ISSN: 2456-8090 (online)
DOI: https://doi.org/10.26440/IHRJ/0802.05634

REVIEW

QR CODE

Cybersecurity in Healthcare: Need of the Hour

ISHA THAKUR*[1], NIDHI BHALLA*[2], SURABHI DUGGAL[3]

ABSTRACT

Data is said to be the new oil which has the highest value in the black market and the healthcare sector has the highest amount of data in the form of patient information. The healthcare sector is poor in securely managing the data and cyber attackers leverage on this information to steal the data through phishing, ransomware and other methods. Phishing is the most common cybercrime in healthcare. In ransomware attacks, malware is injected into a system through phishing emails to encrypt sensitive data and demand ransom to restore access to the system. Insider threats are very tough to detect and prevent. The healthcare institutions have now realised there shortcomings and have adopted various cybersecurity methods and frameworks to protect them from heavy loss. Cybersecurity in healthcare can be improved by various ways such as encryption, network segmentation, employee training and regular security assessment. All cybersecurity strategies should incorporate the 5 C's – change, compliance, cost, continuity, coverage. Cybersecurity frameworks provide a structured approach to managing and mitigating cyber risks. During COVID 19 the healthcare sector was affected both workwise and digitally because of increased cyber-attacks.

KEYWORDS: Cybersecurity, Cybercrimes, COVID-19

INTRODUCTION

Recently, the world has moved on from keeping physical data to digitalised methods of data collection to keep data accurate, easily accessible and up-to-date. This modernization has also caused tremendous increase in cybercrimes. Healthcare sector is one the most affected sectors because of the huge amount of patient data it holds. In a recent study, 94% of healthcare institutions reported having been victims of cyberattacks[1].Cybercrime against health care has manifested as four specific threats: data Loss, monetary theft, attacks on Medical devices, and attacks on Infrastructure[2]. In this article, we will discuss about the various reasons for healthcare to be so prone to cyberattacks, various ways cyber attackers use to target healthcare institutions and how the healthcare sector has started adapting to this increased cybercrime and many methods and cybersecurity frameworks that have been implemented to protect the health sector. Cyber crime also took great toll on healthcare area during the crucial times of COVID 19 which shall also be put light on in this article.

WHY IS HEALTHCARE PRONE TO CYBERATTACKS?

1. High market value of Patient information: The thing that is valued the most is stolen the most. In the era of digitization, personal data holds a great value in black market. The data of patient not only has their medical history but also their bank and card details and other important information which increases the chance of cyberattacks.

2. Unprepared healthcare staff: The healthcare staff is not so well versed with cybersecurity due to the shortage of time, budget and resource constrainments. They require special training sessions to deal with cyberattacks but as we know they barely get time from their duties.

3. Medical devices can be easily attacked: Medical devices are used in every aspect of healthcare. Unlike computers, medical devices like X-ray machines , ECG monitors etc. Are not facilitated with advanced security parameters to protect them. This makes these devices entry points for hackers to Target the server and access confidential data[3].

FOUR BIGGEST CYBERSECURITY CHALLENGES IN HEALTHCARE

1. Phishing: Phishing is the most common cybercrime in healthcare. In 2022, human interaction had role in about 82% of the breaches. Phishing is the method of stealing sensitive information by infecting malware in innocuous emails. Email phishing are the most prevalent form of phishing. The emails are very convincing and have some point of appeal to make the

Submitted on: 03-Feb-2024; **Accepted on:** 08-May-2024

healthcare worker click on it[4].

2. Ransomware: Ransomware and phishing go hand in hand. In ransomware attacks, malware is injected into a system through phishing emails to encrypt sensitive data and demand ransom to restore access to the system. Healthcare is prone to such attacks as they have sensitive patient data and they receive tons of emails every day.

3. Medical device vulnerabilities: As we have discussed earlier, medical devices are prone to attacks. This 11 vulnerability allows attackers to gain access to data and even control the devices remotely and potentially risk the health of the patients.

4. Insider threats: Insider threats are very tough to detect and prevent. In 2022, 39% breaches were caused by an internal personnel. Insider threats could be from employees, contractors or anyone having access to patient's data. They can be intentional as in selling the information for money or unintentional like accidentally clicking on phishing emails.

