designed purposely to collect personal or organizational data. This application aims to get information and sell it to a third party

- **Keylogger**: Keylogger is an application that is used to store all keystrokes so that hackers can capture sensitive information like banking details or passwords.

- **Masquerading**: Masquerading is a cyber-attack where a hacker overrides the identity of any system to gain access to the resource stored in the system. An attacker can impersonate a base station network by emitting a signal of more power than the actual legitimate user.

- **Denial of service / Distribute Denial of Service(Dos/DDoS):** Dos/DDoS is one of the most used cyber-attacks, in this attack the hacker or attacker makes network service unreachable or unavailable to the legitimate users, or service interruption. This attack mostly is used to attack financial organizations, airlines, and other reputable organizations. This attack makes a normal site temporary out of service by sending many requests to the server, which makes it busy, zombies' term is used where a non-stop request is sent to the server and makes other systems act like zombies.

- **Phishing**: Phishing is used by an attacker to deceiving the user to provide their access keys to a malicious site, thinking is a legitimate site. According to Miedema (2018) stated that phishing is a much more elaborate attack and is often exposed as a clear example of so-called social engineering.

- **Eavesdropping**: Eavesdropping is an attack where the attacker obtains information from the communication channel, where he is neither the emitter nor the receiver. It is referred to as a passive attack. The information obtained can be used to perform another attack called masquerading. The above-explained attacks are not the only cyber-attacks, but those are the most frequently used by most attackers in attacking financial organizations and also other organizations as well. Even though organizations may focus on protecting their networks and critical assets, employees or customers especially financial institutions are being left out of the loop or often neglected unknowingly they might be the weakest link to the organization networks. Today as everything mostly depends on the internet it is therefore responsible for everyone to try to protect their data, organizations need to educate consumers and employees about the risk and the measure they can take to protect their personal information and to be familiar with the recent cyber-attacks.

NIGERIA MAIN CYBERSECURITY ISSUE REPORTS

Based on the Nigeria n cyber Security report 2016 by Serianu agency, Nigeria has a total number of 97,210,000 internet users and subscribers as of 2016 with the increase of users' cyber threats and attacks also increases, the estimated cost of cybercrime is $550M and with less than 1550 estimated No. of Certified professionals and 122,292,079 i.e. 60.9% as of June 2019 is the top 6 countries in top 20 internet users in the world (Internet World Stats, 2019). Among the top 5 priorities from 2016 regarding cyber Security challenges in Nigeria are: Awareness and training, continuous monitoring and log analysis, vulnerability and patch management, continuous risk assessment and treatment, and managed service, and independent review (Serianu, 2016). Besides, among the top 10 Africa's cybersecurity challenges in 2018 is lack of Employee Security awareness as the survey shows, were Over 300 respondents across organizations in Africa precisely in Nigeria participated in the survey which includes: academic, government, banking, healthcare, cybersecurity service sector, financial services, legal advisory, telecommunication, private sector. based on the survey many expert answers similar to a particular question.

Table 1.3 Nigerian Cybersecurity Issue Survey Result

Name	Question	Respond
Aashiq Shariff Tanzania 2017 Raha –Liquid telecom Ltd, CEO.	what should African countries/ universities focus on to inspire innovation in the development of cybersecurity solution	Conduct the awareness and ready with a solution, the solution depends on the organization
	In African what are the top 2018 cybersecurity priorities for African countries and organization	Awareness and information sharing. Also collaboration between government and private companies in addressing cybersecurity issues
Henry Kaya Uganda 2017 Assistant Commissioner of Cyber Security Unit	What would be the top priority to address cybercrime across the African continent?	Public and private organization to intensify awareness campaigns, also investment should be increased in securing IT system
John Ayora Senegal 2017 Director, Information Systems Security, Bank of Africa Group	what are the top 2018 cybersecurity priorities for African countries and organization	Invest in user training and awareness programs, also invest in effective cybersecurity product and solution
Brady S Senegal 2017 Associate Director, Digital transformation and cybersecurity led by Finetech Groupe (Senegal)	Considering the shortage of skilled resources in Africa, How can we limit the impact of the Ransomware case	Investing more in raising awareness and training end-user who is, as always the weakest link of the chain.
	from the African context, what are the top 2018 cybersecurity priorities for African countries and organization	Set up a national CERT. Awareness and training

From the above table 1.3. it shows some response of security experts, the almost same question was ask regarding the best approach to tackle or minimize cyber Security issue from an African point of view and up to Nigeria n context, from the above responds its shows almost 95% of the respondents have the opinion that: Awareness training is the main driving force that will make everyone familiar with the issues and danger of cyber-attacks to their companies. Some respondents also have the view of an increase in budget to IT so technical measures will be included too. Respondents from Nigeria in context also have the opinion that the best approach in dealing with cybersecurity issue in Nigeria is ***"Education and awareness is the best approach, once a common man is aware of this, he will be careful***." from this, we will see that the first step in dealing

with cyber Security is by educating both public and private personal on the danger of cyber-attacks, before applying any technical measures, because if only technical is visible if the knowledge of cyber-attacks are limited then the user themself will pose a threat to the organizational asset. Therefore, according to Ben Robbert the Chief Technical Officer, Liquid Telecom Group, Kenya says in responding to the question what are the top 2018 cybersecurity priorities for African countries and organizations he answered "My top3 priorities are education, education, and education. All organization needs to make sure all employees are aware of cybersecurity risk. Many organizations are vulnerable to cybersecurity attacks because students might compromise the network of the university by connecting to the internet(Garba et al., 2020).

