A Systematic Study on Cyber Attacks on Medical Data

[1]Meera S, [2]Akhil Sekharan

[1]PG Scholar , [2] Assistant Professor
[1&2]Department of MCA , St. Joseph's College Of Engineering And Technology, Palai

Abstract: Since users' lives are made easier by new technology and digital opportunities, healthcare is gradually becoming more digital. On the one hand, this offers a great potential, but it also exposes healthcare organizations to a number of risks (both digital and non-digital) that might allow an attacker to compromise the security of medical processes and even the safety of patients. Technical cybersecurity countermeasures are being utilized, particularly in the healthcare sector, to ensure the privacy, accuracy, and accessibility of data and information systems. Digital data breaches in the healthcare industry have been said to cause particularly sensitive harm due to the unauthorized use of private and sensitive information. In the face of such a hazardous threat, medical institutions must evaluate the financial ramifications of a prospective cyber-attack that results in a compromise of patient data. The study's findings demonstrate that estimates of overall digital data breach expenses vary greatly between reports and analyses. The major causes are the use of various estimating methodologies and a lack of full and accurate databases as a result of inadequate disclosure of cyber events. Furthermore, the paper's most crucial conclusion is that there is an urgent need to do study on potential data breaches. This is a review article developed by evaluating numerous research publications on the topic "cyber assault on medical data".

Keywords: Medical data, Health care, Patient data

I.INTRODUCTION

The healthcare industries are going towards digitalization as new technology and digital opportunities can make users' life easier. The usage of electronic health records has greatly enhanced medical procedures as well as patient care, disease diagnosis, and information accessibility. The potential attack surface has grown due to the increased accessibility of healthcare applications and data. The privacy of the data for patients, workers, and facilities could be compromised by a number of security breaches because medical records are a large source of crucial data.

Information security or privacy breaches in the healthcare industry could have a negative impact on patient care and overall health. When a legitimate transaction reads a group of data items and updates additional data items based on the value received, the damage caused by an attacker propagates throughout the database. This will influence how decisions are made. Therefore, the harm must be effectively and swiftly repaired. Financial costs are associated with how cyberattacks on medical data are felt. In order to take steps to lessen the financial effects, medical entities must estimate them.

II.IMPORTANCE OF MEDICAL DATA

Health care professionals can deliver more effective, higher-quality, safer, and more individualized care and care coordination when they have access to a patient's most recent health information. Patients who examine their own health information get knowledge about how their health changes over time. As a result of their enhanced health knowledge and empowerment, the quality of their treatment and their quality of life will both improve, making it easier for them to modify their lifestyle .They will also be able to communicate with their healthcare professionals more successfully .Scientific research using health data can hasten the creation of new medical devices and therapies for those who require them.

Organizations can Determine risk variables to hasten diagnosis, identify disease transmission channels to stop the spread of illnesses and other problems, predict results and make treatments more successful, enhance the effectiveness and security of therapies, make knowledge available, improve public health policy.

Health data can be used by distinct health and care specialists as well as provider organizations to improve the care pathways, boost patient care, obtain information for strategic planning and enhancing organizational quality, make better use of the resources available for healthcare and to become more active in clinical research.

III.HEALTH CARE CYBER ATTACKS

Threats can take the form of incorrect use, loss, unauthorized disclosure, or alteration. Four new subcategories of network security hazards were produced as a result of further specialization: interruption, interception, modification, and fabrication.

The three assault surfaces mentioned by the authors are displayed all around the patient in a concentric circle arrangement. Any holes in a healthcare facility that, if utilized maliciously, could have an instant negative impact on the patient are the principal assault surfaces. The secondary assault surface does not instantly cause harm to the patient, but it may be used to support more harmful attacks. The tertiary attack surface, which also includes financial and administrative systems, inventory systems, electrical infrastructure, etc., might have a substantial impact on the hospital or business as a whole.

