Unizik Journal of Educational Management and Policy (UJOEMP), Vol 7, No. 1, September, 2025. ISSN: 2276-7630

CYBER SECURITY ISSUES CONFRONTING SCHOOL ADMINISTRATORS IN THE MANAGEMENT OF INFORMATION SYSTEM IN SECONDARY SCHOOLS IN ANAMBRA STATE.

Jude, Azubuike Anynawu[1], Ugochi Ehiahuruike[2*], Chidimma C.Thompson[3]

[1,2,3] Educational management and policy, Nnamdi Azikiwe University, Awka,

Correspondence Email address: Ja.anyanwu@unizik.edu.ng

Abstract

Digital information management systems have impacted critical technical infrastructure development around the world but cyber security management issues are constantly at the fore, therefore, the need to strengthen and protect these systems against the ever-evolving cyber threats is pertinent. The study therefore, analyzed cyber security issues confronting administrators in management information systems in the secondary schools in Anambra State. The study adopted descriptive survey design and two research questions guided the study. The population of the study is made 265 principals of the public secondary school in Anambra state. A researcher developed instrument titled 'Cyber security Issues confronting secondary school administrators in management information system questionnaire" (CSICSSAMISQ) was use to collect data. The questionnaire containing 20 items, structured on 4 point liket structure of Strongly Agreed (SA), Agreed (A), Strongly Disagreed (SD), and Disagreed (D). It was validated by three experts who are lecturers in the department of Educational Management and policy and Measurement and Evaluation all in the Faculty of Education, Nnamdi Azikiwe University, Awka. Cronbach-alpha was used to test reliability of the instrument which yielded a coefficient value of 0.85. Data were analyzed using mean and standard deviation. The findings of the study showed that there are constant cyber threats on school information systems and cyber security measures have been applied minimally. Therefore, the study concluded that cyber-attack and threats are the bane of information technology and to mitigate this challenge, Administrators of school organizations have to be ahead of these attackers in making sure that all kinds of vulnerabilities and gaps are constantly closed in by applying multiple security measures. It was recommended that; the Administrators should organize periodic capacity building seminars and workshops for their Administrative Staff on digital information management and cyber security. Also Government should be proactive in prosecuting internet fraudsters. If all these are done, they will ensure a sustainable school information management system.

Keywords: Cyber-Security, Administrators, Management, Information, Systems,

Introduction

Cyber security is the practice of protecting critical systems and sensitive information from digital attacks. It is also known as information technology (IT) security. Cyber security measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization. Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security (Uzochukwu, 2021). Similarly, Osuala (2017), posited that cyber security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware. Cyber security focuses on keeping software and devices free of threats. Successful cyber security begins at the designing stage, well before a program or device is deployed. Cyber security protects the integrity and privacy of data, both in storage and in transit (Okeke, 2018). Cyber security includes the processes and decisions for handling and protecting data assets (Osuala, 2019). However, The Cyber security Body of Knowledge defines cyber security as protecting information systems (hardware, software, and related infrastructure), data, and services from unauthorized access, harm, or misuse (Martin, Awais, Howard, Steve, Emil, and George, 2021). Cyber security involves the use of technical and non-technical controls with functions of identification, protection, prevention, detection, response, and recovery (NIST, 2018) and (Putro, Adi, and Dana Indra. 2022). According to Harris, and Fernando (2019), security here is associated with information because security risks are determined by data value. This is became the basis for the explanation of information security that focused on the confidentiality, integrity, and availability of information. This security system includes computer security, digital security or information technology security (IT security) which is the protection of computer systems and networks from attack by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data, as well as from the disruption of management of information system direction and, of the services they provide (Adeleye, 2017). Cyber security therefore, is the protection of internet-connected systems such as hardware, software and data from cyber-threats. It also refers to every aspect of protecting an organization and its employees and assets against cyber threats. For Okonkwo (2019), Cyber security is a discipline that covers how to defend devices and services from electronic attacks by nefarious actors such as hackers. In a nutshell; it is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber-attacks and internet fraudsters.