CONCLUSION

In conclusion, from the above literature, it indicated how cybersecurity knowledge is essential in all aspect of life, precisely in Nigeria from the above opinions by various experts in the field, its shows that Nigeria has policy and strategy to combat cyber Security but most organization are not following it, due to lack of proper awareness to the employees on the issue of a cybersecurity threat, also the general public as a whole are less or have no knowledge on the dangers of cyber-attacks and tend to ignore it. This research also indicated the way forward is "education on cybersecurity" i.e. proactive cybersecurity awareness programs are needed to be implemented all over the section to increase the awareness level and minimize basic cybersecurity attacks.

.

REFERENCES

1. Tikk-Ringas, E. (2015). Evolution of the Cyber Domain: The Implications for National and Global Security. IISS Publications.
2. Dunn Cavelty, M. (2012). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. (n.d). Science and Engineering Ethics, 20(3), 701-715.
3. Garba, A. A., Siraj, M. M., Othman, S. H., & Musa, M. A. A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach.
4. Rueter, N. (2011). The Cybersecurity Dilemma. MA thesis. Duke University
5. Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). Digital Crime and Digital Terrorism. Prentice-Hall Press.
6. Healey, J. & Grindal, K. (Eds.). (2013). A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Washington, DC: Cyber Conflict Studies Association. 77
7. Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. MIS Quarterly, 42(1), 285-A22.
8. Weishaupl, E., Yasasin, E., & Schryen, G. (2018). Information Security Investments: AnExploratory Multiple Case Study on Decision-Making, Evaluation, And Learning.Computers & Security,
9. Langer, S. (2017). Cyber-Security Issues in Healthcare Information Technology. Journal ofDigital Imaging, 30(1), 117-125. DOI:10.1007/s10278-016-9913-x
10. Effendy, D. A., Kusrini, K., Sudarmawan, S. (2017). Classification of Intrusion Detection System (IDS) Based on Computer Network. 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE
11. Jin, H., Xiang, G., Zou, D., Wu, S., Zhao, F., Li, M., & Zheng, W. (2013). A VMM-BasedIntrusion Prevention System in Cloud Computing Environment. Journal of Supercomputing, 66(3), 1133-1151. DOI:10.1007/s11227-011-0608-2
12. Tagarev, T., Sharkov, G., & Stoianov, N. (2017). Cyber Security and Resilience of Modern Societies: A Research Management Architecture. Information & Security, 38(1), 93-108.doi:10.11610/isij.3807
13. International Organization for Standardization (ISO (2012). ISO/IEC 27032:2012 – Information Technology – Security Techniques – Guidelines for Cybersecurity
14. Denardis, D. & Raymond, M. (2013). Thinking Clearly about Multistakeholder Internet Governance. Eighth Annual GigaNet Symposium.
15. Day, R. E. (2001). The Modern Invention of Information: Discourse, History, and Power. Carbondale: Southern Illinois University Press.
16. Deibert, R. J. & Rohozinski, R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security. International Political Sociology: 15-32.
17. Hansen, L. & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and CopenhagenSchool. International Studies Quarterly: 1155–1175.
18. Mueller, M. & Klein, H. (2014). Sovereignty, National Security, and Internet Governance: Proceedings of a Workshop. Syracuse University: Georgia Institute of Technology School of Public Policy.

19. Global Cybersecurity Index, (2017) Global Cyber Ranking, retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
20. Johnson, K. N. (2016). Managing Cyber Risks. Georgia Law Review, 50(2), 547-592.
21. Makulilo, A. B. (2016). The Right to Privacy Relating to Credit Reporting: A Critical Review of The Emerging Africa's Credit Reference Market. Journal of Internet Law, 19(9), 3-17.
22. Ibikunle, F. & Eweniyi, O. (2013). Approach to Cyber Security Issues in Nigeria: Challenges and Solution. International Journal of Cognitive Research in Science, Engineering and Education:(IJCRSEE), 1(1), 100-110.
23. Andoh-Baidoo, F., Osatuyi, B., & Kunene, K. N. (2014). Architecture for Managing Knowledge on Cybersecurity in Sub-Saharan Africa. Information Technology for Development, 20(2), 140-164.doi:10.1080/02681102.2013.832127
24. Orji, U. J. (2012). Cybersecurity Law and Regulation (pp. 398-400). Wolf Legal Publishers
25. Korte, J. (2017). Mitigating Cyber Risks Through Information Sharing. Journal of Payments Strategy & Systems, 11(3), 203-214.
26. Wueest, C. (2016). Financial Threats 2015. Retrieved from Symantec: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/financial-threats-2015. pdf.
27. Richardson, R. & North, M. (2017). Ransomware: Evolution, Mitigation, and Prevention.International Management Review, 13(1), 10-21.
28. Miedema, T. E. (2018). Engaging Consumers in Cyber Security. Journal of Internet Law, 21(8), 3-15.
29. Internet world stats, (2019), Countries with Highest Number of Internet Users, retrieved from https://www.internetworldstats.com/top20.htm
30. Serianu, (2016), Nigerian Cybersecurity report, Retrieve from http://www.serianu.com
31. Aliyu, A., Danjuma, S., Dai, B., Waziri, U., & Ado, A (2014). An Integrated Framework for Detecting and Prevention of Trojan Horse (BINGHE) in a Client-Server Network. 3(1), 2319-8753.
32. Garba, A. A., Siraj, M. M., & Othman, S. H. An Explanatory Review on Cybersecurity Capability Maturity Models.
33. Gabra, A. A., Sirat, M. B., Hajar, S., & Dauda, I. B. (2020). Cyber Security Awareness Among University Students: A Case Study.