WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cyber Attack - Envenom in Indian Healthcare – A Review

Dr. Parvathi Balaji [1], Dr. Divya Raghunathan [2], Dr. Aravinth. V [3], Dr.Shyam Sivasamy[4], Swetha.V[5], Dr . Preetha Elizabeth chaly[6.]

[1]Department of Public Health Dentistry, Meenakshi Ammal Dental College and Hospital, Chennai, India
[2]Department of Public Health Dentistry, Meenakshi Ammal Dental College and Hospital, Chennai, India
[3]Department of Public Health Dentistry, Meenakshi Ammal Dental College and Hospital, Chennai, India
[4]Department of Public Health Dentistry, Meenakshi Ammal Dental College and Hospital, Chennai, India
[5]Department of Public Health Dentistry, Meenakshi Ammal Dental College and Hospital, Chennai, India
[6]Department of Public Health Dentistry, Meenakshi Ammal Dental College and Hospital, Chennai, India
DOI: https://doi.org/10.55248/gengpi.4.623.45359

A B S T R A C T

The year of lockdown in 2019 had drawn attention to the rise in cyberattacks on healthcare organizations in recent years. While embracing digital technology to raise the standard of patient care, healthcare professionals are growing more and more concerned about these cyberattacks. As a result, it is crucial to combat cyberattacks on healthcare systems as a whole and inside them. Cybersecurity, IT networks, and software deployment are all necessary for a successful electronic health record system. The benefits of these safe electronic health records for patients include better healthcare efficiency, which has a substantial positive impact on the standard of treatment and patient safety. The number of phishing attacks in the healthcare industry found to be increasing. Accurate detection of these attacks is one of the major challenges in healthcare organizations. With help of basic security standards and strategies at both organizational and individual levels will help us to rise against cyberattacks. Cybersecurity offers information on the scope of cyberattacks and their effects on employee well-being and makes the case that cybersecurity education for all employees in healthcare organizations has to be improved. Hence the current state of cybersecurity in healthcare facilities should be knocked upon and related safety preventive measures should be evaluated. Therefore, the importance to have protection controls to guard the personal information of human beings has to be sorted and cognizance and awareness amongst people involved in cyber security ought to be created.

Keywords: cyberattack, cybersecurity, healthcare organization, medical devices, covid-19.

INTRODUCTION

The Indian healthcare system is regarded as a most important and fast-growing sector with the availability of an accessible and affordable treatment plan which serves as an essential key for enabling easily accessible healthcare to all the individuals in our country. When the Pandemic was declared, the healthcare system struggled to cope with uncontrolled and exponential demand so the rise in teleconsultation evolved.[10] This transformation has set an advanced step in the healthcare industry which had integrated patient data saved along with cybersecurity measures for networked medical devices.[7] A lifelong medical record is simply not feasible without standards and security, as various records from various sources that may span more than 80 years must be brought together effectively. Nowadays, Security and privacy in Electronic Health Reports (EHR) can be threatened by hackers, viruses, and worms. If the networks are not rightly monitored at the organizational level, it can undoubtedly jeopardize the health care given to patients.[6] Because of the risks that accompany poorly monitored healthcare information systems, healthcare industries must be assisted with an extensible network monitoring solution.[3,9] Health record systems must be secured to ensure that the data available are safe for longer. So Cyber Security works to establish appropriate controls and protections to protect the data. In this review article, cyber-attack in the Indian healthcare system and the need for cyber security are explored.[12]

1.1 DIGITAL HEALTH CARE

Digital transformation is a holistic effect created by a software application that fundamentally transforms a particular domain. Nowadays, with the ever-growing number of internet users and the expanding range of internet services, the demands on the security of users are questionable[7]. With the help of integrated technologies, doctors and patients built a healthy step toward a digitalized healthcare system. Digital health care makes simple and easy ways of diagnosing and monitoring the pattern of diseases.

Digital technologies for health have influenced health services should be accessed easily and operated efficiently. When implementing an EHR, hardware, and networking are considered as important.[6] Linux/Unix systems or Microsoft OS servers are used to operate the majority of EHR software. Modern EHR software applications and older legacy programs can function on the same server. It should exploit any telecommunications-related

connectivity like the Internet, WAP, WAN, GSM, CDMA, LAN, or even Cloud Computing. Mostly Local Area Network (LAN) is used in the medical field, a combination of wired and wireless, and using a firewall, the network must be kept secure to keep intruders from hacking into the network. Remote or off-site sites would connect to the LAN and the internet using high-speed Internet connections like DSL, cable, fiber, or a dedicated T1.DICOM PS3.0-2015 is a standard protocol used in the majority of medical and healthcare facilities to manage and transmit medical pictures and related data.[8,14,17]