Management Information system (MIS) according to Adeleye (2019), refers to any framework of software that facilitates the collection, storage, organization, and distribution of information. Similarly, Brown (2018) posited that Management of Information System (MIS) refers to any framework of software that facilitates the collection, storage, organization, and distribution of information. For Igwe (2019) Management of Information System is a comprehensive set of applications, processes, and technologies that are used to collect, store, and manage data. Information management encompasses a series of organizational activities about acquiring, storing, and distributing information to stakeholders. Management of information system involves the recording, correct storage, retrieval and use of information for effective decision making in an organization. In information management, the guiding principle is that information must be readily available at the time and in the form required. It must be accurate, reliable and

informative for the basis of functional decision. Management information system now becomes the application of electronic media in managing, processing, storing, retrieving and communication of information for decision making (Ikediugwu and Anyanwu 2019).

School information system is the backbone of any school organization. This process has become the most modern method of acquiring, processing and communicating among formal organizations. They help management in reaching out to any information, data, and knowledge in a structured way. It is a computer system (or set of computer programs) used to track and store information. The goal of an MIS is to provide better access to information for decision-making purposes (Adebola, 2019).The management of secondary school education requires lots of information to ensure good organizational performance. Information is regarded as a fundamental resource to organization and as such its management is apparently one of the most strategic operational instruments for organizational efficacy. Management of information system plays indispensable roles in the smooth running of secondary schools. Effective management of information in secondary schools aids the school administrators in resolving administrative challenges emanated from paucity of accurate, dependable and timely information for decision-making. Information gathering technique could be utilized to improve administrative decisions in the school system in areas like; planning of school program, teaching and examination, Preparing of school timetable and activities, managing human and material resources, taking timely decisions on students admission and enrolments, hostels, offices, staff quarters allocations among others (Turban, Aronson& Liang, 2019). Others include processing and transmitting of school results and result checker cards. Management of information system has taken a central focus in educational practices, procedures and process. MIS cannot be said to have been deployed without the ancillary resources of ICT and Artificial Intelligence. Anyanwu, Amaefula and Anyaeji (2021) observe that schools use a diverse set of ICT tools to communicate, create, disseminate, store, and manage information. In some contexts, ICT has also become an integral process of the teaching-learning interaction where chalkboards have been replaced with interactive digital whiteboards and screens. Online platforms such as Google Meet, Zoom, You tube, WhatsApp, and other Learning Management Systems (LMS) are utilized. Students attend lectures virtually on their computers and with their smart phones. These entire systems have come as innovations and impact educational management process, practice and procedure.

Management of information system is undoubtedly a veritable tool for effectiveness of secondary school administration and hence, its proper management is a panacea for institutional success. Poor information management technique has been observed as a logjam to the successful management of schools in Nigeria (Okeke & Ikediugwu, 2021). However, students, teachers and administrators in Nigerian secondary schools are yet to be adequately exposed to the realities of numerous challenges of the 21st Century that is technologically driven in outlook (Nkata, 2020). One of such realities and challenges is the internet of things and the cyber security threats and measures that come with it. One of the salient issues about the use of management of information system in Nigerian secondary schools is hinged on adequate measures being put in place to ensure cyber security of school information. According to Onu (2020) cyber criminals tends to tamper with the information system of many secondary schools in Nigeria. Consequently, this has resulted in many challenges to official school information system in many secondary schools

such as such as tempering with official school information, cracking and hacking of school password systems which grants fraudsters assess to school information resulting to licking of examination question papers, faking of online result checker card and falsification of results. In this regard, Igbokwe (2021), deduced that school data/information are tampered with by internet fraudster for instance licking of examination questions, (internal or external WAEC or NECO) cracking of school password, faking of results or certificates. All these are as result of lack of basic cyber security measures in information management in secondary schools and other examination organization. This threatens the validity, serenity and credibility of these institutions.

