SOCIAL FACTORS INFLUENCING THE KNOWLEDGE AND PRACTICE OF CYBERSECURITY AMONGST EMPLOYEES OF NNAMDI AZIKIWE UNIVERSITY MEDICAL CENTER

Chikwendu Stephen Chilaka
sc.chikwendu@unizik.edu.ng
&
Eke Leona
la.eke@unizik.edu.ng
Department of Sociology/Anthropology, Nnamdi Azikiwe University, Awka

Abstract
This study focused on the factors influencing the knowledge and practice of cyber security amongst employees of Nnamdi Azikiwe University medical center, Awka. The Health Belief Model and Broken Window Theory were adopted as the Theoretical frameworks for the study. The sample size was 189 respondents. This sample size was arrived at using the total sampling procedure. The questionnaire and in-depth interview guide were used for quantitative and qualitative data collection respectively. Quantitative data were analyzed using Statistical Package for Social Sciences (SPSS) and interpreted in percentages, frequency distribution tables and charts while qualitative data was categorized into themes and content analyzed. Findings indicate that most respondents have little or no knowledge about cyber security and the ability to identify threats. The study found that the major factor influencing the knowledge and practice of Cyber security in NAU Medical Center is training and education. The study recommends that every technologically inclined organization should provide regular cyber security awareness programs and training sessions for employees in order to improve their knowledge on cyber security thereby preventing cyber threats.
Keywords: Cyber security, knowledge and practice of cyber security, cyber-attacks, cybercrime, employees.

Introduction

Cyber security is indeed an ever present factor in every aspect of computing (Gilheany, 2017). Green (2016) notes that recent advances in technology and the proliferation of digital technologies like cloud, mobile and personal computing devices has enabled a lot of global crimes to be committed in the cyber space. Consequently, it has become imperative that cyber security practices become integrated into the very fabrics of everyday use of computing technologies. Therefore, cyber security is the practice of protecting systems, networks and programmes from digital attacks (Smith, 2017). It also refers to any activity carried out to ensure integrity, confidentiality and availability of information systems (Chai, 2021). Gilheany (2017) noted that due to proliferation of internet and ICT enabled devices, more people interact with computing devices such as servers through smart phones, smart watches, laptops, etc. These devices can be exploited and compromised by hackers using various malicious programmes or techniques. As a result, cyber security experts are always very busy trying to rectify security breaches across a huge variety of devices and systems, and checking to make sure that each type of device is fully safe and not being compromised or leveraged as a weak point in a probable cyber attack (Gilheany, 2017).

Maisikeli (2020) observes that most employees believe that cyber security is the responsibility of government, security applications and tools like (antivirus, firewalls, etc), some corporate individuals believe that it is the duty of the Information Technology (IT) department to handle cyber security; this may not be accurate. The human factor has been the weakest link through which several successful cyber-attacks have been perpetuated. Yet this erroneous view exists among a host of internet users (Maisikeli, 2020). Another scenario that presents little knowledge of cyber security among Nigerian workers is the belief that even though cyber threat is real, they can never become victims. These set of employees feel that sensitive institutions such as banks should be more concerned about cyber security (Smith, 2017). Even with low knowledge on cyber security some still think that they are well secured by their limited security practices. Others do not see cyber threat as much of a big deal to be prioritized because it does not inflict physical harm (Kostyuk & Wayne, 2019).

There are many factors influencing the knowledge and practice of cyber security, some of which include level of computer literacy, social status, internet infrastructure in the country, etc. According to Smith (2017), most internet users feel unsusceptible to threat. The reason for this mindset varies among individuals. The knowledge that some Nigerians have is that cyber attackers are more channelled towards national infrastructure and government agencies. Few others hold an optimistic view that they cannot fall victim of cyber-attack probably because they have never fallen victim, this over familiarity and confidence is usually not based on any technical security setup put in place, but sheer optimism (Ghosemajumder, 2017). Chai (2021) argues that if government and skilled professionals cannot attain hundred percent security guarantees on their computers, then there is no need arguing over what is beyond human control. There are also skilled employees with optimal knowledge of cyber security but may be practicing unsafe internet access. These set of users are in complete control of their

cyber activities ranging from device control to sites visited and their passwords, but even at that rate one is not immune to cyber threats and attacks.

