CYBER SECURITY AND ITS IMPLICATION ON LIBRARY USERS' PRIVACY

YUSUF, Rukayat Abimbola (CLN)
Law Library, Adekunle Ajasin University, Akungba-Akoko, Ondo State.
bimruk@gmail.com, rukayatyusuf@yahoo.com

AWOYEMI, Olubunmi O. PhD (CLN)
Law Library, Ekiti State University, Ado-Ekiti,
wumibunmi@gmail.com, olubunmi.awoyemi@eksu.edu.ng

ABSTRACT

It is an undisputed fact that technology advancement has reached a stage that hardly can an individual do away with internet connected devices, or totally abstain from services offered by way of internet connection. From financial services, military and defence, to regular stock purchases, to complex transactions, even for medical and health services; internet of things (IoT) has changed the way the world operates. In all these, the library is not left out. The attendant evil associated with this internet advancement is the threats, attacks and crimes committed in the cyberspace. The near invisibility of individual contact has made cyberattacks a daunting crime to fight. However, technology advancement that brought into being the cyberspace with its attendant insecurities is also running a rat race keeping up with addressing and making tools and products that can provide security in the cyber space. Different solutions are being regularly proffered, examples like two-step verification, running anti-virus programs, setting up firewalls, and many more as discussed in the body of this paper. This paper reviews the issue of invasion of privacy of users by security measures put in place to guide against cyber-attacks, the ethical implication in respect to the library. The article concludes by suggesting and identifying ways in which the library can safeguard users' data while employing cyber security measures

.

Keywords: Cyber security, Cyber-attacks, Privacy, Library, Users' data, Nigeria

INTRODUCTION

The term "cyberspace" has been attributed to William Gibson in 1982 though the concept of cyberspace became popular in the 1990s in the advent of the world wide web (www) (Lippert & Robert, 2021). The term "Cyberspace" has no general definition; the definition by Lippert and Robert (2021) describing it as a global domain within the information environment consisting of a network of information technology infrastructures, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers accommodating reference to objects and identities that exist within it, is more encompassing. The definition encompasses similar description by other authors (Craigen,Diakum-Thibault & Purse,2014; CSRC, n.d; Injac & Sendelj, 2016). Simply, the cyber space is a virtual space that supports and allows online communication. The cyberspace has been said to be in three layers: the physical layer which includes the geographical component and the physical network component, the logical layer which consists the logical network component, and the social layer which consists of the cyber persona and the persona components (AcqNotes, 2021). Cyberspace has been made more popular with social media and cloud computing.

Technology advancement has reached a stage that hardly can an individual do away with internet connected devices, or totally abstain from services offered by way of internet connection. From financial services (Chassidim, Perentis, Toch & Lepri, 2020), military and defence, to regular stock purchases, to complex transactions, even for medical and health services; internet of things (IoT) has changed the way the world operates (Adakawa, Al-Hassan & Auyo, 2020 citing Raytheon, Forcepoint and the National Cyber Security Alliance 2017). The library is not left out in the list. Libraries have moved online and adopted virtual space to ease library management, usage and services to users (Nicholas-Rocca & Burkhard, 2019, Zia, Theseen & Kathane, 2020). The attendant evil associated with this internet advancement is the threats, attacks and crimes committed in the cyberspace. The near invisibility of individual contact has made cyberattacks a daunting crime to fight. However, technology advancement that brought into being the cyberspace with its attendant insecurities is also running a rat race keeping up with addressing and making tools and products that can provide security in the cyber space, at a time where nearly everything is internet enabled or connected, it is daunting to be able to keep one's personal data or information away from cyberspace.

The virtual world is the present world and this has advanced how things are done now as compared to the early times of computer technology (The Open University, n.d.). Each and every webpage visited is noted and archived somewhere; such that one can only imagine the extent of personal imprint that we leave in the cyberspace (Kaur, 2020). This resonates with the reasoning of Adakawa, Al-Hassan and Auyo (2020) quoting Farley (2015) that the information needs and seeking behaviour of users is a major factor in the issue of cybersecurity and that addressing it requires a study of individuals' information seeking behaviour.