Cyber Security Threats

Although cyber security professionals work hard to close security gaps, attackers are always looking for new ways to escape IT notice, evade defense measures, and exploit emerging weaknesses. According Odion and Akachukwu (2021), the latest cyber security threats are putting a new spin on "known" threats, taking advantage of work-from-home environments, remote access tools, and new cloud services. These evolving threats include:

Malware: The term "malware" according to the Wilson and Okeke (2019) refer to malicious software variants such as worms, viruses, Trojans, and spyware that provide unauthorized access or cause damage to a computer. Malware attacks are increasingly "file less" and designed to get around familiar detection methods, such as antivirus tools, that scan for malicious file attachments.

Phishing/social engineering: Phishing is a form of social engineering that tricks users into providing their own sensitive information. In phishing scams, emails or text messages appear to be from a legitimate company asking for sensitive information, such as credit card data or login information. The study by Nwankwo (2019) has noted about a surge in pandemic-related phishing, tied to the growth of remote work.

Insider threats: Current or former employees, business partners, contractors, or anyone who has had access to systems or networks in the past can be considered an insider threat if they abuse their access information systems. Insider threats can be invisible to traditional security solutions like firewalls and intrusion detection systems, which focus on external threats.

Distributed denial-of-service (DDoS) attacks: A DDoS attack attempts to crash a server, website or network by overloading it with traffic, usually from multiple coordinated systems. DDoS attacks overwhelm enterprise networks via the simple network management protocol (SNMP), used for of modems, printers, switches, routers, and servers.

Advanced persistent threats (APTs)

In an APT, an intruder or group of intruders infiltrate a system and remain undetected for an extended period. The intruder leaves networks and systems intact to spy on business activity and steal sensitive data while avoiding the activation of defensive countermeasures. The recent Solar Winds breach of United States government systems is an example of an APT.

Man-in-the-middle attacks: Man-in-the-middle is an eavesdropping attack, where a cybercriminal intercepts and relays messages between two parties in order to steal data. For example, on an unsecure Wi-Fi network, an attacker can intercept data being passed between guest's device and the network.

Cyber security measures

These are measures that will be applied to prevent cyber-attack of information of any organization. Schools are under attack, though, almost constantly from increasingly organized and sophisticated cyber-criminal gangs (Adebayo, 2021).According to Wilson (2021) this is very much because the connected physical devices have a unique identifier (UID) and have the ability to transfer data over a network without any requirements of the human-to-human or human-to-computer interaction. The firmware and software which is running on Internet of Things devices make secondary schools highly susceptible to cyber-attacks. To avert all, every school organization should work with cyber security professionals to ensure the security of their password policies, session handling, user verification, multifactor authentication, and security protocols to help in managing the potential risk and attack. Some security measures to be adopted are:

End to End-Encryption (E2EE): This is privacy and security which is built into social media apps that ensures messages, photos, videos, voice messages, documents and calls are secured from cyber attackers and hackers**.** With this, the messages are secured with lock, and only the recipient and the sender have the special key needed to unlock and assess the information. It ensures cloud storage and security of information which brings about true confidential computing that encrypts cloud data at rest (in storage), in motion (as it travels to, from and within the cloud) and in use (during processing) to support privacy, business requirements and regulatory compliance standards. This conforms to the General Data Protection Regulation (GDPR) that secure most sensitive data from unauthorized access, exposure, or theft. It prohibits and criminalizes cyber attackers and hackers. This measure ensures confidentiality, integrity and authentication of data both in transit and reception and storage. There are three types of end to end encryption: Symmetric key encryption, Asymmetric and Hybrid encryption which is a combination symmetric and asymmetric. This measure could be applied in messaging apps such as whatsapp, signal, Telegram. Email services such as Protonmail and Tutanota, File sharing: drop box, Google drive, Video conferencing: zoom, Skype, Social media platforms: face book messager, Tiktok, Instragram

Two Step Verification Codes (**2SV**): This is a mobile app security setting that adds an extra layer of protection to the traditional username/password login process. This makes it harder for attackers to gain unauthorized access to their information system. It reduces and limits the effectiveness of phishing attacks; also it helps apps meet regulatory requirements and enhanced user trust by demonstrating commitment to security. There are different types of two steps verification measures

1. SMS-based 2SV
2. Time-based>one –time Password (TOTP)
3. HMAC-based one Time Password (HOTP)
4. Authenticator app-based 2SV
5. Biometric-based 2SV > Facial recognition, fingerprint scanning. Voice
6. Push –based 2SV > Push notification.

