Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/18002
DOI URL: http://dx.doi.org/10.21474/IJAR01/18002

RESEARCH ARTICLE

"THE NETWORK SECURITY (NS) OF HEALTHCARE ANDMEDICAL FACILITIES: AN ANALYTICAL OVERVIEW OF THE EMERGING CYBERSECURITY THREATS/RISKS AND COUNTERMEASURES"

Mohamed Qasim Mohamed Alomari[1] and Fatema Jaber Ali Alshowaikh[2]

1. Halwan University- Egypt.
2. Mutah University- Jordan.

Manuscript Info

Manuscript History
Received: 15 October 2023
Final Accepted: 18 November 2023
Published: December 2023

Key words:-
Security Network, Information Technology, Cybersecurity, Cyberattacks, Cyber Threats & Risks, Digital Transformation, Countermeasures

Abstract

This research study discusses key issues concerning the Network Security (NS) of the healthcare and medical facilities. Particularly, it aims to shed light on the emerging cybersecurity threats and risks encountered by these facilities and the proposed countermeasures that can prevent, detect and respond to security threats (e.g., cyberattacks), vulnerabilities, and risks (e.g., financial or operational risks), and can serve to mitigate any damages and/or disruption caused by the exposure to any of the aforesaid incidents. In the current qualitative study, the researcher adopted the 'Analytical Approach' as the research method that was utilized for the sake of gathering, analysing, interpreting the available literature of the subject -under investigation-, and eventually making inferences and reaching conclusions. Based on carrying out the previously-mentioned 'Analytical Literature Review', several findings were revealed by this study. Precisely, the study demonstrated that due to the 'Digital Transformation' and the 'Digitization' adopted by the healthcare sector, the vulnerability and fragility of the healthcare and medical facilities' security networks and information/operational systems have been increased. Such deficit in the cybersecurity level had eventually led to the exposure of these facilities to several types of cyberattacks, network penetration, and many other cybercrimes. The findings of the study also demonstrated that the cyber threats can take the forms of: 'Malware', 'Ransomware', 'Phishing', and 'Insider Threats'. Similarly, the cyberattacks' types include 'Network Attacks', 'Wireless Attacks', 'Malware Attacks', and 'Social Engineering Attacks'. Finally, the study revealed several cyberattacks' countermeasures, include: 1) Raising the awareness of the healthcare and medical facilities' workforce; 2) Keeping the organizations' software and systems fully up to date; 3) Implementing 'Endpoint Protection Software'; 4) Installing a Firewall; 5) Backup the organizations' data; 6) Securing the organizations' Wi-Fi network; and 7) Managing the healthcare and medical facilities employees' personal accounts. Further countermeasures include the implementation of 'Risk Assessment', 'Authentication', 'Data Retention'.

Corresponding Author:- Mohamed Qasim Mohamed Alomari
Address:- Halwan University- Egypt.

……..

Introduction:-

In today's digitally interconnected world, a lot of valuable opportunities brought about by the rapid advancement and the integration of modern technology into almost every aspect of our daily lives and which eventually led to an achievement of a quantum leap forward by all mankind. Nonetheless, this transformative process has led to the emergence of unprecedented challenges that have started to pose a real risk to human's' safety and welfare. Truly, the latest trends in today's high-tech sphere, including the rapid growth of technologies and the latest technological breakthroughs, had been accompanied by that multifaceted cyber risks and threats that affected all sectors and industries in all societies ona global scale (Zarour, et al., 2021).

By the same intimation, Bendovschi indicated that in this age of technology, which represents the dawn of the global information revolution, 'Social Media Networks and Applications', 'Internet Commerce' (Also referred to as 'Online Transactions'), and multi-purposes 'Automated Processes' have become the prominent features of this era. Additionally, technology is advancing quickly and in contrast cybercrimes are also advancing on the same rapid pace, which create novel types of cyberattacks through which cybercriminals have become capable of breaching highly-secured and complex information systems and security networks and eventually cause catastrophic damages to their targeted victims and sometimes remain untraceable (ibid: 2015).