1.2 COVID-19 AND CYBERATTACK

As COVID-19 spread across the globe, a major secondary threat to a technology-driven society emerged. During the year of lockdown 2019, Cybercriminals contemporaneously had a bullseye on critical national infrastructure like the healthcare industry.[10] As health documents contain sensitive financial and personal information, the health industry became an attractive target for cybercriminals. The extensive demand for electronic health records of a patient in the illegal market aggravated the virtual attacks destroying the reputation and wealth of the medical institutions.[16] Attackers tried injecting malicious payloads into the network. It is extremely challenging for organizations to develop appropriate protection and response measures to give the dynamic environment. The cyber-crime incidents from the COVID-19 pandemic caused serious threats to the global economy and the safety of the worldwide population.[10] The increasing frequency and the evolving nature of cyberattacks launched against healthcare and clinical environments require an organization-wide effort to undertake risk prevention and mitigation actions. Hence understanding their mechanisms, propagation, and reach of these threats became essential.[12]

Globally, a total of 94% of health organizations experienced data breaches regarding patients and hospital records.[12] A phishing attack on the World Health Organization was identified in March 2020.[5] The goal of cyber-attackers was to steal passwords from WHO employees by creating a malicious website that looked like the organization's internal email system. Although the attempt was unsuccessful, it highlighted the level of sophistication of phishing attacks targeting healthcare organizations. A Major ransomware assault on the Irish health system in May 2021 impacted more than 80% of its Computer infrastructure, stole data, and prevented medical professionals from accessing clinical and non-clinical systems including finance and procurement. The incident started when a staff member opened a spreadsheet that had been corrupted by malware that was provided to them via email. It took 4 months to fully recover[5]. According to the World Economic Forum (WEF), between December 31, 2019, and April 14, 2022, there were 30,000 cyberattacks expressly related to COVID-19, a 50.1% increase in cyberattacks as a result of the pandemic. It was reported that COVID-19 alone caused a 30,000% increase in the number of cyber threats.

Recently India faced a cyberattack in our prestigious medical institution, AIIMS NEW DELHI, which struggled to bring its digital services back online after the hack. In November, the Safdarjung Hospital in New Delhi similarly experienced a cyberattack, but it was able to quickly recover its system with no indication that any data had been compromised. According to the Cyber Peace Centre of Excellence (CCoE), the healthcare sector has experienced over 1.9 million attack events from 2022 to November 28.

1.3 TYPES OF CYBER ATTACKS

Various kinds of cyber-attacks have been launched against healthcare organizations. There are three main sorts of cyber-attacks that healthcare organizations frequently encounter[12]. They are

(i) Attacks exploiting IT infrastructure vulnerabilities resulting from misconfigurations of network components, such as firewalls, overwhelming digital services by flooding requests (denial of service (dos), DDoS), software bugs in the system (such as structured query language organizations, privilege escalation, man-in-the-middle (MITM) or eavesdropping, Cryptographic attack .[10]

(ii) Ransomware attacks against healthcare organizations occurs with the intention of causing service disruption and holding the healthcare organization’s data hostage for economic gains.[7]

(iii) Emerging threat of exploiting a human vulnerability in gaining access to healthcare infrastructure.

2. VARIOUS MODES OF ATTACKS IN HEALTHCARE

2.1 VULNERABLE SOFTWARE:

The healthcare system becomes an easy target for cyber-attacks because of the usage of vulnerable internet-facing systems like Remote Desktop Protocol (RDP), Server Message Block (SMB), Database services enabled software, and old Windows server platforms[14]. A total of 1527 unique payloads belonging to Trojan, Ransomware, etc. were captured by the deployed network. With the widespread adoption of digital technologies, many aspects of society from social interactions and commerce to business and industry, but regrettably also crime have gone online.[7]

2.2 SOCIAL ENGINEERING ATTACKS AND HEALTH CARE

The most effective technique of assault to target medical professionals is social engineering which makes use of personal information provided on social media. Such risks which are frequently referred to as "social engineering," enable the attacker to obtain the personal information of healthcare professionals by taking advantage of the vast amount of public information housed on social media platforms.[10,12]

Attacks using social engineering are intended to get over conventional cybersecurity defenses. Phishing is a popular form of social engineering, and while the impact of cybersecurity is not unique to the healthcare sector, coordinated efforts to protect stakeholder data have lagged behind other sectors in the healthcare sector.[12]

2.3 PHISHING ATTACKS

Phishing attacks describe a particular type of scam where an attacker sends a fraudulent email or text message from a seemingly trusted individual or organization. The goal is to persuade the recipient to open an attachment that will enable the attacker to do something the victim might not be aware of, such as steal login information or passwords. Interacting with phishing emails allows attackers to obtain login information and infect the IT infrastructure with malware. The increasing reports of phishing attacks launched against healthcare professionals are reported as the root cause of attacks as employees of an organization still clicking on phishing links.[5,12]