To ensure best practices in the implementation of this of measures certain protocols and procedures

will be established. The administrator must choose a secure 2SV method. Must make 2SV optional or mandatory depending on the app requirements and be able to provide clear instructions for users and offer backup and recovery codes, finally provide regular update and patch 2SV systems. To ensure the security of the system app, it will require the integration and use of application programming interfaces(APIs) such as Google authenticator API that enable different applications, services, or systems to communicate with each other in data exchange, functionality reuse and integration of service. This will enable the system app to send verification requests, receive verification codes and validate user credentials before approving further action. Furthermore the Software Development Kits (SDKs) which are inbuilt software libraries that provide a set of tools, documentation and sample codes to help developer integrate specific functionality into their apps. In this context it helps the system app to integrate 2SV functionality and display and handle verification logic which is mostly applied in Google authenticator SDK, Facebook account Kit SDK and Microsoft Azure Active Directory SDK. All are necessary application of 2SV provides and integrate login and registration flows

End-user`–**Education**: Building security awareness across the school organization to strengthen endpoint security. For example, users can be trained to dictate suspicious email attachments, avoid using suspected or compromised USB devices, and not granting unauthorized access to individuals into the computer systems and websites. It also includes network security measures for protecting a computer network from intruders, including both wired and wireless (Wi-Fi) connections.
Application security-these are Processes that help protect applications operating for management of information systems and in the cloud. Security should be built into applications at the design stage, with considerations for how data is handled, user authentication, etc.

Therefore, cyber security measure in school information system has become a necessity. Therefore, there is need to carry out investigation on the cyber security issues which confronts administrators in the management of information system in secondary schools. It is on this basis that this research is being carried out to find out the cyber security threats and measures confronting administrators in the management information systems in secondary schools in Anambra State.

Statement of the Problem

Management of information system in school organization has transformed schools and organizations today by making information accessible for decision making. Many schools today have migrated to digitalized system of information management which makes use of the computer and internet facilities a necessity. The state government in order to make the school move with the trend of time has provided computer and internet facilities in all schools in the state and organized periodic cyber trainings for all staff of the commission. Despite all these, there are complains of tempering, manipulating, licking and forgery of official documents and falsification of school results checker cards and unauthorized accesses to school website. Therefore, one wonders if there are any measures put in place by the secondary school principals to counter cybercrime being experienced in the management of information systems in their

schools. Some many people are of the view that there many threats to management of information system in schools while others said that secondary schools in the state are not yet ready to face the challenges of cyber security. Therefore, there is need to carry out an investigation on the cyber

security issues confronting the principals in the management of information systems in secondary schools in Anambra state.

Purpose of the Study

The main purpose of the study is to investigate the cyber security threats and security measures adopted by administrators in the management of school information systems in secondary schools in Anambra State. Specifically, the study sought to:

1. Find out the cyber security threats to management of information system in secondary schools in Anambra state.

2. Find out the cyber security measures adopted by the administrator in the management of information system in secondary schools in Anambra state.

Research Questions

The following research questions guided the study:

1. What are the cyber security threats to management of information system in secondary schools in Anambra state

2. What the cyber security measures adopted by the Administrators for management of information system in secondary schools in Anambra state.