For Maisikeli (2020), poor knowledge of cyber security management practices can lead to any of the following consequences: data loss, productivity loss due to downtime, damage of organization's reputation, law suits amongst others. Inadequate end-user security, employee negligence and weak password management are some of the reasons why hackers succeed in infiltrating systems. Once cyber attacker breaches organization's network, data can be stolen or corrupted. Loss of data integrity is disastrous if a business or organization does not have a backup plan. Data theft or loss has grounded and led to the closure of many organizations today. Kostyuk and Wayne (2019) buttresses that downtime caused by cyber-attacks may lead to productivity loss. When systems become infected with malware (i.e. computer virus), employees cannot perform routine tasks while the issue is remediated and systems restored. This research focused on identifying the extent/level of cyber security knowledge among staff of Nnamdi Azikiwe University Medical Centre and factors influencing the knowledge and practice of cyber security in NAU Medical Centre.

Literature Review

Concept of Cyber Security:

Cyber security is a critical concern in today's world as the internet has become an integral part of our lives. According to Al-Saggaf and Islam (2018), cyber security involves the use of technologies, processes, and policies that ensure the confidentiality, integrity, and availability of information in the digital domain. It aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks and technologies. According to a study by Ponemon Institute, the average cost of a data breach for organizations is $3.86 million, and the average time to identify and contain a breach is 280 days (Ponemon Institute, 2020). This highlights the importance of investing in cyber security measures to prevent or mitigate the impact of cyber-attacks.

One of the significant issues in cyber security is the increasing number of cyber-attacks. Ahmed, Zeki and Al-Ameen (2021) highlight that during the COVID-19 pandemic there was an increase in cyber-attacks, particularly on healthcare systems. Their study emphasized the need for cyber security measures to be implemented to secure healthcare systems and protect sensitive patient data

The extent of Cyber security knowledge among staff in a Medical center:

According to DePietro and Kimmel (2018), the level of cyber security knowledge among staff in medical centers is generally low. They believed that few of the healthcare professionals were able to identify a phishing email, which is a common tactic used by cybercriminals to gain access to sensitive information, making it impossible for these professionals to know what to do in the event of a data breach. This study was published in the year 2010 and 2017. Additionally, according to Sittig and Singh (2016), many of these healthcare professionals lack understanding of fundamental cyber security ideas like encryption and two-factor authentication. Essentially as a result of healthcare workers' ignorance of the significance of cyber security.

Additionally, according to HIMS Analytics (2017), only a small number of healthcare companies have a thorough security program in place. Stating that only a small number of these healthcare groups have a dedicated security team, while others regularly train their staff in cyber security.

In essence, there is a serious knowledge gap regarding cyber security among medical facility staff, which might expose private patient data to online threats. In order to better their staff's capacity to recognize and avoid cyber-attacks, medical centers must give priority to cyber security education and training.

A study conducted by Adeleke and Olugbara (2021) investigated the cyber security knowledge of healthcare staff in a tertiary hospital in Nigeria. The study found that while staff had some awareness of cyber security, there were significant gaps in their knowledge. Specifically, the study found that only 43% of staff were aware of the need for strong passwords, and only 33% knew how to identify phishing emails. Similarly, a study by Oyeyemi, Adeniyi, and Olawumi (2020) found that only 44.5% of healthcare staff in a tertiary hospital in Nigeria had basic knowledge of cyber security.

Another study conducted by Olumide, Oyeyemi, and Olawumi (2021) investigated the cyber security practices of healthcare staff in a university teaching hospital in Nigeria. The study found that while staff had some knowledge of cyber security, their practices were inadequate. Specifically, the study found that only 45.6% of staff used complex passwords, and only 38.3% changed their passwords regularly. The study also found that 46.7% of staff did not have antivirus software installed on their computers.

Factors influencing the knowledge and practice of Cyber security in medical centers:
A critical component of safeguarding private data is cyber security. To safeguard patient information in healthcare settings, cyber security is especially crucial. For healthcare companies to be protected from cyber threats, employee cyber security training and practice are essential.

The understanding and application of cyber security among staff members in a medical facility are influenced by a number of factors. Employees should be conscious of cyber security, according to Göktas and Celik (2020). They held the opinion that workers are more likely to adopt secure behaviours if they are aware of cyber security threats. Highlighting how the adoption of secure actions favorably correlates with awareness level.

Another factor that influences the knowledge and practice of cyber security is the level of training and education provided to employees. Caudill, Landers and Miller (2020) emphasize that employees who received cyber security training were more likely to practice secure behaviors. They were also of the view that the frequency of training was positively correlated with the adoption of secure behaviours.

