ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP714

An Examination of Threats and Countermeasures Relating to Healthcare Cyber Risks: The Case of Kenyatta National Hospital

Stephen Okongo Ario[1]; Dr. Jecton T. Anyango[2]; Jenu John[3]
[1.] MSc. Computer Information Systems Kenya Methodist University (KEMU)
[2.] Lecturer, Department of Computer Science KEMU University.
[3.] Lecture, KEMU University.

Abstract

➢ ***Background***

Africa has seen an exponential increase in internet penetration and ICT affordances since the turn of the twenty-first century. Healthcare institutions are scrambling to put in place the appropriate safeguards to protect their patients' data from unauthorized access since the need to protect private information has become critical, particularly for cybercriminals eyeing the data of medical patients. This thesis investigates cyber security threats and countermeasures in healthcare, with a focus on Kenyatta National Hospital (KNH). Given Africa's increased internet use and the critical need to protect patient data from cybercriminals, the study explores how data protection and cyber security influence healthcare delivery at the hospital.

➢ ***Key Objectives***

To examine cyber threats and countermeasures employed by KNH as well as analyzing the impact of Kenya's Cybercrime Act.

➢ ***Results***

The survey at Kenyatta National Hospital shows strong cybersecurity measures, with 89% having dedicated resources and 88% using computers regularly. Regarding the Kenya Cybercrime Act, 74% know how to detect and report hacks, though 8% have encountered malware and 12% lack basic malware knowledge. 78% have anti-virus software, and 63% verify email attachments, while knowledge of social engineering and email scams is limited, revealing a need for further education. The second objective looked at the impact of Kenya Cybercrime Act, as a local data protection laws on supporting patient-healthcare system at Kenyatta National Hospital. A significant majority, 74%, are aware of when their computer is hacked or infected and know whom to contact in such cases. The results also show that 79% of respondents have never encountered a virus or trojan on their computers. When opening email attachments, 63% of respondents always verify that the attachment is from a known and expected source. Knowledge of social engineering attacks is limited, with only 18% of respondents aware of these threats and 82% unfamiliar with them. Regarding email scams, 51% do not know what an email scam is or how to recognize one, underscoring a need for further training. Finally, while 85% of respondents believe their computers are not valuable to hackers, 15% recognize their potential as targets, reflecting differing perceptions of risk and emphasizing the need for ongoing cyber security education.

Keywords:- *Cyber Threats, Cybercrime, Cyber Security*.

I. INTRODUCTION

Sarker et al. (2020) stated that a number of security incidents, including malware attacks, phishing scams, denial of service attacks, malware attacks, unauthorized access, and zero-day attacks, have increased in frequency in recent years due to the growing reliance on digitalization and the Internet of Things (IoT). For instance, the security industry was aware of fewer than 50 million distinct malware executables in 2010, but by 2019, that figure had skyrocketed to almost 900 million dangerous executables.

Countless economic and social operations are rapidly being digitized as internet technology evolves. Internet banking, interactive sites, healthcare networking and data storage, smart metering, and corporate platforms are just a few examples of digital data-driven activity. The volume and rate at which digital information is produced and preserved is expanding at a rapid pace. Although most content is insignificant, a significant chunk contains salient information or personally identifiable information (PII) which must be safeguarded. Scholars have consented that to keep data confidential, explicit physical and digital cyber security defenses are required (Seemma, Nandhini & Sowamiya, 2018).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP714

Turner (2018) asserts that while the Internet has made the world smaller, it has also made us more aware of viewpoints that were previously less varied and challenging. Hacking has also quickly gained traction among cybercriminals and evolved at a similar pace to security. Seemma, Nandhini, and Sowamiya (2018) contended that there are many contradictions and ambiguities surrounding the idea of security, which can be understood as a process rather than an end in and of itself. It is the process of maintaining a suitable level of risk, and an organization cannot be considered safe at any point after the most recent confirmation that it is complying with its security plan (Rosenzweig, 2013).

Hardware, software, and data that are enabled by the internet have taken on the responsibility of protecting cyber security from cyber-attacks. Cybersecurity is a branch of security that aims to ensure data availability, confidentiality, and integrity (Rohrer & Hom, 2017). Accordingly, McKenna (2017) agreed that cyberspace is the environment in which communication over networks of computers takes place, and that the vast majority of people on the planet are connected to and interact with every aspect of society, including the government, courts, legislators, law enforcement, police stations, banks, infrastructure, healthcare, and educational institutions in addition to schools and students.