The Library and Cyberspace

The library is a custodian of diverse and multiple sources of information. Before the advent of computers, information technology, the library was primarily a storehouse of books and manuscripts though with a structured and organised collection. The growth to books and manuscripts came after the early ages when information were primarily in carvings, parchments, scrolls, pictorials and the likes. However, with the advent of computers came data/information stored on disks, CD-ROMs, microfilms, etc. With the advancement in technology came advancement in medium of information resources found in the library (Candela, Castelli, & Panago, 2011, Abo-Seada, 2019). The library grew from manually carrying out routines to automated services; to escape the toil of repeatedly performing jobs manually and enhance efficiency of library service delivery (Shabana, Saleem & Batcha, 2013). The library grew from being automated to going digital; the possibility of the library going digital translates to it being able to hold more information resources without having to seek larger physical spaces. Electronic resources, digital collections and digital services became the way to go (Emmanuel & Anele, 2018).

Twenty-first century ICT compliant libraries now have a digital presence, with real-time services rendered to users/patrons. Nearly all services that take place in the physical library can be accessed online: registration of users, access to library catalogue, charging and discharging book loans, current awareness services, reference services, even reading the information materials (Candela, Castelli & Panago, 2011). The virtual space brought ease to library usage and library management (Zia, Theseen & Kathane, 2020, Candela, Castelli & Panago, 2011). Information management has moved from the computer network-based to cloud computing. With the development comes greater risk of threats and risks associated with the cyberspace. The library must seek to prevent a breach into its systems and networks, users' data must be protected against unauthorised access and use (Adakawa, Al-Hassan & Auyo, 2020).

WHAT IS CYBER SECURITY THREAT OR CYBERCRIME?

What is cyber security?

Cyber Security is also called information technology security though some authors (Solms & Niekerk, 2013; Analytics India, 2020) have argued that it is different from information technology security in that it does not deal specifically with the information at all times as when the attack is targeted not to access data, but to for instance sabotage or disrupt the online activities or network of the target, or a case of cyber bullying which though cause harm to the individual user, it does not corrode or compromise loss of confidentiality or integrity of the information on the computer network. Information security is created to cover three objectives of confidentiality, integrity and availability, while cyber security is meant to protect attacks in cyberspace (Analytics India, 2020).

According to Seeman, Nnadhunu and Sowmiya (2018), cyber security is when the cyber environment of the individual, company, institution or organisation is being protected by internet-connected systems, including hardware, software and data, from cyber-attacks. While this mostly is the case, a computer not presently internet-connected may be subject to cyberattacks of malicious applications like the Trojan from an external drive or device that is already corrupted with the virus, been used on the internet-disabled computer. Injac and Sendelj (2016) described cyber security to be the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorised use or modification, or exploitation.

Despite the growth and advancement in technology, cyberattacks and cyber threats keep growing; the list includes network intrusion, dissemination of computer viruses, identity theft, cyber stalking, cyber bullying, cyber terrorism, etc. (Vadza, 2013). It becomes necessary in the realities of these attacks, crimes and other cyber threats for individuals, companies and organisations that access or use internet to have in place security applications or tools that will protect against such attacks or threats or crimes like phishing, malicious applications, web jacking, amongst many others (Bhavsar & Bhavsar, 2017). The converse though is that while this security applications, like anti-virus software, encryption, firewalls, etc. help protect against these cyber threats, attacks and crimes, they likewise tend to invade privacy of users by accessing and collecting a large amount of data (sometimes, sensitive data) about users. Therefore, library and its users need to weigh the benefits and the risks between the security features and the possible privacy invasion when deciding on which protection mechanisms to use.