2.3 RANSOMWARE ATTACK

It is difficult to ignore the current spike in reports of hospital ransomware attacks. With the increasing frequency and severity of ransomware attacks on hospitals, healthcare organizations can disrupt operations and patient access for weeks or even months. Malicious software (malware) known as Ransomware locks down computers in hospitals until the victim pays a ransom. Ransomware uses encryption to block access to a hospital's own vital information, such as databases, file servers, patients' case histories, etc.[5]

2.4 SQL INJECTION ATTACKS

One of the oldest, most common, and most harmful web application vulnerabilities is known as an injection attack or SQL Injection (SQLi) attack. It is possible to execute malicious SQL statements via this injection technique These statements are used to manage a database server that is hidden behind a web application. Application security protections can be evaded by attackers using SQL Injection flaws. The full content of a SQL database can be retrieved by getting past authentication and authorization of a web page or online application. They can also add, alter, and delete records in the database using SQL Injection.[10]

Every website or web application that makes use of a SQL database, such as MySQL, Oracle, or SQL Server may be vulnerable to a SQL Injection flaw. Attackers may use it to get unauthorized access to healthcare systems' sensitive data, which includes patient information, personal information, trade secrets, intellectual property, and other information.

3. CYBERSECURITY

Due to the scale, complexity, and existence of various legacy and stand-alone systems, it has been highlighted that several healthcare organizations are struggling to have proper cybersecurity measures to cope with cyberattacks. This is recognized as the key challenge in putting into practice efficient cybersecurity measures. However, Cybersecurity increasingly becoming a prominent concern among healthcare providers in adopting digital technologies for improving the quality of care delivered to patients. The successful adoption of digital transformation strategies within the healthcare industry relies on the successful acceptance among healthcare professionals towards addressing risks posed by cyber threats.[5,11] Healthcare cybersecurity is a responsibility, not an obligation or a duty.[11] When patients and their families entrust the health system and its professionals with their lives, their total dedication to provide excellent care becomes their fundamental expectation. so basic security standards and strategies must be followed at both organizational and individual levels to fight against cyberattacks.[3,4]

3.1 THE SECURITY STANDARDS

In accordance with the security standards, healthcare organizations must put in place reasonable and suitable administrative, physical, and technical precautions to[13]:

• guarantee the privacy, accuracy, and accessibility of every e-PHI they generate, transmit, receive, or keep.

• safeguard their e-PHI from reasonably expected threats or dangers to both security and integrity.

• guard against e-PHI uses or disclosures that aren't authorized by or allowed by the Privacy Guidelines.

• guarantee that their staff will adhere to their security policies and procedures

3.2 ORGANIZATIONAL STRATEGIES

Organizational strategies must be adopted to counteract cyberattacks. It is recommended that healthcare organisations create a specialized cybersecurity workforce framework to reduce the risk of attacks.[12] Seven important roles must be incorporated into the framework to make it efficient they are

(i) **Security provision-**which is tasked with conceptualizing, designing, and constructing secure ICT systems;

(ii) **Operation and maintenance**— in charge of the administration, maintenance, and support of ICT systems;

(iii) **Supervising and governing**—whose duty it is to give direction, administration, and leadership for putting cybersecurity protection and resilience measures into practice;

(iv) **Protection and defense** - whose role it is to identify, assess, and neutralize risks to internal ICT systems and/or networks.

(v) **Analysis**- whose role it is to conduct a highly specialized assessment and evaluation of incoming cybersecurity information in order to identify its usefulness for intelligence collection.

(vi) **Collection and operation**- whose duties include collecting cybersecurity data that could be helpful in the development of intelligence and performing specific denial and deception operations;

(vii) **Investigation-** whose responsibility is to investigate cybersecurity events or crimes related to ICT systems, networks, and digital evidence.

3.3 CYBER SECURITY TRAINING

While many organizations and researchers have recognized the necessity for healthcare personnel to receive cybersecurity training. The need for formal training and educational standards to enable organizations to address human factors of cybersecurity, critically mitigating cyber risks, is rightfully growing in academia and healthcare.[9,12] These standards will enable organizations to empower students to understand digital health technologies. We must implement a strategy that allows IT systems to identify phishing emails and other social engineering attacks while also arming healthcare personnel with the expertise to recognize social engineering in order to start a coordinated effort to promote good practices for cybersecurity measures.[11] Several healthcare organizations educate their staff members on cybersecurity. Healthcare practitioners' increased levels of training and resulting awareness have been shown to be essential for effectively combating phishing.