Similarly, Möller (2020) asserted that many advanced innovations and new technologies (e.g., the 'Artificial Intelligence', 'Blockchain', 'Cloud Computing', the 'Internet of Things', etc.), have been adopted by the majority of organizations across all industries and sectors. Furthermore, this adoption has triggered the emergence of the state of 'Digital Transformation' (DT is defined as the adopting digital solutions in the course of action and workflow of organizations) worldwide. As per to the extensive benefits and unlimited advantages of the aforesaid revolutionary transformation, organizations have been in an ongoing pursuit to accelerate the digital transformation drive in the extreme.

On contrary, the accelerated technology adoption and the novel digital transformation have led, according to Hai, et al., (2021), to many unexampled challenges, at the head of which is the abrupt increase in the information security deficit. Along the same lines, Möller (2020) emphasized that as a sequence of the resulted security deficit, cybersecurity has grown into a complicated matter that has increased the concern of organizations, which were still undergoing the transformative process, and accordingly they have become obliged -in order to protect and secure their information systems, operational systems, and databases from potential cyber threats and/or mitigate the damages if they are exposed to cyberattacks- to consolidate their security networks and adopt cybersecurity countermeasures.

Problem Statement:

In proportion to Scheldt (2023), while technology keeps progressing, cybercriminals will simultaneously keep stepping up their efforts to exploit the emerging advances to develop parallelled counter technology and employ it in their malicious activities and maintain an increased level of their cyber hostilities.

In agreement with Scheldt's (2023) point of view, Saeed (2023) indicated that organizations must make certain that their technology solutions are fully protected from cyberattacks as cybercriminals may exploit any possible vulnerabilities and fragility in the security networks of these organizations as well as in and their adopted digital technologies to execute their cyberattacks.

Taking into consideration the reported cases of security breaches and data disclosure incidents witnessed by healthcare sectors worldwide, and as the enormously escalating cyber-attacks keep penetrating many healthcare organizations, this placed additional and heavy burden on healthcare and medical facilities (Zarour, et al., ibid).

Besides, the costs of cybersecurity and cybercrimes, as stated by Sharif & Mohammed (2022), are exhibiting an increasing trend worldwide. As a matter of fact, the economic cost of cybersecurity breaches, according to Haislip, et al., (2019), is underestimated. Furthermore, the aforementioned breaches and attacks' damages and impacts are not only limited to the targeted organizations. They can reach the entire industry or sectors to which these organizations belong.

Hence, given the importance of the subject under investigation, and in responseto the multifaceted cyber challenges faced by the healthcare sector worldwide, the current study took the initiative to highlight key issues related to the emerging cybersecurity threats faced by the healthcare and medical facilities andto identify the effective and sufficient countermeasures.

Research Objectives:-

The present study sought to fulfil the below listed objectives:

1. To highlight key issues concerning the Information Technology (IT) and Network Security (NS) of the healthcare and medical facilities.
2. To shed light on the emerging cybersecurity threats and risks encountered by facilities concerned.
3. To identify the countermeasures that are needed by the respective facilities to prevent, detect and respond to potential cybersecurity threats as well as to mitigate any damages and/or disruption caused the exposure to cyberattacks.

Chapter Two Literature Review

Contemporary Trends In Cybersecurity:

Bearing in mind the high stakes of cyber warfare at a human scale and the widespread cyber dangers that currently constitute a major threat to the international peace and security., especially as the public and privateorganizations in various sectors worldwide have clearly acknowledged that cyber-attacks are among the most prevalent and high impact risks they are confronting at the present time, accordingly, and in recognition of this urgency, it is now imperative and incumbent upon researchers from various scientific fields to intensify their collective efforts and utmost endeavours to conduct more specialized studies and in-depth research to address this dilemma thoroughly and from scientifically diversified perspectives, while putting more emphasis onexamining all of its relevant aspects.

In a nutshell, it is only through initiating continuous line of research that will direct the searchlight cumulatively and maintain conducting extensive analyticalinvestigations and comprehensive discussions that are continuously updated, the existing cyber vulnerabilities and emerging information security threats targeting the healthcare and medical facilities will be tackled expeditiously, andwith a lasting commitment and joint resolve.