Due to the increasing reliance of most areas of modern life on digital networks, cybercrime is becoming a greater threat to both individuals and enterprises. As a result, there is an annual growth in the amount of data collected and kept electronically, which provides hackers with greater and greater motivation. Increased reliance on online platforms like social media, e-commerce, and online banking greatly increases the potential entry point into related technical networks, which promotes an exponential increase in theft, bribery, and information fraud. According to GyunNo and Vasarhelyi (2017), cyber security is the protection of systems, networks, and technologies through the use of technology, policies, and processes. It is crucial to remember that information security and information assurance should be considered when conceptualizing cyber security.

Renatta (2020) states that the idea of cyber security has drawn interest from all societal stakeholders worldwide. The United States has integrated electronic systems into its healthcare delivery system as a result of technological advancements. Patients now receive higher-quality care thanks to the usage of electronic health records, telemedicine, and other technical innovations. However, as technology has become more integrated, cyber threats to healthcare systems have increased, raising the risk of data breaches, sensitive information loss, and patient injury.

Cybersecurity lapses in healthcare systems may result in the loss of private patient information, interruptions of medical care, monetary losses, and harm to the standing of healthcare institutions. Cyberattacks can also jeopardize patient safety and result in physical injury to patients. Strong cyber security measures are unquestionably necessary for healthcare companies to preserve the quality of patient care, protect patient confidentiality, and preserve the integrity of their systems (Seemma, Nandhini & Sowamiya, 2018).

According to Kahyaogl and Caliyurt (2018), digital technology is becoming more and more important in healthcare, which has enhanced patient care, decreased expenses, and boosted efficiency. But this reliance on technology has also left healthcare providers open to cyberattacks, which can have serious negative effects on their finances, legal standing, and reputation in addition to perhaps jeopardizing the health and safety of their patients.

Kenya, like many other nations, has a lot of cybersecurity challenges. Organizations in the public and commercial sectors are finding it difficult to stay up to date with the changing threat landscape as a result of the increasing frequency and sophistication of cyberattacks. The government has improved cybersecurity in the nation by taking a number of actions. To operate as the primary point of contact for cybersecurity issues in the nation, the government established the National Kenya Computer Incident Response Team Coordination Center (National KE-CIRT/CC) in 2014. The center is in charge of organizing countermeasures to cyberattacks and giving impacted organizations support and information (Renatta, 2020).

At 1800 beds spread across 50 wards, Kenyatta National Hospital (KNH) is the largest teaching and referral hospital in East and Central Africa. It also boasts 24 theaters, 22 outpatient clinics, and a sizable ER. It serves 70,000 inpatients and 520,000 outpatients annually on average with 4,600 staff members. It was founded in 1901, and in 1987 it gained some degree of autonomy as a state corporation. The hospital has its own management, as well as medical and support personnel, and is overseen by a Board of Directors. According to the 2018 Kenyatta National Hospital (KNH) annual report and financial statement, the hospital is to be used as a teaching institution by the University of Nairobi under a Memorandum of Understanding (MoU).

It was a major role in the regional health sector when it was founded in 1901. "To be a world class hospital in the provision of innovative and specialized healthcare," states its mission. As stated in its mandate, it is essential to the healthcare delivery systems in the nation, East Africa, and other African countries (Willis, 2015). Referral cases for specialized healthcare are received by the hospital from both domestic and international sources, thanks to its very efficient and successful referral system.

Alongside hospital specialists, the teaching staff is responsible for referrals and consultations under that memorandum of understanding. As the nation's premier referral hospital, it accepts patients from all regions of the

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP714

nation; however, the second national referral hospital, located in Eldoret, almost 400 kilometers northwest of Nairobi, serves the provinces of North Rift, Nyanza, and Western. Additionally, KNH sees patients from abroad.

Individuals who believe they will receive the greatest care due to the highest concentration of physicians and medical specialists as well as the availability of amenities not present in lower-level health facilities are also admitted there; these individuals are not referred by other hospitals or physicians. As a result, KNH sees so many patients that it is unable to accommodate them all. It takes seven to nine hours on average for a patient who arrives at the casualty/emergency unit to be admitted to the Private Wing. Patients passing away in the waiting room before receiving medical care is not shocking (Kenyatta National Hospital (KNH) strategic plan, 2018–2023).