Additionally, the range of technical mitigation measures identified includes,[12]

(i) Installing a firewall and network segmentation;

(ii) Doing frequent backups;

(iii) Restricting access to USBS by turning off unused physical ports;

(iv) Adding approved programs to a whitelist;

(v) Implementing regular updates and patches;

(vi) Implementing the least privilege principle for controlling user authentication and access permissions to healthcare resources;

(vii) Using software to guard against malware and viruses;

(viii) Putting in place audit trails and logging for incident reports;

(ix) Establishing data encryption for both at-rest and in-transit use;

(x) Putting in place network monitoring and intrusion detection software;

(xi) Safe system setups;

(xii) Protecting mobile devices with apps.

4. Conclusions and Recommendations

It became vital to suppress healthcare cyber piracy and protect the network infrastructure that supports them. The increase in cyber-attacks on healthcare institutions has made headlines through the COVID-19 pandemic. Cyberattacks in our prestigious medical institution and Dental institution highlighted the level of sophistication of attacks in our healthcare system.[5] However, this threat to healthcare organizations and patient safety is not new; cyber-attacks have intensified with the increased use of digital technology in healthcare. To collectively enhance healthcare organizations, a coordinated and standardized strategy is needed for the creation of training programs, awareness campaigns, and information sharing on the nature and type of

cyberattacks. Each organization should conduct a cyber risk and privacy impact assessment in order to identify potential vulnerabilities that could be exploited by cyber attackers and fix security gaps in the healthcare organization.[12] All medical education programs must advance curriculums and priorities to train clinical staff to prepare for and address, cybersecurity threats as they would any other element of patient safety[5].

References

1. Alshaikh, M., & Adamson, B. (2021). From awareness to influence: toward a model for improving employees' security behaviour. *Personal and Ubiquitous Computing*, *25*(2), 829–841. https://doi.org/10.1007/s00779-021-01551-2
2. Angel, D. (2022). Protection of Medical Information Systems Against Cyber Attacks: A Graph Theoretical Approach. *Wireless Personal Communications*, *126*(4). https://doi.org/10.1007/s11277-022-09873-x
3. Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns, and Security Countermeasures. *Procedia Economics and Finance*, *28*, 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1
4. Dawson, J., & Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology*, *9*, 1–12. https://doi.org/10.3389/fpsyg.2018.00744
5. Niki, O., Saira, G., Arvind, S., & Mike, D. (2022b). Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that. DIGITAL HEALTH, 8, 205520762211046.
6. ELECTRONIC HEALTH RECORD (EHR) STANDARDS FOR INDIA 2016 Standards Set Recommendations v2.0.
7. Faddis, A. (2018). The Digital Transformation of Healthcare Technology Management. *Biomedical Instrumentation & Technology*, *52*(s2), 34–38. https://doi.org/10.2345/0899-8205-52.s2.34
8. Guo, U., Chen, L., & Mehta, P. H. (2017). Electronic health record innovations: Helping physicians – One less click at a time. *Health Information Management Journal*, *46*(3), 140–144. https://doi.org/10.1177/1833358316689481
9. Kweon, E., Lee, H., Chai, S., & Yoo, K. (2019). The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence. *Information Systems Frontiers*, *23*(4), 1–13. https://doi.org/10.1007/s10796-019-09977-z
10. Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. *Computers & Security*, *105*(1), 1–20. https://doi.org/10.1016/j.cose.2021.102248
11. Muthuppalaniappan, M., & Stevenson, K. (2020). Healthcare Cyber-Attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health. *International Journal for Quality in Health Care*, *33*(1). https://doi.org/10.1093/intqhc/mzaa117
12. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors*, *21*(15), 5119. https://doi.org/10.3390/s21155119
13. Rehman, H. ur, Yafi, E., Nazir, M., & Mustafa, K. (2018). Security Assurance Against Cybercrime Ransomware. *Intelligent Computing & Optimization*, 21–34. https://doi.org/10.1007/978-3-030-00979-3_3
14. Seymour, T., Frantsvog, D., & Graeber, T. (2012). Electronic Health Records (EHR). *American Journal of Health Sciences (AJHS)*, *3*(3), 201. https://doi.org/10.19030/ajhs.v3i3.7139
15. Sikora, M., Fujdiak, R., Kuchar, K., Holasova, E., & Misurec, J. (2021). Generator of Slow Denial-of-Service Cyber Attacks. *Sensors*, *21*(16), 5473. https://doi.org/10.3390/s21165473
16. Veeramakali, T., Shobanadevi, A., Nayak, N. R., Kumar, S., Singhal, S., & Subramanian, M. (2022). Preserving the Privacy of Healthcare Data over Social Networks Using Machine Learning. *Computational Intelligence and Neuroscience*, *2022*, 1–8. https://doi.org/10.1155/2022/4690936
17. Wiedemann, L. A. (2012). A look at unintended consequences of EHRs: the industry needs to focus on building EHRs that decrease medical errors and enhance patient care. *Health Manag Technol*, *33*(2), 24–25.