Cybercrimes/ cyber security threats/ cyber-attacks

Cybercrime is a generic term for any form of illegal activity that uses a computer as its major means of commission (Reddy & Reddy, 2014). They are crimes that have been committed with the use of computers, but this will include other type of network aided devices. It involves an unlawful activity in which computer or computing devices such as smartphones, tablets, Personal Digital Assistants(PDAs), etc. which are stand alone or a part of a network are used as a tool or/and target of criminal activity (Pande, 2017). It is often committed by the people of destructive and criminal mind-set either for revenge, greed or adventure.

According to International Business Machines Corporation (IBM) (n.d.) cyber-attacks are motivated under three major categories: criminal, political or personal. Criminally motivated and/or personally motivated attacks could take the form of an attack for monetary gains or financial remuneration e.g. stealing data or information to sell to criminals or competitors or advertisers usually by a spyware, malware; monitoring or tracking user information using mobile malware, and hijacking or taking control of a system through Trojan virus, Botnet and rootkit, though personal motivation like disgruntled employees will do it mainly for retribution. Politically motivated attacks include espionage and it could also be to seek attention for a cause. Another categorisation by Toch, et al (2018) is made based on the attack vector that is the point at which the attack is targeted. They identified three layers of vulnerability to cyber-attack as: Hardware layer the major goal of which is to be able to gain backdoor access to the computer to access its memory and access sensitive information; network layer that targets the network protocol and the goal of which is often to deny the target service or hijack the network connection so as to be able to steal sensitive data; and application layer which mostly take the form of phishing, targeting such applications like the e-mail. At this level, humans are usually involved to compromise the systems, tricking the individual user/target.

Forms of cybercrimes

These include cyber stalking, phishing, cyber terrorism, forgery and counterfeiting, software piracy, child pornography, computer hacking, computer vandalism, spamming, cross site scripting, online auction fraud, cybersquatting, web jacking, introducing malicious software to the system, etc. Malicious software also known as malwares are common examples of cyber-attack, e.g. worms, Trojan, viruses, adware, spyware, scareware. They are deployed to steal sensitive data, or to disrupt network, or hijack the system network. In all, they are very harmful and cause a lot of damage to the target(s) (Vazda, 2013, ITU Telecommunication Development Bureau, 2012, Ajie, 2019).

The Global Cybersecurity Index (GCI) a specialised agency of the United Nations for information and technology ranked Nigeria 47th out of 182 countries on the GCI for 2020. Nigeria held the fourth position among the African nations indexed (The Punch, 2021). Financial scams are the leading crime in the Cybercrimes in Nigeria. The threat posed by the cyber criminals transcend individuals to societies, to organisations and big corporations, even the government is not left out. An example of recent cyberattack on government institution and big corporation is that of the group of hackers known as “Anonymous” that hacked into some organisations system, and some Federal Government’s system during the ENDSARS protests that occurred in Nigeria in October 2020 (Guardian, 2020). In January 2022, the Nigerian

Communications Commission (NCC) through its division the Computer Security Incident Response Team (CSIRT) alerted telecom users to some types of cyberattack; Juice Jacking that allow attackers to compromise public charging ports or plugs by loading a payload that automatically downloads onto a victim's phone when the compromised plug or port is used, and Facebook for Android Friend Acceptance Vulnerability that targets only android operating system (Nigerian Communications Commission, 2022). Another recently identified cyber-attack involves hackers being able to unlock vehicles using safety measures of remote sensor. The attack identified as a Man-in-the-Middle (MitM) intercepts the radio frequency signal sent from a remote key fob, manipulates it and later employs it to unlock the car at will (Guardian, 2022).

A report of an alleged breach of data of a major scale happened in Nigeria in January 2022 when some hacker was alleged to have broken into the database of the Nigerian Identity Management Commission (NIMC) which report was later debunked by the Commission (NIMC). The possibility of such happening created a major scare in the nation at the time (Guardian, 2022). This portends the grave risk attached to having one's "digital personal profile/dossier" compromised.