Similarly, Tsohou, Karyda and Kokolakis (2020) are of the view that the culture of an organization also plays a role in the knowledge and practice of cyber security among their employees. They found out that the organization's culture influenced the employees' attitudes and behaviors towards cyber security. Tsohou et al (2020) believes that organizations with a strong cyber security culture had employees who were more likely to adopt secure behaviours. The level of support provided by the organization also influences the knowledge and practice of cyber security among employees. Haq, Shafique, Yousafzai and Tariq (2020) are of the opinion that employees who received support from their organization were more likely to adopt secure behaviors. The level of support was positively correlated with the adoption of secure behaviors.

One study by Kamal and El-Hadary (2021) finds that the lack of cyber security training, awareness, and education among healthcare professionals is a significant factor that influences the knowledge of cyber security. The study conducted a survey of 352 healthcare professionals including physicians, nurses, and administrative staff, from 11 hospitals in Egypt and the results showed that only 29.8% of the respondents received cyber security training, while 59.4% had no knowledge of cyber security at all. The study showed that the level of cyber security awareness among healthcare professionals in the Egyptian medical sector was generally low.

Another study by Chang et al. (2021) examined the factors that influence the cyber security knowledge and behavior of healthcare workers. The study used a sample of 482 healthcare workers from various healthcare organizations in Taiwan and found that the lack of organizational support, inadequate training, and lack of motivation were significant factors that influenced the knowledge of cyber security. The study suggests that healthcare organizations should prioritize cyber security training for their staff, particularly for older healthcare workers who may have less exposure to cyber security concepts and risks.

Theoretical orientation
The researcher adopts the Health Belief Model (HBM) and Broken Window theory as the theoretical framework for this research work. This is based on the fact that the HBM could be used to understand how individuals perceive the risks and potential consequences of cyber threats, such as identity theft or data breaches. For example, individuals who perceive themselves to be at high risk of cyber-attack (perceived susceptibility) and believe that the consequences of an attack could be severe (perceived severity) are more likely to take steps to protect their online security.

Additionally, the perceived benefits of taking action to reduce the risk of cyber-attacks (such as using strong passwords or regularly updating software) and the perceived barriers to taking such actions (such as inconvenience or lack of knowledge) also play a role in determining whether an individual engages in cyber security behaviors. Overall, the HBM can be a useful framework to guide the design and implementation of cyber security interventions, by identifying the factors that influence individuals' cyber security behaviors and addressing them in a targeted and effective manner.

The Broken Window theory can be applied to suggest that visible signs of neglect in an organization's cyber security practices can lead to an increase in cyber-attacks. For example, if an organization has weak passwords, outdated software, or unpatched vulnerabilities, it may be seen as an easy target for cyber criminals. Therefore, to address this issue, organizations can implement the Broken Window Theory as a theoretical framework to improve their cyber security practices. By taking a proactive approach and addressing small vulnerabilities and weaknesses in their cyber security practices, organizations can send a message that they are vigilant about their security and are not an easy target for cyber criminals.

Methodology

The researcher employs the mixed method design which can be defined as the combination of both quantitative and qualitative research methods in a single study. Mixed methods research design was chosen because it entails collecting information on certain variables in a study population at one point in time using two specific methods of data collection such as the quantitative (questionnaire) and qualitative (interview) methods to arrive at reliable finding(s). Nnamdi Azikiwe University (NAU) medical center is the official Clinic inside NAU-Awka. It has well trained nurses and enough medical facilities for a clinic. The Unizik Medical Center is located close to the school second gate on your way from Awka town. Opposite Glory Chapel church. This is a full-fledged Hospital with facilities for Radiography taking care of students need for X-ray, Medical Laboratory for blood test and the likes, Ambulance services etc. It has various professional workers ranging from doctors to nurses, therapist, technicians, clerical staff, pharmacy staff and the list continues. The total population size for this research is 189. This sample size was arrived at using the total sampling procedure. This sampling procedure involves including all members of a population in the study where the entire population is considered small and manageable in the context of the research topic, scope and resources available.

Two instruments are for the collection of data for the study: questionnaire (which is quantitative) and in-depth interview (qualitative). The questionnaire has structured (close-ended) and unstructured (open-ended) questions. The close-ended questions make it easier for respondents to decide and analyze while the open-ended questions enable the respondents to express themselves more which gives the researcher more insight. The questionnaire consists of different sections. Section A consists of demographic characteristics of respondents such as age, gender, job position and length of employment while other sections centers on substantive issues which are derived from the research questions and objectives of the study.