WAYS TO IMPROVE CYBERSECURITY IN HEALTHCARE

1. Encryption: The act of scrambling 3 data in such a way that only authorised parties can access the information. Encryption is done using a key and algorithm such that anyone without the key cannot decrypt it.

2. Network segmentation: The practice of subdividing a computer network into smaller, distinct sub-networks is known as network segmentation. This improves the efficiency and security of the network and manages traffic more effectively.

3. Employee training: Training the healthcare staff about how to deal with cyberattacks through training sessions can benefit a lot.

4. Regular security assessment: Lastly, security assessments are a critical component. Frequent security audits help in identifying any fresh dangers that may have emerged[5].

THE 5 C'S OF CYBERSECURITY

All cybersecurity strategies should incorporate the following 5 C's:

1. Change: The cyberattacks evolve on daily basis. Keep up with it and adapt to changes accordingly. Maintaining cybersecurity is paramount in today's digital landscape. Regular updates, network monitoring, risk assessments, and robust incident response plans are essential components to safeguard data and systems against evolving threats.

2. Compliance: Awareness of cybersecurity laws and regulations is crucial for any organization. Complying with these regulations not only helps protect sensitive data but also mitigates the risk of severe legal consequences, such as substantial fines or legal repercussions. Seeking expert advice for compliance can be invaluable 14 in navigating the complexities of these regulations.

3. Cost: Investing in robust cybersecurity is a proactive and cost-effective strategy. Prioritizing security measures may seem costly initially, but it pales in comparison to the potential financial losses and operational disruptions caused by a cyberattack. Balancing cost and risk ensures a well-rounded approach that safeguards your business without compromising its long-term resilience.

4. Continuity: Badly, cyberattacks leave none. Even after implementing all the cybersecurity measures one may fall victim to cyberattack. But without giving up, one should implement a continuity plan. Having a well-defined continuity plan is crucial in today's digital landscape. It helps minimize 15 the impact of cyber threats and ensures a systematic response to potential disruptions. Regular testing and updating of the plan are also vital to adapt to evolving threats.

5. Coverage: Cybersecurity insurance can help mitigate 9 financial losses resulting from cyber attacks by covering costs like data breach response, legal expenses, and business interruption. There are 2 types of cyber insurance coverage. Network business interruption coverage can cover you against net income lost after a cyberattack. Network security coverage can reimburse customers after a data breach[6].

CYBERSECURITY FRAMEWORKS

Apart from this, a cybersecurity framework is laid down. 12 Cybersecurity frameworks provide a structured approach to managing and mitigating cyber risks. This facilitates communication among security leaders, ensuring a shared understanding of security postures and enabling effective collaboration, especially in a global and diverse landscape.

7 well-known frameworks are

1. NIST cybersecurity framework
2. ISO 27001 & 4 27002
3. SOC2
4. NERC-CIP
5. HIPAA
6. GDPR
7. FISMA

1. NIST: It was given by National institute of standards and technology. It is considered the gold standard for evaluating cybersecurity maturity, pinpointing security gaps, and ensuring compliance with cybersecurity regulations.

2. ISO 27001 & 27002: It was created by International organisation of standardization and are considered the international standard for validating a cybersecurity program.

3. SOC2: Service organisation 7 control type 2 is developed by American Institute of Certified Public Accountants to help verify that the third party are securely managing client data. SOC2 is one of the toughest frameworks to implement because of its comprehensive.

4. NERC-CIP: Northern American Electric Reliability Corporation- Critical Infrastructure Protection is designed to help the power sector rm mitigate rising attacks.

5. HIPAA:[8] Health Insurance Portability and Accountability Act focuses more on protecting the privacy and security of individuals' health information, rather than being a specific cybersecurity framework. It sets standards 5 for the use and disclosure of protected health information (PHI) by covered entities, including healthcare organizations, to ensure patient privacy is maintained.

6. GDPR:[16] The General Data Protection Regulation was adopted in 2016 to enhance individuals' control over their personal data and standardize data protection laws across EU member states.

7. FISMA — The Federal Information Security Management Act is a U.S. federal law that establishes a framework for securing government information and systems[7].