CYBER SECURITY IN THE LIBRARY AND USERS' PRIVACY

The purpose of the cyber security measures is to protect data, programs and computer networks from unauthorised access or attacks. Securing the cyberspace accommodates confidentiality and integrity of data that is stored on and is accessed via these technological devices. Reddy and Reddy (2014) listed some cyber security techniques to include: access to control and password, authentication of data, malware scanners, firewalls, and anti-virus software. Also installing updates of applications regularly as they are released helps prevent or guard against attacks (Bhavsar & Bhavsar, 2017). This is because most update are made to address issues like bugs, vulnerability to certain malwares and generally respond to making a better and more secured version of a program or application than the previous version. Library and its users can also adopt a strong and not easy to decipher password to secure their information.

According to Romdhani (2017) while security and privacy are closely related and are often used interchangeably, they actually differ. Privacy according to him deals with persons. It has to do with the control that the person has over the information that he/she discloses in the context of an application and ensuring that the information is not used or disclosed for other purposes or used by other unauthorized entities asides the ones for which it was disclosed by the person/user. Security on the other hand is how the different properties of data is guaranteed. Properties such as confidentiality, integrity and authenticity, availability, nonrepudiation, and access controls.

The issue of security and privacy is more embedded as mobile devices too have become mini-computers capable of user programs and third party software (Clarke, Symes, Saevanee &Furnell, 2016). Mobile devices have become ubiquitous that it is employed in commerce transactions as electronic commerce transactions, in military, in governance and even in health care and medical services (ITU, Organisation Internatinale De La Francophonie and AfricaCert, n.d.). A study about associated threat of invasion of privacy where users' data may become compromised considered autonomous vehicles (AVs) which provide ease and lower human error in vehicle transportation: two risks are identified with it; privacy and cyber security. The study reported that data privacy laws may conflict with the storage and communication of personal data by AVs, so also a compromise of the communication networks employed for the safe operation of AVs is a major cyber security threat (Lim & Taeihagh, 2018). The availability of e-resources in the library necessitated the library to re-adjust the safety measures used in securing its resources.

The information age herald freedom of information. However, freedom of information embeds the right to privacy; which right includes right to open inquiry without outsider's scrutiny. Privacy is being free from outside interference, not having uninvited intrusion. Library information management system is in possession of library users' personally identifiable information; how it deals with these information is a reflection of its data privacy policy and respect for users' right to privacy. Such information procured as a result of registration of users, reference services to users, circulation records, and other records from the usage of library resources, services and facilities, must be maintained under strict confidentiality. According to American Library Association (2019), Article III of the *Code of Ethics of the American Library Association* states that confidentiality extends to "*information sought or received and resources consulted, borrowed, acquired or transmitted,*" including, but not limited to, reference questions and interviews, circulation records, digital transactions and queries, as well as records regarding the use of library resources, services, programs, or facilities. Protection of users' privacy and confidentiality is a fundamental part of the mission and the ethical practices of libraries.

Sometime in 2020 at the height of COVID-19, some libraries not fully in digital space were compelled to transition to quickly, rendering their services online as physical dealings was rendered impossible by the imposition of major lockdowns and observation of physical distancing. At this point, more user data found their way to the digital space in the process of charging and discharging information resource loans, interlibrary loans, and selective dissemination services. Nkamnebe, et al (2015) referenced in Ifijeh and Yusuf (2020), in Nigeria, due to identified challenges like unstable power supply, inadequate funds, inadequate ICT skills of librarians, poor technology infrastructure, lack of support or apathy towards libraries and libraries, the transition to fully digital library services in the wave of COVID-19 era was problematic (Ifijeh & Yusuf, 2020). The University of Lagos, Lagos State, Nigeria in June 2020 made history when it received donation of free cloud based intelligent service robots. The robots one of which was donated to the University library is to be deployed to perform services of taking users' and usage statistics, reference services, organization of library books, amongst others. It was also to take temperature of users entering the library. This innovation of employing artificial intelligence embeds the users' data in addition to data on information resources in the library to be able to perform effectively, efficiently and optimally (University of Lagos, 2020).