Network Security And The Healthcare Sector:

Nowadays, and more than ever, Network Security's (NS) significance has been increasing in intensity, given its greatest abilities and potentials in sustaining and increasing the protection of the operational systems and databases of any foundations, facilities, institutions, organizations, and any other corporate entities from and possible outside interferences (e.g., hacking) which have notably increased in incidence in today's digitally-driven world (Scheldt, 2023).

For all intents and purposes, the Network Security (NS), as per to Roohparvar (2023), represents a crucial requirement for any sector's components. But in the healthcare sector, in particular, it is considered critical and an undoubtedly inevitable necessity that will ensure the long-term continuity, sustainability, andsuccess of this dynamic sector.

Yet, on another note, the 'Healthcare Sector' is characterized by being complexin nature; owing to the fact that it encompasses many different stakeholders, including healthcare providers (e.g., hospitals, doctors, nursing staff, clinics, nursing homes, medical practitioners, nutritionists, dieticians, etc.), patients, insurers (i.e., the party in an insurance contract undertaking to pay compensation), regulatory authorities, and many other partners of concerned official and private bodies. In view of the foregoing, and as part of this vital sector's endeavours to overcome the hurdles resulted from complexity of this sector's nature, as well as to keep pace with scientific and technological advancements in today's world, 'Digitization' (defined as theadaptation of a system, process, etc. to be operated with the use of computers and the internet) was integrated within the course of action and the workflow ofthe healthcare and medical facilities. Despite the fact that such integration has led to simplifying the process of storing, accessing, and exchanging patients' data, and many other tasks and activities, however it had simultaneously increased the vulnerability of these facilities, particularly their security networks, to several types of cyberattacks, network penetration, sensitive data exposure, and a wide range of threats connected with malicious acts (ibid).

Alternatively stated, healthcare and medical facilities have been recently turned into a prominent target for cybercriminals and this is due to the immense and enormous amount of sensitive data these facilities hold, such as medical records, billing information, Personally Identifiable Information (PII), and other types ofdata, which are seen valuable by those criminals as they can be exploited to achieve a numberless malicious and suspicious goals (e.g., blackmailing).

In a related context, Roohparvar (2023) pointed out that the already stated cyberthreats can take the forms of:

1. Malware: a type of software that is designed to disrupt, damage, or gain unauthorized access to computer systems. It is worth noting that a 'Malware' can be introduced to the targeted network through phishing emails, malicious websites, or infected software.
2. Ransomware: a type of malware that encrypts a victim's data and demands a ransom in exchange for the decryption key. Healthcare and medical facilities are particularly vulnerable to ransomware attacks because of the criticality and the sensitivity of the patients' data they hold.
3. Phishing: a form of social engineering that involves tricking individuals into revealing sensitive information or downloading malware. It should be indicated that Phishing attacks have been severely harmful for the healthcare sector in particular and this is because the working healthcareproviders are often busy and may not have the time to verify every emailthey receive and/or check for suspicious links.
4. Insider Threats: intentional threats of harm that come from within the targeted organization, facility, institution, etc. Moreover, these threats revolve around the ultimate pursuits of carrying out a theft or a disclosureof sensitive and/or classified data.

Cybersecurity Of The Healthcare Sector:

Cybersecurity in the healthcare sector, pursuant to Mijwil, et al., (2023), deals mainly with the privacy of patients' data. Likewise, it deals with the security ofmedical devices (Sethuraman, et al., 2020).

Paul, et al., (2023) examined the integration of digital technology in the healthcare sector and presented an in-depth discussion towards the privacy and security issues related to the aforesaid technologies. Particularly, Paul, et al., investigated how the 'Digitization' process has contributed to transforming the healthcare sector digitally. Besides, they explored the impact of the emerging 'Digital Transformation' on patients care. On the other hand, Paul, et al., asserted that 'Digital Solutions' (e.g., biosensors and software) have been introduced into this vital sector to meet the growing needs for maintaining on- demand healthcare services. Over and above, concerns about security and privacy arising from the digitization of healthcare sector may be addressed in a variety of ways, including mutual authentication, key agreement, lightweight cryptography, blockchain-based solutions, etc., (ibid).