In 2021, there were a considerable number of healthcare-related data breaches, with over 40 million patient records compromised in the USA. As a result of the threat of cybercrime to the healthcare sector, the FBI released numerous advisories. In the wake of Russia's invasion of Ukraine, the FBI has released additional warnings on Russian hacks on US healthcare organizations. According to a Protenus investigation on the effects of healthcare-related data breaches, which found that 905 incidents were recorded, over 50 million patient records were compromised last year. This was brought on by a 44% rise in hacking attempts against healthcare organizations. Healthcare-related data breaches affected more than 22.6 million patients in 2021, with the largest revealed breach involving more than 3 million people. In the USA, nearly 600 healthcare security incidents were reported last year. In accordance with the HITECH legislation, the US government publishes a list of all alleged healthcare breaches involving 500 or more

individuals. For the previous five years, there has been an increase in healthcare data breaches, and when the pandemic hit in 2020, there was a startling 42% increase. In 2020, the healthcare sector was the target of 60% of ransomware attacks that were recorded globally.

According to a survey of 100 hospital IT directors, small and midsize hospitals are particularly vulnerable to cyberattacks, with 48% of executives saying that their organization had to shut down in the preceding six months as a result of a cyberattack.

The analysis found that larger hospitals those with 1,000 or more beds shut down for longer periods of time and at a higher cost $21,500 USD per hour. Smaller hospitals, on the other hand, frequently had closures that lasted more than nine hours and were very costly which is almost $47,500 USD each hour. It is obvious that smaller healthcare organizations are most negatively impacted by cyberattacks. Smaller companies sometimes have lower cybersecurity costs, which makes them a popular target for criminals. An investigation by the cybersecurity firm Tenable found that scammers routinely target medical suppliers. Third party companies are used to get unauthorized access to healthcare systems in order to get around internal security safeguards. According to reports, third-party suppliers were responsible for 60% of healthcare data breaches in 2021.Pharmaceutical firms are experiencing a sharp increase in data breaches outside of hospitals, with malevolent activity accounting for 53% of these incidents. Due to poor security expenditures and very valuable personal data, care facilities have also turned into a very valuable target for cybercriminals.

Ransomware is the cyberattack that poses the greatest risk to healthcare businesses. Researchers discovered 68 healthcare ransomware infections worldwide between July and September of last year alone. The majority of healthcare ransomware assaults in the United States, which made up 60% of all attacks, were directed against medical facilities.

In 2020, 34% of healthcare organizations worldwide are expected to experience ransomware attacks, according to a Sophos estimate. Of those, 65% of healthcare firms claimed that cybercriminals' attempts at data encryption had been successful. An additional 34% paid the ransom to have their data returned. Ransomware assaults have increased by 45% in the healthcare industry since 2021. Uncomfortably, 41% of healthcare businesses who haven't been struck by ransomware think they will be in the future. Healthcare ransomware attacks may result in more disastrous outcomes. According to a recent assessment, ransomware shutdowns in hospital data bases and even equipment can and have resulted in patient deaths.

One of the most prevalent cyberthreats overall is phishing, which affected 81% of firms last year. Phishing attacks are among the most frequent attacks in the healthcare industry, and healthcare is no exception. Phishing can take many different forms, from targeted tactics aiming to obtain phony invoice payments to mass email campaigns intended to fool staff into giving up passwords. During the height of the COVID-19 outbreak, phishing attacks climbed by an astonishing 220%. Business Email Compromise (BEC) is a subcategory of phishing campaigns in which attackers try to get access to email accounts in order to carry out even more convincing phishing schemes. BEC assaults, sometimes referred to as the "26-billion-dollar scam" by the FBI, can be very successful in the healthcare setting. The amount of email-related cybercrime, such as phishing attempts and business email compromise, increased by 42% in the healthcare sector

IV.FINANCIAL IMPACT OF HEALTHCARE DATA BREACH

In 2020, the entire cost of healthcare-related data breaches will be $21 billion. According to a recent IBM research, the average cost of a healthcare data breach was $9.23 million US Dollar , up $2 million US Dollar from the prior year.