In-Depth Interview (IDI) with open-ended questions are used to collect qualitative data and it is developed and arranged in line with the objectives of the study.

Data Presentation and Analysis

Table 1: Personal Data of Respondents

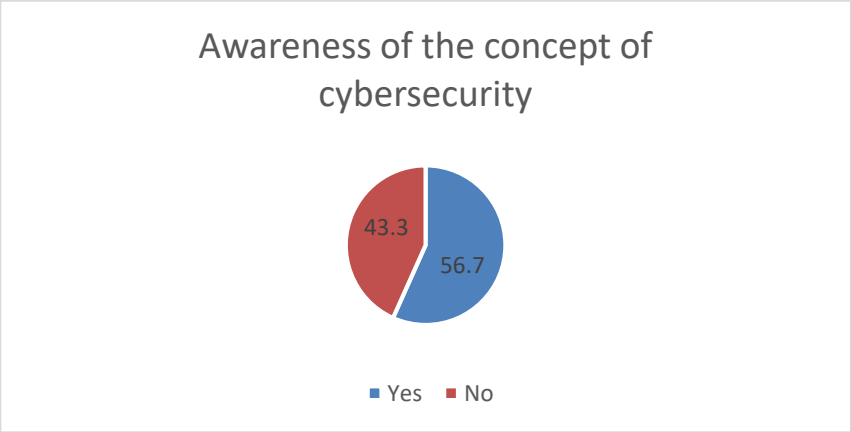
Variable	Frequency	Percentage
Sex		
Male	58	31.0
Female	129	69.0
Total	187	100
Age		
20-25	8	4.3
26-31	23	12.3
32-37	91	48.7
37 and above	65	34.8
Total	187	100
Marital status		
Single	80	42.8
Married	107	57.2
Total	187	100
Role in the medical center		
Admin staff	22	11.8
Nurse	16	8.6
Physician	4	2.1
Med lab technologist	14	7.5
Psychical therapist	9	4.8
Medical receptionist	12	6.4
Others	110	58.8
Total	187	100
Years of experience		

Less than a year	6	3.2
1-5 years	76	40.6
6-10 years	78	41.7
11-15 years	21	11.2
16 years and above	6	3.2
Total	187	100
Religious affiliation		
Christianity	185	98.9
Traditional	2	1.1
Total	187	100

Field Survey, 2024

Table 1 shows that majority of the respondents (69.0%) are females. The table also shows that majority of the respondents (48.7%) are between the ages of 32-37. On the marital status of the respondents, table 1 shows that majority of them (57.2%) are married. Further findings show the different roles of the respondents in their place of work. Majority of the respondents (58.8%) identified others as their role in the medical center. Also, the table shows that majority of the respondents (40.6%) have been employed in their current role for 6-10 years. Finally on religious affiliation, majority of the respondents (98.9%) indicated that they are Christians.

Objective 1: Extent/level of cyber security knowledge among staff of NAU Medical Centre



Filed survey, 2023

Figure 1: Respondents view on their awareness of the concept of cyber security

Figure 1 shows that majority of the respondents (56.7%) are of the opinion that they are aware of the concept of cyber security.