Method:

The design for the study is the descriptive survey research design. The population of the study is made of 263 principals of public secondary schools in Anambra State (PPSSC, 2023). A research developed instrument titled "Cyber security issues confronting secondary school administrators in information management systems questionnaire" (CSICSSAIMSQ) was used for data collection. The instrument contained 20 items structured on 4 point liket structure of Strongly Agreed (SA), Agreed (A), Strongly Disagreed (SD), and Disagreed (D). The instrument was validated by three experts, two from the department of Educational Management and Policy and one from the Measurement and Evaluation in the department of Educational Foundations all in the Faculty of Education, Nnamdi Azikiwe University, Awka. The instrument was pilot tested on 20 Administrators from Owerri Urban zone secondary school to determine its reliability. Cronbach-alpha was used to calculate the reliability of the instrument which yielded a coefficient value of 0.80. Data were analyzed using mean and standard deviation. Any item whose mean score is above the benchmark of 2.50 was regarded as agreed while those items with mean score below the mean benchmark of 2.50 were regarded as disregarded.

Results

Research Question 1

What are the cyber security threats to Management of information system in secondary schools in

Anambra state?

Table 1: Mean rating of respondents on the cyber security threats to Management of information system in secondary schools in Anambra state

S/N	Cyber security threats	$\bar{X}$	Remark
1.	Malware	3.44	Agreed
2	Phishing/social engineering	3.13	Agreed
3	Insider threat	3.28	Agreed
4	Distributed denial of service (DDOS) attack	2.68	Agreed
5	Advanced persistent threat (APTs)	3.64	Agreed
6	Man-in-the middle attack	3.62	Agreed
7	Structural query language (SQL) injection attack	2.56	Agreed
8.	SIM swap attack	3.35	Agreed
	Mean of Means	**3.20**	**Agreed**

In Table 1, all the items (1, 2, 3, 4, 5, 6, 7, and 8) indicated a mean score which is above 2.50 the mean decision level the mean of means is 3.20. Thus indicating agreement to all issues in the items as being cyber security threats to management of information system in secondary schools in Anambra state

Research Question 2

What are the cyber security measures adopted by administrators for management of information system in secondary schools in Anambra state?

Table 2

Mean rating of respondents on the cyber security measures for Management of Information System in secondary schools in Anambra state

S/N	cyber security measures for management of information system	$\bar{X}$	Remark
9.	End to end-encryption (E2EE)	2.56	Agreed
10.	Multi factor Authentication	3.04	Agreed
11.	Web application firewall security (WAF)	2.06	Disagreed
12.	End –user- education	2.54	Agreed
13.	Keeping software up to date	2.18	Disagreed
14.	Protection of servers with a reserve Roxy	1.09	Disagreed
15	Anti-virus application software	2.23	Disagreed
16	Using strong passwords	2.76	Agreed
17	Data Backup plan	2.42	Disagreed
18	Incident response plan	1.67	Disagreed
19	Compliance regulations	1.09	Disagreed
20	Continuous monitoring	2.36	Disagreed
	Mean of Means	**2.35**	Disagreed

Data contained in Table 2 indicate that the respondents agreed to all the items , 9, 10, 12 and 16 as cyber security measures adopted by the Administrators in managing information system in their schools but disagreed in items, 11, 13, 14, 15 18, 19 and 20. Then the mean of means of 2.35 which

is below the criterion of mean score of 2.50 indicating the respondents' opinion which shows that the Administrators disagreed to adopting those cyber security measures for management of information system in secondary schools in Anambra state.

Summary of Major Findings

Based on the findings of the study, it was discovered that:
There are cyber security threats to school information management such as: SIM swap attack, Malware, phishing/ social engineering, Structural query language (SQL) injection attack, insiders attacking which grants fraudsters assess to school information there by tampering with the school official information.
It was also found out that the school Administrators has not being able to apply the cyber security measures in secondary school information management systems.