Healthcare firms are expected to lose $6 trillion USD as a result of data breaches over the next three years, according to estimates. Healthcare firms are heavily investing in their cybersecurity defenses to assist combat this. Healthcare businesses will invest $125 billion US Dollars in cybersecurity between 2020 and 2025.

Medical entities must project the financial impacts in order to lessen the financial impact of cyberattacks on medical data. As a result of inadequate disclosure of cyber incidents and the lack of comprehensive and accurate databases, the cost of a digital data breach varies greatly according to different estimation techniques.

The results of the study show how estimates of the overall expenditures related to digital data breaches vary dramatically between studies and assessments as a result of different estimating methodologies, a lack of comprehensive and reliable databases, and poor disclosure of cyber events .Since many data breaches go unreported or are not fully disclosed, experts are still unable to estimate the losses accurately.

The principal costs that a healthcare business would incur in the case of a cyber data breach are as follows:

The primary responsibility following the discovery or even the suspicion of a data breach is to ascertain what actually transpired. A healthcare institution typically needs expert third-party services to carry out a thorough examination. between $100 and $1,000 per hour.

A healthcare organization must alert the individuals whose data has been compromised once it is recognized who it is. It costs from $5 to $50.

Protecting patients after a breach:

Additional services, such identity theft protection and credit monitoring, may help keep patients protected from any unauthorized uses of stolen data. It costs range from $10 to $30 per victim.

Legal fees and other court costs include compensation for monetary losses and emotional suffering brought on by a data leak

V.SOME RECOMMENDATIONS TO AVOID CYBER ATTACKS ON MEDICAL DATA

Organizations should specify the cybersecurity responsibilities of employees and devote more funds and resources to IT security. Additionally, important guidelines are presented that suggest risk assessment techniques, penetration testing, intrusion prevention services, and log monitoring systems, as well as firewall implementation, network auditing, privilege restrictions, and procedures for routinely checking crucial server files.

On the subject of linked medical devices, suggestions were made for businesses to put in place appropriate safeguards like device access control and security testing beyond the development stage. Additionally, they are urged to mandate antivirus checks, the deployment of firewalls, and the provision of reporting tools for users to share cybersecurity-related concerns. Regulators are requested to suggest best practices, but must strike a balance between enforcing security and creating onerous regulations. Other

researchers suggest that the task of creating standards for device cybersecurity be given to an independent non-profit group made up of professionals from the medical field, business, and academia. Also recommended are high requirements for security research methodologies and collaboration with security specialists.

Additionally, hospitals are urged to create training plans that are at least yearly revaluated and revised in light of recent incidents. Training in privacy rules, preventing data leaks, and using social media at work is advised, but a focus on digital hygiene—good security habits like selecting stringent privacy settings and robust password protection—is particularly important. End users shouldn't trust dubious emails, use the same password across many accounts, or leave their laptops unattended. Additionally, setting and enforcing appropriate policies for password protection and information exchange is advocated for healthcare institutions.

VI.CONCLUSION

Healthcare technology has a significant impact on society's health, yet it is prone to security problems due to its connectivity, accessibility, out-of-date systems, and lack of attention on cybersecurity. Although patient care has always gotten the majority of the emphasis, healthcare technology also hold vast amounts of sensitive and significant data. Attacks are typically carried out for monetary gain since a medical identity is more valuable than other forms of identification. Certain attacks, like cyberwarfare, could be motivated by politics. Yet, human lives are at danger if vital health systems are targeted.

Cyberattacks on medical data have become a significant issue in recent years. These attacks run the risk of compromising private patient information, disrupting healthcare operations, and costing healthcare providers money.