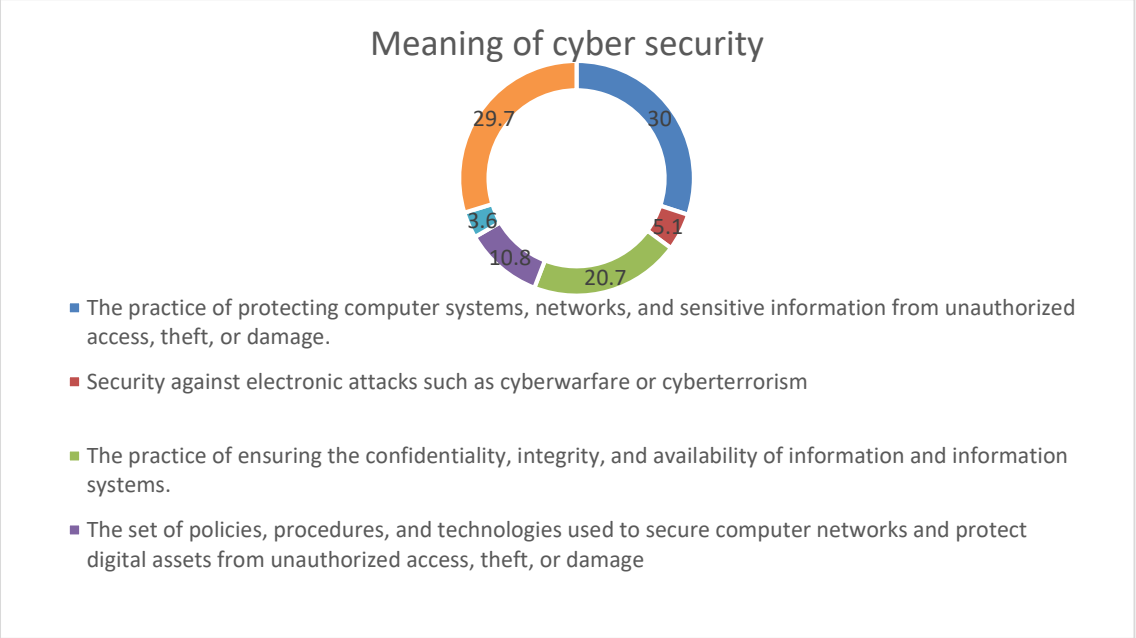


Figure 2: Respondents' view on their understanding of the concept of cyber security.
Figure 2 shows that majority of the respondents (30.0%) indicated that cyber security refers to the practice of protecting computer systems, networks, and sensitive information from unauthorized access, theft, or damage. This aligns with data from the interviews conducted.

One of the interviewees stated:
Cyber security means the actions taken to protect the information stored in computer systems. So it is designed to keep information and details safe in the cyber space especially university information as we have them here (Female, 36, married, Nurse).

Another interviewee stated:
Yes I know what cyber security entails. I am very much aware of this. It basically involves ensuring that the details we have online and in our computers are kept safe from intruders (Male, 40, married, med lab technologist).

Objective 2: Factors influencing the knowledge and practice of cyber security in NAU Medical Centre.

Table 2: Respondents' level of experience in cyber security

Responses	***Frequency***	***Percentage***
Expert	1	0.5
Beginner	66	35.3
Advanced	2	1.2
Intermediate	48	25.7
No experience	70	37.4
Total	187	100

Table 2 shows that majority of the respondents (37.4%) indicated that they have no cyber security experience while 35.3% of them indicated that they are beginners in the field of cyber security. This is supported by data from the IDI.

Another interviewee stated:
I honestly don't have enough knowledge on the issue of cyber security because I have not been thought by anyone at my place work. If we have been thought it would have been easier to understand and even put to practice in several occasions (Female, 31, married, nurse).

Another interviewee stated:
There is no experience o, we have been doing our things our way. Personally, I don't believe that cyber security is easy to learn because it is for the experts to take care of in the workplace (Male, 37, married, therapist)

Table 3: Respondents' view on the factors influencing the knowledge and practice of Cyber security in NAU Medical Center

Responses	*Frequency*	*Percentage*
Training and education	65	34.7
Leadership and management	25	13.3
Incentive and rewards	27	14.4
Compliance and regulations	30	16.0
All of the above	40	21.4
Total	187	100

Table 3 shows that majority of the respondents (34.7%) identified training and education as the factor influencing the knowledge and practice of Cyber security in NAU Medical Center. This is supported by data from the IDI.

One of the interviewees stated:
Like I mentioned earlier, training and education is lacking so it is the major factor in this place, in my opinion. We have no training and education on cyber security in this place. It appears that it is very necessary but there has not been any kind of training and education for us so it continues to prevent the progress needed in that area (Female, 31, married, nurse).

Another interviewee stated:
Cyber security requires education and training which is lacking. Also, there are no regulations and rules properly stipulated for adherence. I believe this can be corrected (Female, 40, married, medical receptionist).

Discussion of Findings

The study examined the factors that influence employees' knowledge and practice of cyber security at NAU medical center. The study found that cyber security refers to the practice of protecting computer systems, networks, and sensitive information from unauthorized access, theft, or damage. This aligns with the findings from the study of Adeleke and Olugbara (2021. The study looked at the factors influencing the knowledge and practice of cyber-security in NAU medical center. It was found that training and education is the major factor influencing knowledge and practice of cyber security in NAU medical center. This also aligns with the data from the study conducted by Adeleke and Olugbara (2021.

Recommendations

Based on the findings of this study, the following recommendations are made:
1. Regular cyber security training sessions should be provided for all employees.
2. Encryption of sensitive patient's data to protect it from unauthorized access
3. Multi-factor authentication for all employees
4. Implementation of access control policies and procedures.