Nwaiwu & Mbelu (2020) indicated that the 'General Data Protection Regulation' (GDPR) is considered very crucial for governmental and nongovernmental healthcare entities to comply with in order to track and monitor people's health. In a related context, Garcia-Perez, et al., (2016) confirmed thatthe digital transformation of healthcare systems must be managed effectively from a cybersecurity perspective. This is due to the fact that a secure digital transformation drive, with accordance to Abbas, et al., (2023), can help improvehealth organizations' organizational governance.

It is worth mentioning that many large-scale cyberattacks, according to Murray (2917), had occurred worldwide and impacted many organizations as well as individuals who became anxious about possible future risks.

Concerning the healthcare sector, in particular, Murray reported that a devastating cyberattack has occurred on May, 2017. The attack that later given the name 'WannaCry', has had an impact on several prominent healthcare and medical facilities in the UK, namely 'the United Kingdom's National Health Service' hospitals. These hospitals were hit by the ransomware. The reported damages included: around 70,000 devices and various hospital technologies (e.g., MRI scanners and blood refrigerators) were affected. In fact, the 'WannaCry' attack has shed the light on software vulnerabilities in healthcare facilities and the potential devastation cyberattack could cause.

As per to Murray, healthcare and medical facilities (e.g., home health care, assisted living facilities, and nursing homes) are considered vulnerable to cyberthreats and this is caused by the high level of computer-based technology integrated in these facilities, such as computers, medical hardware, MRI scanners, refrigerators, ventilators, microscopes, etc.

To boot, the potential impacts of healthcare and medical facilities' cyber breach or any malicious cyber act can be great. In addition to the obvious potential for disrupting treatments, surgeries, and other facility operations, these facilities contain a great deal of sensitive information. 'The Ponemon Institute' has stated, "The most lucrative information for hackers can be found in patients' medical records", as electronic health records contain 'Personally Identifiable Information' (PII) such as social security numbers, health care provider details, credit card information, addresses, treatment history, and, for select facilities, valuable research information.

The reputational damage from a cyber breach is also not to be taken lightly; a health care institution's credibility will be greatly damaged by such an attack. In addition to the above, post-attack analysis of the WannaCry attack has revealed several potential vulnerabilities and hence all healthcare and medical facilities must develop risk management strategies to reduce the chances of their exposureto cyberthreats.

'The Ponemon Institute' indicated that the most common cyberattacks occurred with software that was more than three months old and they also occurred as a result of system failure. Consequently, for healthcare and medical facilities to prevent their networks from falling victim to cyberattacks and any relevant threats or risks, these facilities must carry out continuous audits of their machinery to confirm that all software is fully up-to-date and hence can operate properly. The facilities must also prioritize network security to secure their information systems from cyberattack. Finally, it is highly recommended that the segmentation of the network can prevent the entire network from being affectedif one part is exposed to a cyberattack (ibid).

Data breach and cyberattacks incidents occurred worldwide look like a disaster for information security in the healthcare sector. Actually, the continuous cyberattacks have cause several cases of information systems' penetration in many healthcare facilities all over the world. Department of Health and Human Services (HHS) of the USA released a statement in which it revealed its concernstowards the high possibility of its exposure to cyberattacks, especially after it noticed a rapid growth in cyberthreats that targeted its.

The department has also reported that cybercriminals were trying to implement distributed denial of service attack on its server and try to make various facilitiesunavailable of users (Filkins, 2014).

Cyberattacks:

A cyberattack is defined by Swanagan (2022) as a malicious act that is performed by a cybercriminal with suspicious intent to exploit a vulnerability or weaknessin a particular system. Swanagan added that cyberattacks threaten to steal, alter,destroy, disable or gain access to or make use of an unauthorized asset.

In the same line, Leaf-IT (2023) also defined the cyberattack as a deliberate exploitation of individuals or entities' information systems and/or network. In cyberattacks, cybercriminals use malicious code to compromise computers, logicor data and steal, leak or hold the targeted data hostage. Examples on common cyberattacks and types of data breaches can include: 1) Identity theft, fraud, extortion; 2)Malware, phishing, spamming, spoofing, spyware, trojans and viruses; 3) Stolen hardware, such as laptops or mobile devices; 4) Denial-of- service and distributed denial-of-service attacks; 5) Breach of access; 6) Password sniffing; 7) System infiltration; 8) Website defacement; 9) Private andpublic Web browser exploits; 10) Instant messaging abuse; and 11) Intellectual property (IP) theft or unauthorized access.