To defend their systems and data against hackers, healthcare firms must take preventative action. This may entail installing strong security measures like firewalls, encryption, and access restrictions as well as offering frequent training to employees to improve their capacity to recognize and respond to threats.

Together with preventing attacks, it's essential to have a strategy in place for what to do in the event that one does occur. To do this, you might need to isolate the affected computers, restore your data from backups, and notify the appropriate authorities about the problem.

Additionally, it's crucial to comprehend how complex and dynamic cyberthreats are to medical data. By being informed about the most recent advances and best practices in cybersecurity, healthcare firms can better protect their systems and data and react to any attacks.

VII. ACKNOWLEDGMENT

First and foremost, I give all glory, honor and praise to God Almighty who gave me wisdom and enabled me to complete this work successfully.

I also want to thank my parents from the bottom of my heart for their encouragement and help with this work and with all of my other endeavors.

I am incredibly grateful to Dr. V. P. Devasia, Principal of SJCET in Palai, for letting me use all of the facilities there as well as for his support. Words cannot adequately express how grateful I am.

Sincere thanks go out to Mr. Anish Augustine, HOD Incharge, Department of MCA, SJCET, Palai, who has been a continual source of inspiration and whose tremendous help and support have made this effort possible.

I owe a particular debt of gratitude to Akhil Sekharan, Asst. Professor, Department of Computer Science and Applications, SJCET, Palai, for all the necessary help and support that he has extended to me. His valuable suggestions, corrections, and sincere efforts to accomplish this work even under a tight time schedule were crucial to the successful completion of this work.

I want to express my gratitude to all of the instructors and other support personnel at SJCET, Palai, for the information they have given me over the last three years.

Additionally, I would like to thank all of my friends for their encouragement, advice, and support.

REFERENCES

1. A. Razaque et al., “Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical domain,” in IEE Access, vol. 7, pp. 168774-168797 ,2019, doi:10.1109/ACCESS.2019.2950849.
2. Meisner.(2019.(2017).Financial consequences of cyber attacks leading to data breaches in health-care sector. Copernican Journal of Finance & Accounting,6(3), 63-73. http://dx.doi.org/10.12775/CJFA.2017.017.
3. Coventry,Lynne and Branely,Dawn(2018) Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113.pp. 48-52.ISSN 0378-5122.
4. K. Kandasamy, S Srinivas, K. Achuthan an V. P. Rangan, “Digital Healthcare – Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risk, NIST Perspectives, and Recommendations,” in IEEE Access, vol. 10,pp. 1234512364,2022,doi:10.1109/ACCESS.2022.3145372.
5. Y. K. Saheed and M. O. Arowolo, “Efficient Cyber Attack Detection on the Internet Of Medical Things – Smart Environment Based On Deep Neural Network and Machine Learning Algorithms,” In IEEE Access, VOL. 9,PP. 161546161554,2021,doi:10.1109/ACCESS.2021.3128837.
6. Tervoot, Tom, et al. “Solutions for mitigating Cybersecurity risks caused by legacy software in medical device: a scoping review.” IEEE Access 8 (2020): 84352-84361.
7. Argaw, S.T., Bempong, NE., Eshaya-Chauvin, B. et al. The State of Search on cyberattacks against hospitals and available best practice recommendations.”a scoping review. BMC Med Inform Decis Mak19, 110 (2019).
8. Khan , Shahidullslam, and AbuSayedMd Hoque. ‘Digital health data:a comprehensive review of privacy and security risks and some recommendations.” Computer Science Journal Of Moldova 71.2(2016): 273-292.
9. Ahmed, Samara M., and Adil Rajput. “Threats to patients’ privacy in smart healthcare environment.” Innovation in Health Informatics. Academic Press, 2020.375-393.
10. Keshta, Ismail, and Ammar Odeh. “Security and Privacy of Electronic health records: concerns and challenges.” Egyptian Informatics Journal 22.2(2021): 177-183.