Discussion of Results
The findings of the study showed that cyber security threats to Management of information system in secondary schools in Anambra state include malware, phishing/social engineering, insiders threat, distributed denial of service, man in the middle attack, structured language but Sims swap attack are among the most prevalent which has resulted into various level cyber threats. These cyber threats on information management systems lead to cracking of school password systems which grants fraudsters assess to school information, hackers tampering with the school official school information, licking of question papers by hackers, faking of semester results and certificates by hackers and developing fake online result checker card. This is an indication that there no security measures in school information systems. To support these findings, Onu (2020) agreed that cyber criminals tend to tamper with the information system of many secondary schools in Nigeria. Consequently, this has resulted in many challenges to official school information system in many secondary schools. In this regard, also Igbokwe (2021), deduced that school data/information are tampered with by internet fraudster for instance licking of examination questions, of (internal or external WAEC or NECO) cracking of school password, faking of results or certificates. Most of the times these threats will send online as virus to attack vulnerable school information systems which will corrupt their database and enable them to manipulate the information there in. According to the Wilson and Okeke (2019) there are malicious software variants such as worms, viruses, Trojans, and spyware that provide unauthorized access or cause damage to a computer. Malware attacks are increasingly "file less" and designed to get around familiar detection methods, such as antivirus tools, that scan for malicious file attachments. Most of the school administrators are vulnerable because of their inability to understand the tricks of phishing before supplying their school sensitive information or responding to text massages or emails which automatically grants the cyber-criminals automatic access to school information. Therefore school administrators should be trained on how to identify social engineering and phishing and other cyber threats to avoid cyber-attacks on their websites and data base.

The findings of the study showed that cyber security measures for management of information system in public secondary schools in Anambra state are provision of: End to end-encryption, multi factor authentication security, Authenticator apps generate time-based codes that can be used for identity verification, rather than relying on SMS messages that can be intercepted or redirected.

Anti-virus application, system update and use of password are the only security measure being adopted by the administrators. While Network security, Cloud security, Physical security, mobile security Application security, Web application firewall security and end user security among others were not being applied. This means the cyber security measures were minimally applied in secondary schools in Anambra state. To support these findings, Igbokwe (2021) posited that cyber security issues in school information system has become a necessity such as network security, cloud security, physical security, endpoint security, mobile security, IoT = Internet of things security, application security and Zero Trust security should adopted. Appropriate measures should be put place through training and deployment of cyber security professionals to work hard to close security gaps, because we know that attackers are always looking for new ways to escape IT notice, evade defense measures, and exploit emerging weaknesses and vulnerabilities in the system. Adequate human and artificial intelligence technologies should be deployed in the management of school information systems.

Conclusions

Management of information system has transformed organizations today by making information accessible for decision making. Many schools and organizations have migrated to digitalized system of information management which makes use of the computer and internet facilities a necessity. Hindustan Industrial Research (2023) observes that in today's digital age, cyber security is a critical concern for individuals and organizations alike. The deployment of internet and artificial intelligence (AI) in management has come as an innovation and has transformed the system and process of management making it less cumbersome in tracking the progress of an organization. However cyber-attack and threats are the bane of information technology. To mitigate this challenge, management of organizations has to be ahead of these attackers in making sure that all kinds of vulnerabilities and gaps are constantly closed in. They have to be abreast with the latest and most updated strategy in cyber security to ensure the credibility and sanctity of the system. Therefore, in the fight against cyber threats, it is important to take a compound approach rather than relying solely on only one approach.

Recommendations

To win the fight against cyber threat and attack, Organizations and Administrators of MIS facilities must be intentional about the application of the different measures. Cyber security experts recommend using a multi authenticator app instead of relying on SMS-based authentication. By taking steps to protect against SIM swap attacks, individuals can further enhance their overall cyber security and minimize their risk of falling victim to identity theft and account takeover, Administrators should use strong and complex password system, End to end-encryption (E2EE), and Web application firewall security (WAF).

School administrators should apply continuous monitoring and periodic data back up; this will ensure compliance to some specific regulations that govern organizations to protect sensitive

data and continuous end–user education which updates administrators and all staff of the latest strategy should be adopted. This can be done through seminars and workshops and conference on data management and security in the system.