Indeed, cyberattacks, cyber threats and risks, and cyber vandalism can beextremely catastrophic to any organizations in any sectors or industries. It is worth noting that due to the digital transformation that took place in this recent decades, almost all modern-day organizations should be now equipped with a network of computers, servers, printers, switches, access points, software tools, and routers to operate properly and effectively. Unfortunately, despite of the unlimited advantages of the above-mentioned devices and applications, howeverthey represent a potential risk to organizations (Swanagan, ibid).

Cyberattacks, as per to Saeed (2023), have drastically escalated; therefore, individuals in charge of organizations must be fully aware of cybersecurity threats and any aspects related to this critical issue. They should be also equipped with the sufficient knowledge on how to mitigate the potential cyber threats and risks comprehensively. Saeed added cyberattacks usually aim to assess, change, or destroy sensitive information; extort monetary benefits from users; or interrupt the workflow within an organization.

Swanagan argued that there is no such a thing as an information system/network that is 100% vulnerability free or 'hacker-proof'. Actually, in case of the availability and sufficiency of time and resources, then the cybercriminal's ability to launch a cyberattack is very high. In the same vein, Swanagan mentioned that cyberattacks can come in all shapes and sizes. In other words, it can vary from deploying an application-specific attack against a database server to sending phishing emails with malicious attachments or URLs. In a more detailed manner, below is a clarification of the main types of cyberattacks (2022):

1. Network Attacks (common network attacks include: Denial of Service (DoS), Distributed Denial of Service (DDoS), Buffer Overflow Attacks, Ping Attacks, SYN Flood, DNS Amplification, Back Door, Spoofing, Smurf Attack, TCP/IP Hijacking, Man in The Middle Attacks, Replay Attacks, DNS Poisoning, ARP Poisoning, Domain Kiting, Typosquatting, Watering Hole Attacks, and Zero Day Attacks).
2. Wireless attacks (common wireless attacks include: Explore All Wireless Attacks, Data Emanation, Jamming, Bluetooth Vulnerabilities, Near- Field Communication, War Driving, Evil Twin, Deauthentication and Disassociation, War Chalking, Packet Sniffing and Eavesdropping, WPS Attacks, WEP/WPA Attacks, IV Attack, TKIP Attack, and WPA2 Attacks).
3. Malware attacks (there are thousands of malware variants and different types of malwares including: Viruses, Keyloggers, Worms, Trojans, Ransomware / Crypto-Malware, Logic Bombs, Bots/Botnets, Adware & Spyware, and Rootkits).
4. Social engineering attacks (common types of social engineering attacks include: Email Phishing, Vishing, Smishing, Pretexting, Whaling, and Tailgating).

Concerning the impacts of cyberattacks, since organizations do not often tend to disclose information to the public with regard to their damages and loses when being exposed to cyberattacks, therefore it can be challenging, if not impossible, to estimate the precise costs that organizations incur to be able to function again, to recover loses, to rebuild their reputation, and to restore their customers and stakeholders' trust. Nevertheless, the relevant literature indicates that the impacts of cyberattacks typically involve information loss, disruption of operations, revenue loss, and equipment damage. The most frequent cyberattack types encompasses unauthorized access to data that included phone numbers, email addresses, financial information, full names, birth dates, personal IDs, complete addresses, medical records, and credentials (passwords and usernames)(Bendovschi, 2015).

Cyperattacks' Countermeasures:

The ever-changing virtual threat-landscape, with reference to Scheldt (2023), prioritize the urgent need for adopting improved defences (i.e., robust cybersecurity measures) against cyber adversaries that frequently launch harmful and more complex assaults against vital information systems' infrastructures.

For the purpose of maintaining a high-level of cybersecurity, organizations should implement countermeasures, including encryption, authentication, and access control, as such measures play a key role in protecting these organizations' databases and networks from any possible unauthorized accesses' attempts or any malicious activities that might be carried out by cybercriminals (Saeed, 2023).