However, in the light of the increasingly reliance and presence in cyberspace in all facets of living, some platforms pose greater challenge to organisations, individuals, and institutions, and in particular the library; and are where the cyber criminals are able to perpetrate their activities. These are web servers, cloud computing and its services, mobile security networks, IPv6 (the latest internet protocol) (Reddy & Reddy 2014). This is supported by the report by

Office of Privacy Commissioner of Canada (2014) that cyberspace has become increasingly difficult to manage. The complexity of the environment, more volumes of data involved in the constant online presence that is fallout of the internet of things (IoT), third party business dealings, and many more poses more challenge to cyber security and users' privacy. The technology that makes these activities possible also opens up the users to detailed monitoring where users' data can be captured, modified, shared and generally put to such use outside the purpose for which users entered the details; and without an informed consent of the user. These very possibilities for wide-ranging surveillance of a user's cyber activities portend a grave threat to data privacy.

The dilemma of users, extensive of library users, in choosing to be vulnerable to cyberattacks or to adopt cybersecurity applications that will likely compromise their privacy by accessing personal and sometimes sensitive data was a subject examined by Chassidim, Perentis, Toch and Lepri (2020). The study identified that users were willing to open up their privacy moderately in exchange for a medium level of protection. However, the result from the study supports that the understanding of users that lesser exposure of private data translates lesser level of protection by cybersecurity applications, was a decisive factor in determining which cybersecurity application to choose; though there was no such positive effect in choosing an application with a higher privacy invasion.

Caches and web cookies collect data on and about the library users (browsing history, IP addresses, device identification, e.t.c). While some sites have the cookies privacy settings where the user can control the type and amount of data that can be collected or stored about him/her, some do not. Where a user has such control, and is not comfortable with the policy terms and conditions of the site, s/he has the option to reject or decline in which case, though may not be able to gain access to the information or data sought on the site. By this, library user has the right to sharing personal data domiciled within his/her control. Unlike where data is collected without the consent or prior information of such data collection to the user. Toch, et al (2017) in their study on dealing with privacy invasion opined that it could be viewed in three categories; (1) the No control category where due to the configuration of the system, user cannot interact in a straightforward manner with it and as such has no control or means of choosing a preference as it relates to privacy policies because such policies are not displayed at all to the view of the user. (2) Indirect control where there is a potential of interaction of system with the user and so there is the possibility of user controlling the privacy aspect; and (3) full control where the user can interact with the system to modify or control the settings of privacy aspects as the infrastructure or/and configuration allows the user to view the privacy policy and gives room to set privacy preferences.

There have been arguments that cyber security is more than technical issue, rather it deals with the security of an entire communications ecosystem. Therefore, it necessitates cooperation amongst multiple stakeholders to develop social norms, global cooperation, and regulatory framework in addition to the technical developments. The recognition that cyber security is linked to data protection, trust and privacy is very important (Privacy Commissioner of Canada, 2014). It has been argued however that though most pages or sites have data privacy policies and end-user agreements detailing what type of data is being collected and to what use they would be put; such policies and agreements are often very lengthy, and also unreadable by the average user (McDonald and Cranor, 2008 cited in Sumeeth et al. 2010).

CONCLUSION

In trying to safeguard the data privacy of library users, it is believed that the users should be given the leeway to make an informed choice as to what type of data could be stored or collected about them and/or their device; this is done where the webpage or site has a data privacy policy or statement that informs users of the type of data been collected about them and the use to which such data would and could be put. This some websites have incorporated. You are required to accept or decline after reading the terms and conditions or data privacy statement; it could also inform you that you click "continue" and that by agreeing to continue into the site or page you are accepting and agreeing to their data privacy policy. However, the data privacy statements are often so lengthy that the user may find it cumbersome to read and understand to arrive at a decision whether to accept or decline. It almost defeats the purpose of making an informed decision.

The library as custodian of information resources, inclusive of e-resources, is a stakeholder that must be in cooperation with the other stakeholders to ensure that regulations that will secure users' data privacy and be overly beneficial to the users are what is developed. The library too should position itself to monitor and enforce regulatory compliance.