Kenyatta National Hospital has six thousand workers. The private wing has 209 bedrooms, out of a total of 1800 beds (Abdulla, 1985). Every day, Kenyatta National Hospital sees between 2000 and 3000 patients. 1157 healthcare professionals work in the hospital, comprising 100 physicians, 800 nurses, 130 pharmacists, 70 LT, 50 CO, and 5 dentists. Two accountants serve in the administrative division (Willis, 2015).

Schlosberg (2021) defines cyber-security as a set of procedures for protecting computer-related technologies, documents, and systems against unauthorized access, modification, and destruction by employing tactics that either lessen the effects of cybercrime or eventually eradicate it completely. Undoubtedly, cybercrimes directed towards the healthcare industry are on the rise. Numerous hospital records are pilfered by hacking, ransomware, and insider threats, among other techniques (Williams & Woodward, 2015).

Africa has seen an exponential increase in internet penetration and ICT affordances since the turn of the twenty-first century. Saaleh (2022) reports that Internet usage has increased dramatically in Africa. Over 570 million people on the continent used the internet in 2022—a number that had more than doubled since 2015. Nigeria, the most populous nation in Africa, has the highest proportion of users. This adds up to more than 100 million overall, of which 76 million are in Egypt and 41 million are in South Africa. Internet connectivity has expanded across Africa in recent years due to advancements in telecommunications architecture and a growing rate of smartphone usage. As a result of increased internet connectivity, digital operations and services such as social networking sites, e-commerce, and mobile banking have grown in popularity. Yet, the continent has not yet fully realized its digital capabilities. Despite the growing number of users, the internet penetration rate was approximately 43 percent.

This astounding rise has been attributed to developments like the deregulation of markets in the African telecommunications sector, the increased diversity of mobile telecommunications technology, and the increasing prevalence of broadband bandwidth (Global System for Mobile Communications Association, 2013). This trend is anticipated to continue in the future (Global System for Mobile Communications Association, 2016). However, worries regarding the need to bolster cyber security laws and cyber integrity across the continent have been raised by the spread of ICTs and Internet usage in Africa. Network and computer system security is a technological consideration. The organizational viewpoint is concentrated on creating institutional capacity to support cyber security, including the formation of Computer Emergency Response Teams (CERTs) and law enforcement institutions. Policies include laws that prohibit actions that compromise data availability, integrity, and protection as well as initiatives to promote international collaboration (Gercke, 2016).

Healthcare institutions are scrambling to put in place the appropriate safeguards to protect their patients' data from unauthorized access since the need to protect private information has become critical, particularly for cybercriminals eyeing the data of medical patients. This is because there are several examples of cybercrimes in the healthcare sector that have resulted in unheard-of losses and harm to reputations. Perhaps the biggest referral hospital in East Africa, Kenyatta National Hospital manages a lot of data for its patients. There is no denying the necessity of a complex and efficient cyber security architecture. This is to stop data breaches, which are incredibly profitable for fraudsters.

II. METHODOLOGY

The present research adopted the use of a mixed method research approach which brings out the mathematical inferences like percentages, means, and others as well as the lived experiences of the respondents at the Kenyatta National Hospital. Furthermore, by using a mixed method, the researcher was able to incorporate in-depth interviews, a quantitative survey, and both qualitative and quantitative data collection techniques. "Drawing together multiple types of evidence gathered from different sources using different methods of data collection" is how Barker (1999) describes a mixed approach (p. 483). Mixed methods improve the "validity of research and its findings," as noted by Ezzy (2013) (p. 38). The population for this study consisted of 6000 employee at Kenyatta National Hospital and a sample of 384 employees were interviewed. A questionnaire was used for data collection. Both descriptive and inferential statistics was applied for the research. Ethical approval was done by the department of library science of the Kenya Methodist University as well as the National Commission for Science Technology and Innovation (NACOSTI) which is mandated with the responsibility of protecting human subjects in research will be sought. All respondents who voluntarily

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP714

accepted to participate were informed of the reason for conducting this research before being given the questionnaire to fill. All participants were also debriefed about the purposes for the research and the benefits accruing thereof. The debrief form contained information regarding confidentiality and the anonymity of the participants.

III. RESULTS

- *Demography*

The study achieved a high response rate of 94.8%, with 365 completed questionnaires out of 370 distributed. Respondents spanned a diverse age range, with the largest group being 41-50 years old (30%), followed by those aged 51-60 years (25%) and 31-40 years (23%). The youngest age group (21-30 years) accounted for 10%, while 12% were 61 years and older. In terms of gender distribution, 58% of respondents were male (210 individuals) and 42% were female (155 individuals). Educational backgrounds varied, with 47% holding a Bachelor's degree, 24% having vocational training, 21% possessing a Master's degree, 6% having secondary education, and 3% with a PhD. Respondents' positions within their organizations were also diverse: nurses represented the largest group at 33%, followed by doctors at 18%, administrative personnel at 17%, auxiliary personnel at 13%, lab personnel at 10%, technical personnel at 7%, and other roles at 3%. This demographic distribution provides a comprehensive view of the study's participants, highlighting their varied backgrounds and roles within the healthcare system.