CYBERSECURITY REGULATIONS IN INDIA

Laws, rules, and guidelines that govern how data, networks, and information systems are safeguarded from cyberattacks are together referred to as cybersecurity regulations. In order to safeguard digital assets and lower the risks associated with cyberattacks, cybersecurity guidelines establish a framework of guidelines and norms that companies must adhere to.

Current cybersecurity legislation in India:

1. The Information Technology Act, 2000: The IT Act of 2000 officially takes into account transactions (both international and national) conducted using electronic data and offers legal authority to digital signatures for the authentication of any information. The Indian Parliament enacted this comprehensive section of regulations to assist e-governance, authorize electronic transactions, and address cybersecurity and cybercrime issues. After recognizing the Information Technology Act of 2000 [IT Act 2000], India became the 12th country to establish cyber legislation.

2. Information Technology (Amendment) Act 2008: The Information Technology Amendment Act 2008 (IT Act 2008) was approved in October 2008 and went into force the following year as a significant update to the Information Technology Act of 2000. The changes helped in the enhancement of the original bill, which had previously failed to establish the path for future IT-related development. It was praised as a major and long-awaited move toward a more strong cybersecurity framework in India. It also applies to any individual, firm, or organization (intermediaries) in India who uses computer resources, computer networks, or other information technology. It also covers web hosting, internet, network, and telecommunications service providers.

3. Information Technology Rules, 2011: Another major piece of cybersecurity law under the IT Act is the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011. The most significant modifications include provisions for intermediate regulation, modified penalties and violation costs for cybercrime, cheating, defamation, and unintentional sharing of private photographs, as well as censorship/restriction on particular opinion.

4. National Cyber Security Policy, 2013: In 2013, the Department of Electronics and Information Technology (DeitY) issued the National Cyber Security Policy 2013 as a security framework for public and commercial businesses to better protect themselves from cyber threats.

The National Cyber Security Policy aims to build and develop more dynamic policies to strengthen the safety of India's cyber environment. The policy seeks to train and develop approximately 500,000 expert IT professionals over the next five years.

5. IT Rules, 2021: The Ministry of Electronics and Information Technology released the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 on February 25, 2021, as an alternative for the IT Rules, 2011. The planned revisions aim to empower ordinary users of digital platforms to seek justice for claims and to hold companies accountable when their rights are violated, as well as to impose higher standards of investigation on organizations.

IT Rules, 2021 also differentiates between smaller and more prominent social media mediators based on user numbers, with bigger social media mediators bearing a far harsher responsibilities in terms of personal data security.

6. The Digital Personal Data Protection Act of 2023 (DPDP): On August 11, 2023, the Indian Central Government enacted the long-awaited Digital Personal Data Protection Act (DPDP). The act takes its broad understanding of personal data from the European Union's General Data Protection Regulation (GDPR) and attempts to protect data principals while restricting the activities of data brokers. The Act's major goal is to regulate the processing of digital personal data and respect people' right to data protection while acknowledging the necessity of processing and using such data for authorized reasons.

CYBERSECURITY ISSUES DURING COVID-19

During COVID 19 the healthcare sector shifted it's focus from security of their systems and devices to managing the pandemic and this gave the attackers increased chances of data breach. Cyber attackers leveraged 2 the increased reliance on remote working, decreased mobility, the closure of borders between countries and the disruption in supply chains. Hackers went on a run, hacking people who had access to digital networks such as computers, laptops, tablets, and phones. As a result, sensitive data such as passwords, usernames, bank account information, and other personal information were stolen. Some hackers exploited the stolen information to take funds from people's bank accounts. Similarly, at the height of the COVID-19 crisis, bank loan frauds proliferated rapidly, with many of the frauds focusing on fraud individuals of their money and personal information through internet purchasing. Phishing emails include fake web sites that can steal a user's personal information. Because most individuals used to rely on internet means to deal with the pandemic, they were prone to phishing efforts. Vigilance and robust cybersecurity measures are crucial to safeguard against such threats. COVID affected the healthcare sector a lot both workwise and digitally. So to sum up, Cybercrimes in today's world are like a pandemic with only 1 cure, that is, enhancing the cybersecurity[8].