RECOMMENDATION

- It is suggested that the policies and agreements should be written in simple and concise terms that is easily understandable to the average user and can be conveniently compared with policies and agreements of other websites or pages.
- Library personnel should instruct users on Cyber ethics or Online etiquette that teaches good use of web and how to browse safely. User education that teaches how to identify websites that are safe, e.g. where a URL starts with "https", it is considered a secure site as against where it reads only "http". Being conscious and cautious in following links and opening hyperlinks.
- Users should be mindful to delete caches after browsing especially when it is on a public computer station and/or from a signed-in device.
- Users should endeavour to check the privacy settings on the page or site they are visiting as most default settings are set up to allow snooping or storing of personal and sometimes sensitive information or data about browsing activities.
- More importantly, the library should understand its role in providing protection to its users and their data while also delivering its services as information providers. The library staff should be trained and have regular re-training on matters of cyber security.
- It should be normalised in libraries to have as a member of the library personnel, an expert IT system librarian.
- There should be a unit saddled with timely disseminating of information about security vulnerabilities or issuing advisories to users on identified cyber threats. The unit is to be responsible in providing regular reports on security breaches and steps taken to arrest such breaches. The system librarian should be the head and/or a member of this unit.

REFERENCES

Abo-Seada, A. A. (2019). *Magazines > Computers in Libraries > January/February 2019>Feature: the impact of the internet of things on libraries and users*. Retrieved August 2022, from Information Today Inc.: https://www.infotoday.com/cilmag/jan19/Abo-Seada--The-Impact-of-the-Internet-of-Things-on-Libraries-and-Users.shtml

AcqNotes. (2021, November 1). *Information Techology/Cyberspace*. Retrieved November 14, 2021, from AcqNotes website: https://acqnotes.com/acqnote/careerfields/cyberspace

Adakawa, M. I., Al-Hassan, M., & Ayuo, M. A. (2020, December 12). Now and Future of libraries: the necessity to equip librarians with cybersecurity skills. In *Management of Library and Information Centers in the era of global insecurity* (pp. 1-18). Retrieved May 17, 2022, from https://www.researchgate.net/publication/346967054_NOW_AND_FUTURE_OF_LIBRARIES_THE_NECESSITY_TO_EQUIP_LIBRARIANS_WITH_CYBERSECURITY_SKILLS/link/5fd530c392851c13fe80f57a/download

Adepetun, A., & Ityokura, M. (2022, January 12). *NIMC claims servers are secure, denies alleged breach*. Retrieved from The Guardian Nigeria Newspaper Web site: https://guardian.ng/news/nimc-claims-servers-are-secure-denies-alleged-breach/

Adepetun, A., & Onyedika-Ugoeze, N. (2022, May 16). *Hackers can unlock, steal your vehicles, NCC warns Nigerians*. Retrieved May 18, 2022, from The Guardian Nigeria Newspaper Web site: https://guardian.ng/news/hackers-can-unlock-steal-your-vehicles-ncc-warns-nigerians/

Ajie, I. (2019, February 20). A review of trends and and issues of cybersecurity in academic libraries. Retrieved May 15, 2022, from https://core.ac.uk/download/pdf/215162199.pdf

American Library Association. (2019, June 24). *Privacy: An Interpretation of the Library Bill of Rights*. Retrieved May 17, 2022, from American Library Association Web site: https://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy

Analytics India Magazine. (2020, March 05). *Cybersecurity: Difference between cybersecurity & information security*. Retrieved November 15, 2021, from Analytics India Mag website: https://analyticsindiamag.com/difference-between-cybersecurity-information-security/

Bhavsar, S., & Bhavsar, S. (2017). Cyber crimes and measures to prevent in libraries. *Knowledge Librarian, 3*(5), 38-47. Retrieved August 2, 2022, from http://www.klibjlis.com/4.5.7.pdf