- *Threats and Counter Measures in Healthcare Cyber Risk*

The study on cybersecurity and data protection at Kenyatta National Hospital reveals several crucial insights into the hospital's approach to managing cyber risks. A significant majority of respondents (89%) confirmed that their organizations have either a dedicated cybersecurity department or utilize external cybersecurity services, indicating a strong commitment to safeguarding digital assets. However, 10% reported the absence of such resources, and 1% were unsure, suggesting potential vulnerabilities and gaps in cybersecurity strategies. In terms of computer usage, 88% of respondents indicated that they work on computers regularly, reflecting the essential role of digital technology in their professional tasks. On the other hand, 12% do not use computers, which may be indicative of varying job functions within the hospital.

Regarding data protection training, a substantial 70% of respondents have not received training on the General Data Protection Regulation (GDPR), highlighting a significant gap in critical knowledge that could increase vulnerability to data breaches and regulatory non-compliance. Conversely, 30% of respondents have received GDPR training, pointing to some level of awareness but also emphasizing the need for broader education. The study also found that 75% of respondents have access to sensitive patient data, underscoring the importance of stringent data protection measures. The remaining 25% do not handle patient data, suggesting their roles are less directly involved with confidential information. Awareness of cybersecurity policies is notably high, with 85% of respondents reporting that their hospital has established such policies, demonstrating a commitment to formal cybersecurity measures. However, 12% are unsure whether their hospital has these policies, indicating a potential gap in communication regarding the existence and importance of cybersecurity protocols.

- *Impact of Kenya's Cybercrime Act on the Patient-Healthcare System*

A substantial majority of respondents (74%) demonstrated a strong awareness of computer security issues, knowing when their computers are hacked or infected and whom to contact. This high level of preparedness indicates effective training and awareness programs. However, 12% of respondents knew how to report a hack but lacked recognition skills, and 10% had partial understanding, while a small group (4%) had neither awareness nor knowledge of response procedures, highlighting a need for further education and readiness enhancement.

Regarding virus or trojan infections, 79% of respondents reported that their computers had never been infected, suggesting robust security measures. However, 8% experienced malware infections, and 12% lacked basic understanding of malware, emphasizing the need for improved training on basic cyber security concepts. In terms of anti-virus software, 78% of respondents had it installed, reflecting a commitment to maintaining computer security. Yet, 15% did not have anti-virus software, and 7% were unaware of its status, indicating gaps in essential security measures and the need for better communication.

When handling email attachments, 63% of respondents consistently ensured attachments were from known and expected sources, showing a cautious approach. However, 27% opened attachments from known sources without full scrutiny, and 10% exhibited less caution, revealing varying levels of vigilance and a need for standardized procedures. Awareness of social engineering attacks was low, with only 18% of respondents understanding these threats. The majority (82%) lacked knowledge about social engineering, indicating a critical area for increased education. Regarding email scams, 29% of respondents knew what an email scam is and how to identify one, while 21% understood what scams are but lacked identification skills. Over half (51%) were unfamiliar with email scams, highlighting a significant knowledge gap that needs addressing. Lastly, 85% of respondents believed their computers were not valuable to hackers, reflecting a general sense of security. However, 15% recognized potential risks, suggesting that while most felt secure, there is a need for ongoing education and awareness about the potential threats to ensure comprehensive cyber security.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP714

IV. DISCUSSION

The results from the survey at Kenyatta National Hospital and the literature highlight the importance of cyber security measures. The survey shows a strong emphasis on security with 89% confirming the presence of a dedicated cyber security department or external services. Similarly, the literature emphasizes the importance of robust cyber security frameworks, laws, and standards like the Computer Misuse and Cybercrimes Act, 2018 (CMCA), and the National Cyber security Framework by the Communications Authority of Kenya (CA) (Communications Authority of Kenya, 2020).