As reported by Bendovschi, among the various countermeasures that aim to prevent or limit cybercrimes are: 1) 'Risk Assessment': Taking into consideration their size, the number of their workforces, their geographical setup, and their risk profile, organizations should continuously conduct an assessment of the extent of the cybersecurity control measures' implementation, the accuracy of the identification of potential cyber threats, vulnerability, risks, and the sufficiency and capability of the implemented countermeasures to address the identified risks. Organizations should also make certain that hardware and software equipment are always up to date and undergo constant maintenance. 2) 'Authentication': Relying on the outcomes of the risk assessment, access to the organizations' databases should be exclusively protected by passwords. On the other hand, for remote access or web-based applications, organizations should impose restrictions and more complex authentication means, such as the 'Random PIN Generating Device' and the 'Biometric Authentication'. 3) 'Data Retention': in order to ensure the confidentiality of the organizations' sensitive and vital information and to limit the risk of unauthorised access, all data that is no longer required for the daily course of action of the organizations should be subject to Archiving and retention. This measure would ensure the unneeded data is removed from the organizations' networks and they are kept on a dedicated back-up servers and archives (2015).

In a related context, Leaf-IT (2023) suggested that the cyberattacks' countermeasures include: 1) Raising the awareness of the organizations'

workforce and train them on cyberattack prevention which is one of the most efficient measures that can contribute to the protection of the organization
against cyberattacks and all types of data breaches; 2) Keeping the organizations' software and systems fully up to date: in actual fact, most of cyberattacks happen because the organizations' systems or software are not fully up to date, which create a weakness in the information systems that can be easily exploited by cybercriminals to gain access to the organizations' network. It is highly
that is responsible for managing all software and system updates as well as for
recommended that organization should implement a patch management system to potential cyberattacks. Therefore, each staff member should have separate logins.
keeping the organizations' information systems resilient; 3) Implementing '*Endpoint Protection Software*': this software is capable of securing the
organizations' networks that are remotely bridged to devices. In fact, mobile devices, tablets and laptops that are connected to corporate networks can create access paths to several cybersecurity threats; 4) Installing a Firewall: Putting the organizations' networks behind a firewall is a highly effective way to defend them from various types of cyberattacks a firewalls systems are capable of blocking any brute force attacks or sophisticated data breaches that attempt to target the organizations' security networks and information systems and even before these attacks can cause any damages or penetration; 5) Backup the organizations' data: In the event of cyberattacks, organizations must have their valuable data backed up to avoid serious downtime and any possible loss of this data; 6) Securing the organizations' Wi-Fi network: there is a high possibility that any device that is connected to a Wi-Fi network can get infected. Further, if this infected device is granted connection to an organization's network, then the entire operational and information systems of this organization will be compromised; and 7) Managing the employees' personal accounts: Every member of the organizations' employees needs their own login for every application and program within the organizations' information systems and networks. However, when different users connect to the aforesaid systems and networks under the same credentials, this can increase the chances for exposing

Chapter Three Research Methodology:-

Introduction:

Research is vital in any scientific field. It plays a key role in revealing new information about various subjects.

Actually, research is a systematic process of collecting, documenting, analysing, and interpreting data. Moreover, research employs different methodologies to perform various tasks. The aforesaid research methodology encompasses specific procedures or techniques adopted to identify, select, obtain, process, andanalyse data related to a particular topic.

The main task of the research methodology is to collect, compose and analyze data on the subject matter and to eventually create new knowledge or applying existing knowledge to invent new concepts (Pitchnhire, 2023).

Over and above, research methods are classified into different categories (namely, descriptive and analytical approaches) based on the methods, nature ofthe study, purpose, and research design (ibid).

The current qualitative research study adopted the 'Analytical Approach'. Despite the fact that there are several qualitative research approaches, however the researcher selected this approach as the objectives sought through examiningthe subject under-investigation belons within the qualitative paradigm.

The analytical research approach:
As mentioned earlier in the 'Abstract' section, the 'Analytical Approach' was utilized as the current study's research method through which the researcher hasgathered, analyzed, interpreted the available literature of the subject -under investigation-, and eventually made inferences and reached conclusions.