References

Adeleke, J. O., & Olugbara, O. O. (2021). Assessing Cyber Security Knowledge Among Healthcare Staff in a Tertiary Hospital: A Case Study in Nigeria. *Journal of Healthcare Informatics Research, 5*(2), 89-102.
Ahmed, Z., Zeki, A. M., & Al-Ameen, Z. (2021). Cybersecurity in Healthcare: A Comprehensive Review. *Journal of Information Security and Applications, 62*, 102847.
Al-Saggaf, Y., & Islam, R. (2018). Cybersecurity education in the digital age. *Education and Information Technologies, 23*(6), 2703-2721.
Caudill, J. G., Landers, T. L., & Miller, C. L. (2020). The Effects of Cybersecurity Training on Cybersecurity Behavior. *Journal of Applied Security Research, 15*(3), 351-369.
Chai, E. (2021). Cyber security: Protecting the digital world. *International Journal of Network Security & Its Applications, 13*(3), 65-72.
Chang, S. H., Shih, S. P., Hsu, M. F., Chen, J. S., & Lai, C. F. (2021). Exploring the factors influencing the cybersecurity knowledge and behavior of healthcare workers. *Information Systems Frontiers, 23*(1), 61-75.
DePietro, R. A., & Kimmel, S. R. (2018). Knowledge of cybersecurity among healthcare professionals. *Journal of Hospital Administration, 7*(3), 27-33.
Ghosemajumder, S. (2017). Overconfidence and cyber security: A dangerous combination. *Journal of Information Security, 9*(2), 87-94.
Gilheany, S. (2017). Cyber security: An essential component of modern computing. *Journal of Computer Security, 25*(1), 45-56.

Göktas, H., & Celik, A. (2020). Cybersecurity awareness in hospitals: An empirical study. *International Journal of Healthcare Management, 13*(4), 299-305.
Green, T. (2016). The impact of technology on global cyber crimes. *International Journal of Cyber Criminology, 10*(2), 110-125.
Haq, M., Shafique, F., Yousafzai, S., & Tariq, A. (2020). Cybersecurity at the workplace: Role of organizational support. *Journal of Public Affairs, 20*(4), e2123.
HIMS Analytics. (2017). Cybersecurity Preparedness in Healthcare: An HIMSS Analytics Study. HIMSS Analytics.
Kamal, E., & El-Hadary, M. (2021). Cyber Security Awareness Among Healthcare Professionals in Egypt: A Cross-Sectional Study. *Journal of Medical Internet Research, 23*(2), e26629.
Kostyuk, N., & Wayne, L. (2019). Consequences of poor cyber security practices: A review. *Journal of Computer Information Systems, 59*(4), 320-333.
Maisikeli, P. (2020). Understanding cyber security: Myths and realities. *Journal of Information Assurance & Cybersecurity, 15*(3), 78-91.
Maisikeli, P. (2020). Understanding Cyber Security: Myths and Realities. *Journal of Information Assurance & Cybersecurity, 15*(3), 78-91.
Olumide, E. A., Oyeyemi, A. O., & Olawumi, T. O. (2021). Cyber Security Practices Among Healthcare Workers in a University Teaching Hospital: A Case Study in Nigeria. *Journal of Information Security and Cybercrimes, 1*(1), 32-46.
Oyeyemi, A. O., Adeniyi, A. O., & Olawumi, T. O. (2020). Assessment of Cybersecurity Knowledge Among Hospital Workers in a Tertiary Hospital: A Case Study in Nigeria. *Journal of Healthcare Informatics Research, 4*(4), 147-162.
Ponemon Institute. (2020). Cost of a Data Breach Report 2020. Ponemon Institute.
Sittig, D. F., & Singh, H. (2016). A New Socio-technical Model for Studying Health Information Technology in Complex Adaptive Healthcare Systems. *Quality & Safety in Health Care, 25*(1), 7-11.
Smith, R. (2017). Cyber security awareness among Nigerian workers. *International Journal of Cyber Security and Digital Forensics, 6*(1), 24-37.
Smith, R. (2017). Cyber Security Awareness Among Nigerian Workers. *International Journal of Cyber Security and Digital Forensics, 6*(1), 24-37.
Tsohou, A., Karyda, M., & Kokolakis, S. (2020). A cyber security cultural perspective on employees' behavior. *Journal of Computer Information Systems, 60*(4), 327-336.