Results also indicates that 70% of respondents have received GDPR training, demonstrating strong awareness of data protection regulations. This aligns with the literature's emphasis on cyber security capacity building, which involves training, awareness-raising, and education programs to enhance cyber security skills and expertise (Choi, Johnson, & Lee, 2020; Elshenawy et al., 2021). Both the survey findings and the literature discuss the presence of regulatory frameworks guiding cyber security measures. The survey notes established cyber security policies known by 85% of respondents, while the literature outlines various laws and guidelines like KICA, CMCA, and the National ICT Policy Guidelines, 2020, which aim to protect critical information infrastructure and sensitive information (Kenya Information and Communications (Amendment) Act, 2018).

While literature discusses the significant risks and financial implications of data breaches in healthcare, such as financial fraud, information loss, and system intrusions. The survey underscores the critical role of digital tools in healthcare work, with 88% of respondents using computers regularly, highlighting the necessity for stringent data protection measures in healthcare settings (Perakslis, 2014; Ponemon, 2016). The results from the survey at Kenyatta National Hospital shows a high level of cyber security implementation (89% having cyber security departments or services), the literature suggests that many healthcare institutions, especially in developing nations, often lag behind in implementing robust cyber security measures. This discrepancy may highlight a specific success at Kenyatta National Hospital compared to broader trends (Kaplan, Davidson, Demiris, Schreiber & Waldman, 2019; Kruse, Frederick, Jacobson & Monticone, 2017).

It was also revealed that 12% of respondents are unsure about the presence of cyber security policies, and 30% have not received GDPR training, suggesting gaps in communication and training. The literature, however, tends to emphasize the existence of comprehensive frameworks and guidelines without delving deeply into the gaps in implementation or awareness within specific institutions (Abdullah et al., 2020). This survey provides a focused view of Kenyatta National Hospital, while the literature encompasses a broader perspective, including the overall cyber security landscape in Kenya and developing countries. The literature discusses challenges in cyber security adoption in small and medium-sized enterprises and underfunded healthcare systems, which may not be as evident in the survey's more focused context (Almutairi et al., 2020; Elshenawy et al., 2021).

Past studies provides detailed insights into specific cyber security threats, such as financial fraud, identity theft, and risks to patient safety due to cyber-attacks. It also outlines specific measures like using shredders for private data disposal and network firewalls. The survey, however, does not provide detailed information on the specific types of threats encountered or the particular measures in place at Kenyatta National Hospital (Weerasinghe *et al.*, 2020).

A notable majority (74%) of respondents at Kenyatta National Hospital reported being aware of computer hacks or infections and knowing whom to contact in such situations. This high level of awareness reflects the effectiveness of training and awareness programs, as emphasized in studies by Choi, Johnson, and Lee (2020) and Kaplan et al. (2019), which underscore the necessity of investing in cyber security education and infrastructure. However, the presence of a small proportion (4%) of respondents who lack awareness and procedural knowledge highlights a critical gap that can leave individuals vulnerable during security breaches. This gap aligns with findings by Abdullah et al. (2020) that inadequate cyber security measures increase the likelihood of data breaches in developing nations.

The majority of respondents (79%) reported that their computers have never been infected by a virus or trojan, suggesting effective security measures are in place. This is consistent with the literature indicating that robust cyber security practices can significantly reduce the incidence of malware infections (Perakslis, 2014; Kruse et al., 2017). However, the fact that 8% of respondents have experienced malware infections and 12% are unaware of what a virus or trojan is indicates a need for ongoing vigilance and enhanced education on basic cyber security concepts. These findings mirror the concerns raised by Weerasinghe et al. (2020) about the detrimental impact of compromised patient information on healthcare quality. A substantial majority (78%) of respondents confirmed having anti-virus software installed on their computers, reflecting a strong commitment to maintaining computer security. This aligns with the recommendations by Almutairi et al. (2020) on the necessity of implementing cybersecurity measures despite the high costs. However, the 15% of respondents without anti-virus software and the 7% who are unsure about its presence highlight areas for improvement in communication and enforcement of security protocols.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP714

The survey revealed that 63% of respondents always ensure an attachment is from a known and expected source before opening it, demonstrating a cautious approach towards email security. This is crucial in avoiding potential threats such as phishing and malware, as discussed by Elshenawy et al. (2021). However, the 10% of respondents who open attachments without scrutiny and the 27% who rely solely on recognizing the sender indicate varying levels of risk awareness. These findings highlight the need for continued education on safe email practices to mitigate cybersecurity threats.