Authentically, the 'Analytical Approach' was utilized by the researcher for the sake of reviewing the literature related to the current study's subject, i.e., the network security (NS) of healthcare and medical facilities. Precisely, a thorough literature review was conducted by the researcher in order to acquire sufficient understand with regard to the current state in a subject area (mainly through examining previous research published on the topic under investigation) and to further relate obtained understanding to the present study to be able to identify possible gaps in the available relevant knowledge and eventually shape the researcher's argument implied in the conclusion.

A literature review is defined by Bruce (1994, p. 218) as "an important chapter in the thesis, where its purpose is to provide the background to and justificationfor the research undertaken". Truly, while carrying out a literature review, the researcher "extracts and synthesises the main points, issues, findings and research methods which emerge from a critical review of the readings" (Nunan,1992, p. 217) for the purpose of building a "coherent argument which leads to the description of a proposed study" (Rudestam & Newton, 2007, p. 63).

Conclusion:-

This research study, titled "the network security (NS) of healthcare and medical facilities: an analytical overview of the emerging cybersecurity threats/risks and the countermeasures" sought to fulfil the following objectives: 1) To highlight key issues concerning the Information Technology (IT) and Network Security (NS) of the healthcare and medical facilities; 2) To shed light on the emerging cybersecurity threats and risks encountered by facilities concerned; and 3) To identify the countermeasures that are needed by the respective facilities to prevent, detect and respond to potential cybersecurity threats as well as to mitigate any damages and/or disruption caused the exposure to cyberattacks. Additionally, in the current qualitative study, the researcher adopted the 'Analytical Approach' as the research method that was utilized for the sake of gathering, analysing, interpreting the available literature related to the subject - under investigation-, and eventually making inferences and reaching conclusions. Several findings were revealed by this study. Initially, the study found that the novel advanced innovations and technologies have been adopted by the modern healthcare sector and this adoption has imposed a state of 'DigitalTransformation' and a state of 'Digitization'. Nonetheless, both states hadincreased the vulnerability of facilities concerned, particularly with regard to thefacilities' security networks, which increased the fragility level of the information and operational systems and eventually led to the exposure of these facilities to several types of cyberattacks, network penetration, and an increase in the facilities' security networks' deficit. In addition, the findings of the studydemonstrated that the cyber threats can take the forms of: 'Malware', 'Ransomware', 'Phishing', and 'Insider Threats'. Similarly, the cyberattacks' types include 'Network Attacks', 'Wireless Attacks', 'Malware Attacks', and

'Social Engineering Attacks'. Finally, the study revealed several cyberattacks' countermeasures, include: 1) Raising the awareness of the healthcare and medical facilities' workforce; 2) Keeping the organizations' software and systems fully up to date; 3) Implementing 'Endpoint Protection Software'; 4) Installing a Firewall; 5) Backup the organizations' data; 6) Securing the organizations' Wi-Fi network; and 7) Managing the healthcare and medical facilities employees' personal accounts. Further countermeasures include the implementation of 'Risk Assessment', 'Authentication', 'Data Retention':