Borgman, C. L. (1997). From acting locally to thinking globally: a brief history of library automation. *Library Quaterly, 67*(3). doi:10.1086/629950

Candela, L., Castelli, D., & Panago, P. (2011). History, evolution and impact of digital libraries. In I. Iglezakis, T.-E. Synodinou, & S. Kapidakis (Eds.), *E-Publishing and Digital Libraries: Legal and Organizational Issues* (pp. 1-30). IGI Global. doi:I:10.4018/978-1-60960-031-0.ch001

Chassidim, H., Perentis, C., Toch, E., & Lepri, B. (2020). Between privacy and security: the factors that drive intentions to use cyber-security applications, behaviours & information technology. *Behaviour & Information Technology*. doi:10.1080/0144929X.2020.1781259

Clarke, N., J. Symes, H. Saevanee, and S. Furnell. 2016. “Awareness of Mobile Device Security: A Survey of User’s Attitudes.” International Journal of Mobile Computing and Multimedia Communications (IJMCMC) 7 (1): 15–31.

Craigen, D., Diakum-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*.

CSRC. (n.d.). *Cyberspace*. Retrieved November 15, 2021, from NIST: https://csrc.nist.gov/glossary/term/cyberspace#

Emmanuel, V., & Anele, E. (2018). Influence of information and communication technologies (ICT) on some library services in libraries of Federal Uniersities in South-South Nigeria. *International Journal of Applied Technologies in LIbrray and Information Management, 4*(2), 9-16.

Guardian Newspaper. (2020, October 14). *Annonymous claims hacking of Nigerian Government's websites in support of ENDSARS*. Retrieved November 13, 2021, from Guardian Newspaper: https://guardian.ng/news/anonymous-claims-hacking-of-nigerian-governmnets-websites-in-support-of-endsars/

Henke, J. S., Joeckel, S., & Dogruel, L. (2018). Processing privacy information and decision-making for smartphone apps among young German smartphone users. *Behavior & Information Technology*, *37*(5), 488-501.

IBM. (n.d.). *Why attacks happen*. Retrieved May 17, 2022, from IBM Web site: https://www.ibm.com/topics/cyber-attack

Ifijeh, G., & Yusuf, F. (2020, August). Covid-19 pandemic and the future of Nigeria's university system: the quest for libraries' relevance. *Journal of Academic Librarianship*, *46*, 1-8. Retrieved May 17, 2022, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7426696/

Injac, O., & Sendelj, R. (2016). National Security Policy and strategy and Cyber Security risks. In M. Hadji-Janev, & M. Bogdanoski (Eds.), *Handbook of Research on Civil Society and National Security in the era of cyber warfare* (pp. 22-48). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-8793-6.ch002

ITU Telecommunication Development Bureau. (2012, September). *Understanding cybercrime: phennomena, challenges and legal response.* International Telecommunication Union (ITU). Retrieved August 2, 2022, from https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Kaur, G. (2020, August 14). Privacy issues in cyberspace: an Indian perspective. *SSRN*. Retrieved May 17, 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3673665

Laaro, M. D. (2021, March). Library services amidst Covid-19 pandemic: adjusting to the new normal. *Emperor International Journal of Library and Information Technology Research*, *1*(3), 24-27. Retrieved May 18, 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3859280

Lim, H. S., Taerigh, & Araz. (2018). Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications. *Energies*(11), 1062. Retrieved May 09, 2022, from https://www.mdpi.com/1996-1073/11/5/1062/htm#B13-energies-11-01062

Lippert, K. J., & Robert, C. (2021). Cyberspace: A digital ecosystem. *Systems*, 1-20. doi:doi.org/10.3390/systems9030048

Mobile Security and Privacy. (2017). In M. H. Au, & K.-K. R. Choo (Eds.), *Mobile Security and Privacy: Advances, Challenges and Future Research Directions* (pp. 1-4). doi:10.1016/B978-0-12-804629-6.00001-8