CONCLUSION

Cybersecurity threats in healthcare continue to evolve, as do cybersecurity solutions to address these threats. To keep ahead of these risks, one must raise thier level of awareness of what is going on and transmit more information with their peers and coworkers. Healthcare cybersecurity is a critical necessity for all health care companies including the field of biotechnology coverage, healthcare providers, pharmaceutical companies, and medical device manufacturers. It involves a number of measures designed to protect organizations from internal and external cyber-attacks, protect the availability of medical services, maintain confidentiality, ensure the effective functioning of medical systems and tools, the integrity of patient data, and follow regulatory requirements. Ransomware attacks, data breaches, phishing emails, insider threats, and medical device vulnerabilities all pose risks to healthcare professionals. These attacks have the potential to compromise patient data and interrupt vital medical services. Inadequate endpoint device management, a lack of security awareness, an insecure remote work environment, insufficient business continuity plans, a lack of coordinated reaction to incidents, and the difficulty in managing safety investments and service delivery quality are the main challenges that health care organizations face. Regular risk assessments, training personnel on recommended procedures, encrypting sensitive data, upgrading and modifying systems, and working together with cybersecurity professionals may all help organizations improve their cybersecurity. Healthcare institutions must continue to provide assistance to cybersecurity professionals as they work to protect patient data. There is no better time than the present to strengthen safeguards for cybersecurity while also improving personnel talents and understanding.

REFERENCES

1. Filkins B. Health care cyberthreat report: Widespread compromises detected, compliance nightmare on horizon paper. Available from: http://www.sans.org/reading-room/whitepapers/firewalls/paper/34735. [Last Accessed June 24th, 2023].
2. Jalali MS, Kaiser JP. Cybersecurity in Hospitals: A Systematic, Organizational Perspective. J Med Internet Res. 2018;20(5):e10059. https://doi.org/10.2196/10059.
3. Mejía-Granda CM, Fernández-Alemán JL, Carrillo-de-Gea JM, García-Berná JA. Security vulnerabilities in healthcare: an analysis of medical devices and software.

Med Biol Eng Comput. 2024;62(1):257-73. https://doi.org/10.1007/s11517-023-02912-0.

4. Alawida M, Omolara AE, Abiodun OI, Al-Rajab M. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. J King Saud Univ Comput Inf Sci. 2022;34(10):8176-8206. https://doi.org/10.1016/j.jksuci.2022.08.003.

5. He Y, Aliyu A, Evans M, Luo C. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. J Med Internet Res. 2021 Apr 20;23(4):e21747. doi: 10.2196/21747. Erratum in: J Med Internet Res. 2021;23(4):e29877.

6. Mathew A. The 5 Cs of Cybersecurity and its Integration with Predictive Analytics, International Journal of Computer Science and Mobile Computing 2023;12(1):47-50.

7. Taherdoost H. Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. Electronics. 2022; 11(14):2181. https://doi.org/10.3390/electronics11142181

8. Ignatovski M. Healthcare Breaches During COVID-19: The Effect of the Healthcare Entity Type on the Number of Impacted Individuals. Perspect Health Inf Manag. 2022;19(4):1c.

Cite this article as:
Thakur I, Bhalla N, Duggal S. Cybersecurity In Healthcare: Need of the Hour. Int Healthc Res J. 2024;8(2):RV1-RV5. https://doi.org/10.26440/IHRJ/082.05634

AUTHOR AFFILIATIONS: (*Corresponding Author)

1. BDS Final Year Student, Department of Public Health Dentistry, Himachal Dental College, Sundernagar, India (https://orcid.org/0009-0002-5308-6402)
2. Intern, Department of Public Health Dentistry, Himachal Dental College, Sundernagar, India (https://orcid.org/0009-0002-5193-8253)
3. Assistant Professor, Department of Prosthodontics, Crown and Bridge, School of Dental Sciences, Sharda University, Greater Noida, UP. India (https://orcid.org/0000-0002-9651-5054)

Source of support: Nil, **Conflict of interest:** None declared

Contact Corresponding author at: nidhiibhalla890[at]gmail[dot]com