References:-

1. Abbas, H.M; Qaisar, Z.H; Ali, G; Alturise, F; and Alkhalifah, T. (2022). "Impact of cybersecurity measures on improving institutional governance and digitalization for sustainable healthcare". PLoS ONE: **17**:0274550. doi: 10.1371/journal.pone.0274550
2. Bendovschi, A. (2015). "Cyber Attacks: Trends, Patterns and Security Countermeasures". Procedia Economics and Finance: **28**, 24 – 31. Available at: https://www.sciencedirect.com/science/article (Accessed on: 20th, August, 2023).
3. Bruce, C.S. (1994). "Research students early experiences of the dissertation literature review". Studies in Higher Education: **19** (2): 217-29.
4. Filkins, B. (2014). "SANS health care cyber-threat report: Widespread compromises detected, compliance nightmare on horizon". Available at: https://www.sans.org/reading-room/whitepapers/ (Accessed on: 2nd, November, 2023).
5. Garcia-Perez, A; Cegarra-Navarro, J; Sallos, M.P; Martinez-Caro, E; and Chinnaswamy, A. (2016). "Resilience in healthcare systems: Cyber security and digital transformation". Technovation: **21**:102583. doi: 10.1016/j.technovation.2022.102583
6. Hai, T.N; Van, Q.N; and Thi-Tuyet, M.N. (2021). "Digital transformation: Opportunities and challenges for leaders in the emerging countries in response to COVID-19 pandemic". Emerging. Sci. Journal: **5**:21–36. doi: 10.28991/esj-2021-SPER-03.
7. Haislip, J; Kolev, K; Pinsker, R; and Steffen, T. (2019). "The economic cost of cybersecurity breaches: A broad-based analysis". Proceedings of the Workshop on the Economics of Information Security (WEIS); Boston, MA, USA. 3–4 June 2019.
8. Leaf-IT. (2023). **"**10 Ways to Prevent Cyber Attacks". Available at: https://leaf-it.com/10-ways-prevent-cyber-attacks/ (Accessed on: 9th, November, 2023).
9. Mijwil, M; Aljanabi, M; and Ali, A.H. (2023). "Exploring the role of cybersecurity in the protection of medical information". Mesopotamian Journal of Cybersecurity: **2023**:18–21. doi: 10.58496/MJCS/2023/004
10. Möller, D. (2020). "Cybersecurity in Digital Transformation: Scope and Applications". Springer, Berlin, Heidelberg, Germany.
11. Murray, C. (2017). "The importance of Network Security for health care facilities". Published on: 6th, July, 2017. Available at: https://www.caitlin-morgan.com/importance-network-security-health- care-facilities/ (Accessed on: 10th, November, 2023).
12. Nunan, D. (1992). "Research Methods in Language Learning". Cambridge: Cambridge University Press.
13. Nwaiwu, F. & Mbelu, S. (2020). "Digital Transformation in Healthcare and Surveillance Capitalism: Comparative Assessment of Data and Privacy Protection Compliance across the European Union". Published on: 5th, July, 2020. Available at: https://ssrn.com/abstract=3643838
14. Paul, M; Maglaras, L; Ferrag, M.A; and AlMomani, I. (2023). "Digitization of Healthcare Sector: A Study on Privacy and Security Concerns". ICT Express: doi: 10.1016/j.icte.2023.02.007
15. Pitchnhire. (2023). "Everything you need to know about analytical research: Its essential uses". Available at: https://www.pitchnhire.com/blog/analytical-research (Accessed on: 14th, October, 2023).
16. Roohparvar, R. (2023). "Network Security in the Healthcare Sector".Published on: 25th, February, 2023. Available at: https://www.infoguardsecurity.com/network-security-in-the-healthcare- sector/ (Accessed on: 2nd, October, 2023).
17. Rudestam, K.E. and Newton, R.R. (2007). "Surviving your Dissertation: A Comprehensive Guide to Content and Process". (3rd Edition). ThousandOaks, CA: Sage Publications Inc.
18. Saeed, S. (2023). "Digital Workplaces and Information Security Behaviour of Business Employees: An Empirical Study of Saudi Arabia". Sustainability Journal: **15**:6019. doi: 10.3390/su15076019
19. Scheldt, A. (2023). "What is a countermeasure in computer security?".Published on 21st, August, 2023. Available at: https://www.comptia.org/blog/what-is-a-countermeasure-in-computer- security (Accessed on: 1st, September, 2023).
20. Sethuraman, S.C; Vijayakumar, V; and Walczak, S. (2020). "Cyberattacks on healthcare devices using unmanned aerial vehicles". J.Med. Syst: **44**:29. doi: 10.1007/s10916-019-1489-9
21. Sharif, M.H. & Mohammed, M.A. (2022). "A literature review of financial losses statistics for cyber security and future trend". World J.Adv. Res. Rev: **15**:138–156. doi: 10.30574/wjarr.2022.15.1.0573
22. Swanagan, M. (2022). "How to prevent cyberattacks & threats". Published on: 16th, October, 2022. Available at: https://purplesec.us/resources/prevent-cyber-attacks/ (Accessed on: 1st,November, 2023).

23. Zarour, M; Alenezi, M; Ansari, M.T.J; Pandey, A.K; Ahmad, M; Agrawal, A; Kumar, R; and Khan, R.A. (2021). "Ensuring data integrity of healthcare information in the era of digital health". Health TechnologyLetters Journal. **16**;8(3):66-77. doi: 10.1049/htl2.12008.