Nicholas-Rocca, S. T. (n.d.). Informatiom security in libraries: examining the effect of knowledge transfer. Retrieved from https://ejournals.bc.edu/index.php/ital/article/download/10973/9495/

Nigerian Communications Commission. (2022, January 29). *Media Centre>News Headlines>Press Statement: NCC-CSIRT identifies two cyber vulnerabilities*. Retrieved from Nigerian Communications Commission website: https://ncc.gov.ng/media-centre/news-headlines/1154-press-statement-ncc-csirt-identifies-two-cyber-vulnerabilities

Office of the privacy commissioner of Canada. (2014, December). *Privacy and Cyber Security: Emphasisng privacy protection in cybers ecurity activities.* Retrieved November 15, 2021, from Office of Privacy Commisioner of Canada website: https://www.priv.gc.ca/media/1775/cs_201412_e.pdf

Pande, J. (2017). *Introduction to cyber security*. Haldwani: Uttarakhand Open University. Retrieved November 10, 2021

Reddy, G. N., & Reddy, G. J. (2014). A study of cyber security challenges and its emerging trends on latest technologies. Retrieved November 15, 2021, from https://arxiv.org/ftp/arxiv/papers/1402/1402.1842.pdf

Romdhani, I. (2017). Securing the Internet of Things. In S. Li, & L. D. Xu, *Existing Security Scheme for IoT* (pp. 119-130). doi:10.1016/B978-0-12-804458-2.00007-X

Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018, November). Overview of Cyber Security. *International Journal of Advanced Research in Computer and Communication Engineering, 7*(11), 125-128. doi:10.17148/IJARCCE.2018.71127

Shabana, T. S., Saleem, A., & Sadik, B. M. (2013). Impact of library automation in the development era. *IOSR Journal of Humanities and Social Science, 17*(5), 20-26. Retrieved August 2, 2022, from https://www.researchgate.net/publication/324829280_Impact_of_Library_Automation_in_the_Development_Era

Solms, R. v., & Niekerk, J. V. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102. Retrieved November 14, 2021, from https://profsandhu.com/cs6393_s19/Solms-Niekerk-2013.pdf

Sumeeth, M., Singh, R. I., & Miller, J. (2010, January). Are Online Privacy Policies Readable? *International Journal of Information Security and Privacy*, 93-116. Retrieved May 17, 2022, from https://ideas.repec.org/a/igg/jisp00/v4y2010i1p93-116.html

The Open University. (n.d.). *Home: Subjects>Science, Maths & Technology>Free courses>Internet of everything>Session 1: What is the IoE?1.1 Internet of everything*. Retrieved from The Open University web site: https://www.open.edu/openlearn/mod/oucontent/view.php?id=48444&section=1

The Punch Newspaper. (2021, July 4). *Nigeria ranks 47th on UN's cybersecurity index*. (T. Jaiyeola, Editor) Retrieved May 17, 2022, from The Punch newspaper web site: https://punchng.com/nigeria-ranks-47th-on-uns-cybersecurity-index/

Toch, E., Bettini, C., Shmueli, E., Radeilli, L., Lanzi, A., & al., e. (2018, February). The privacy implications of cyber security systems: A technological survey. *ACM Computing Surveys, 51*(2), 36:1-27. doi:10.1145/3172869

Toch, E., Wang, Y., & Cranor, L. F. (2012). Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems. *User Model User Adapt. Interact., 22*(1-2), 203-220.

University of Lagos. (2020, June 29). *University of Lagos receives donation of robots from Platform Capital*. Retrieved May 17, 2022, from University of Lagos Web site: https://unilag.edu.ng/?p=6902

Vadza, K. C. (2013). Cyber crimes and its categories. *Indian Journal of Applied Research*, *3*(5), 130-133. doi:10.15373/2249555X/MAY2013/39

Zia, Y., Theseen, S., & Kathane, R. (2020). Information (ICT) securities and libraries. *Indian Journal of Library Science and Information Technology*, *5*(1), 43-45. Retrieved May 17, 2022, from https://www.ijlsit.org/journal-article-file/11781