Finally, Government should be proactive in enforcing the legislating against cyber-crime in the country where internet fraudsters are prosecuted.

By implementing these measures, individuals, schools and organizations can minimize their incidence of cyber-attacks, enhance their cyber security and better protect their valuable data and assets against cyber threats.

REFERENCES

Adebayo, S. (2018). Social media and public administration: Theoretical dimensions and introduction to symposium. *Administrative Theory & Praxis, 33*(3), 325-340.

Adebola, A. (2021). Should we be conserved about children use of internet? - pilot study. *Innovative Issues And Approaches In Social Sciences,6*(2), 7-9; 11-13.

Adeleye, V. (2021).Social software and the future of conferences right now.*Education Use Review, 47*;(59) 117-197.

Anyanwu J.A., Amaefula F.N and Anyaeji V. A. (2021),Principals' ICT Competency: An Imperative for Management of Information Systems in Public and Private Secondary Schools in Anambra State*in International Journal of Innovative Science and Research Technology 6(12) 196-204*

Hindustan Industrial Research Private Limited (2023).*The Role of Antivirus Software in Cyber Security: A Comprehensive Guide*.https://www.linkedin.com/pulse/role-antivirus-software-cyber-security-comprehensive-i/

Igbokwe, K. (2021). Social media & mobile internet use among teens and young adults.*Pew Internet & American Life Project, 1*, (37), 89-156.

Igwe, E. (2021). Perception and use of social media by the students of Calicut University.*DESIDOC Journal of library & information technology, 3*(4), 295-301.

Ikediugwu P.N and Anyanwu J. A. (2019).Comparative Analysis of Principals' ICT Competencies for Management of Information System In Public and Private Secondary Schools in Anambra State, Nigeria in *UNIZIK Journal of Educational Management and Policy 3(1), 131-144*

Martin, A, Awais R, Howard, C. Steve S., Emil L, and George D. (2021) "Introduction to Cyber Security Body of Knowledge Areas." In: Cyber Security Body Knowledge.

Nkata, D. (2020). What anyone can know: The privacy risks of social media. *IEEE Security and Privacy, 5*, 40-49

NIST.(2018) "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1." Cybersecurity Framework. doi: 10.6028/NIST.CSWP.04162018

Odion, J. &Akachukwu(2021). *Facebook identity Theft enough for jail*. Retrieved from http://net.educause.edu/ir/library/pdf/ERSl 103/ERS1103W

Okeke, P.&Ikediugwu, O (2021). *Teens and technology: Youth are leading the transition to afully wired and mobile nation*. Pew Internet And American Life Project.

Okeke, R. (2019). The relationship between multitasking and academic performance.*Computers & Education, 59*(4), 1-10.

Okeke, S. (2018).*Ali ObstajaOdvisnostodInterneta*? [Does exit dependence of Internet?]. Retrieved from http://www.safe.si/uE1259749064Odvisnost odinterneta- B onacicMirj am. doc.

Okonkwo, N. (2019). Social network sites.Definition, history and scholarship.*Journal of Computer-Mediated Communication, 13*(2), 68-73.

Onu, H.T. (2020) *Ethics and technology: Controversies, questions and strategies for ethical computing, third edition, Hoboken*. New Jersey: Wiley & Sons Inc.

Osuala, G. (2017). 'About Face of social media'.*Marketing Age*: *Business & Leadership,, 4*(2), 22-25.

Putro, PrasetyoAdiWibowo, and Dana IndraSensuse. (2022) "Review of Security Principles and Security Functions in Critical Information Infrastructure Protection." InternationalJounralSaf SecurityEngineering(12):459–465

Turban, B. R. & Aronson, C.U.& Liang (2019). *Business studies and value orientation for nationaleconomic empowerment and development* Paper presented at the Owo 2019 annual conference of the Association of business educators of Nigeria (ABEN)

Uzochukwu, T. (2021).*The use of social media among University students in Abia State.*Retrieved from http:// www.news.com.au/story/0,27574,25764253-42 LOO.html.