The low awareness of social engineering attacks (18%) and email scams (29%) among respondents underscores a critical gap in understanding these common cyber threats. This is consistent with the literature, which points out the need for enhanced training and education on identifying and responding to such attacks (Almutairi et al., 2020). The significant majority (82% and 51%, respectively) of respondents who lack awareness about these threats reflect the broader challenges faced by healthcare institutions in developing nations, as described by Kaplan et al. (2019). The belief among 85% of respondents that their computers have no value to hackers indicates a widespread misconception about the potential risks. This perception can lead to complacency and a lack of vigilance, as noted by Schmeelk, Dragos, and Debello (2021). The literature emphasizes that all digital systems, regardless of perceived value, can be targeted by cybercriminals, necessitating comprehensive cybersecurity measures (Ponemon, 2016).

V. 5.0 CONCLUSION AND FUTURE

The study identified significant threats to healthcare cyber risk at Kenyatta National Hospital, including potential vulnerabilities due to inadequate GDPR training and varying levels of awareness about social engineering attacks and email scams. Despite having a dedicated cybersecurity department or external services, the findings indicate that gaps in data protection protocols and training need to be addressed. Implementing comprehensive training and awareness programs will enhance the hospital's ability to counter cyber threats effectively.

The Kenya Cybercrime Act has positively impacted the hospital's cybersecurity by improving preparedness and understanding among staff. The majority of respondents were aware of how to handle cyber incidents and reported effective malware protection. However, low awareness of certain cyber threats and varied training effectiveness suggest that while the Act provides a solid foundation, there is a need for continued efforts to strengthen staff knowledge and preparedness.

REFERENCES

[1]. Abdullah, A., Alzahrani, A. I., Altameem, A., & Alelyani, S. (2020). Cybersecurity risks and data protection in healthcare sector: A systematic review. *Journal of Healthcare Engineering, 2020*.

[2]. Almutairi, S. K., Alharbi, A. A., Aljohani, N. R., Alharbi, R. M., Almutairi, A. R., & Alzahrani, N. A. (2020). Factors affecting the adoption of cybersecurity in healthcare sector in Saudi Arabia. *Journal of Healthcare Engineering, 2020*

[3]. Barker, C. (1999). *Television, globalization and cultural identities (pp. 84-93).* Buckingham: Open University Press.

[4]. Choi, S. J., Johnson, M. E., & Lee, J. (2020). An event study of data breaches and hospital IT spending. *Health Policy and Technology*, 9(3), 372-378.

[5]. Elshenawy, R., Ahmed, A., Hassanien, A. E., & Elsalamony, H. A. (2021). Patients' perception of health information privacy and security: An empirical study from Egypt. *Journal of Medical Systems*, *45*(1), 1-12.

[6]. Ezzy, D. (2013). *Qualitative analysis.* London, UK: Routledge.

[7]. Gercke, 2016). Understanding Cybercrime: A Guide For Developing Countries. Retrieved from https://biblioteca.cejamericas.org/bitstream/handle/2015/3697/Understanding_Cybercrime_Developing_Countries.pdf?sequence=1&isAllowed=y

[8]. Kahyaoglu, B. & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial auditing journal*, 33(4), 360-376.

[9]. Kaplan, B., Davidson, E. J., Demiris, G., Schreiber, R., & Waldman, A. E. (2019). Rethinking health data privacy. In *Proceedings of the American Medical Informatics Association Annual Symposium*, Washington, DC.

[10]. Kenya Information and Communications (Amendment) Act (2018). The Kenya Information And Communications Act Chapter 411A. Retrieved June 24th 2024 from https://infotradekenya.go.ke/media/Kenya%20Information%20Communications%20ACT.pdf

[11]. Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1-10.

[12]. McKenna, S. (2017). "The Design Activity Framework: Investigating the Data Visualization Design Process." PhD diss., The University of Utah, 2017.

[13]. Perakslis, E. D. (2014). Cybersecurity in health care. *N Engl J Med*, 371(5), 395-397.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP714

[14]. Schmeelk, S., Dragos, D., & Debello, J. (2021). What Can We Learn about Healthcare IT Risk from HITECH? Risk Lessons Learned from the US HHS OCR Breach Portal. Retrieved from https://scholarspace.manoa.hawaii.edu/items/da525b5f-ddda-4889-ac2f-8317bb8b965b

[15]. Woodward, A., & Williams, P. A. (2015). An uncomfortable change: Shifting perceptions to establish pragmatic cyber security. In Recent Advances in Information and Communication Technology 2015: Proceedings of the 11th International Conference on Computing and Information Technology (IC2IT) (pp. 1-8). Springer International Publishing.