Mesopotamian Journal of Artificial Intelligence in Healthcare
Vol.2023, **pp**. 82–84
DOI: https://doi.org/10.58496/MJAIH/2023/000 ; ISSN: 3005-365X
https://mesopotamian.press/journals/index.php/MJAIH

Research Article

A Review of the State of Cybersecurity in the Healthcare Industry and Propose Security Controls

Aishwarya Ulhas Desai [1], Manal Desai, MBBS, MPH [1, *]

[1] *Department of Epidemiology, Human Genetics and Environmental Sciences, The University of Texas Health Science Center at Houston, USA*

ARTICLE INFO

Article History

Received 17 Jun 2023
Accepted 11 Nov 2023
Published 9 Dec. 2023

Keywords

Healthcare

Cybersecurity

Healthcare Industry

ABSTRACT

Our study aims to identify the state of cybersecurity in the healthcare domain. Cyber incidents, including ransomware and similar cyber-attacks, impact healthcare entities. The review highlights the government's efforts to protect citizens' health information by passing laws regulating the healthcare industry. The review targeted healthcare-related laws in the United States, the European Union, Singapore, and India. The study identified that while developed countries like the United States, the European Union, and Singapore have health data privacy laws, developing countries like India still need data privacy laws. The nature, value, and sensitivity of data retained by healthcare entities make the healthcare domain a rich target for cyber threat actors. Based on the study, the paper proposes security practices, including security monitoring, secure network architecture, information technology vulnerability management, cyber policies, and user training, that can help prevent cyber-attacks on healthcare entities.

1. INTRODUCTION

In today's age, computers and the internet are vital to human civilization, safety, and development. There is an increasing dependence on computers in the healthcare domain, ranging from storing government-regulated Patient Health Information (PHI) records to high-tech medical computing devices such as surgical robots; thus, cybersecurity has become an essential aspect of the healthcare industry. The basic information security requirements in the healthcare domain can be mapped to the National Institute of Standards and Technology's (NIST) Confidentiality, Integrity, and Availability (CIA) triad [1]. The healthcare domain needs to assure the confidentiality and integrity of the patient data and ensure the availability and integrity of the information systems supporting day-to-day operations. The threat actors targeting the healthcare sector are motivated by monetary gains. Threat actors understand the nature of sensitive information retained by the healthcare systems and the critical availability of the healthcare systems within the healthcare organizations, thus monetizing on the industry-wide weak cybersecurity practices. A cybersecurity compromise can lead a threat actor to exfiltrate and leak sensitive data from the compromised hospital computer network or even cause life-threatening severe injuries due to malfunctioning medical devices during a cyber-attack. In a study by D. Y. Huang et al. (2018, May) Tracking ransomware end-to-end, the author tracked Bitcoin cryptocurrency wallets involved in ransomware attacks and identified 16 million USD in ransom payments made by 19,750 potential victims over two years. This shows the breadth of the profitability of ransomware attacks and why the number of ransomware attacks has increased yearly.

2. DISCUSSION

Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 were created to protect healthcare and patient information [3]. These are United States-based act that enforces the adoption of cybersecurity best practices and imposes fines for violations of the acts. HIPAA's security rule requires covered entities to comply and safeguard Patient Health Information (PHI). The entities had a contractual obligation to comply with HIPPA, but it did not enforce the obligation [3]. HITECH Act is an extension of HIPPA that ensures that healthcare entities are held liable and penalized for violating HIPPA compliance [3]. The government passed the supporting acts to enforce cybersecurity on healthcare entities.

The General Data Protection Regulation (GDPR) law was implemented in Europe in 2018. GDPR covers user data privacy in several industry domains, including healthcare data. The law makes healthcare entities get user consent before collecting, processing, and sharing patient data [4]. GDPR ensures the privacy and security of healthcare data and imposes fines for

*Corresponding author. Email: manali.u.desai@uth.tmc.edu

violating GDPR law while collecting, handling, and processing healthcare data. In addition, Healthcare 4.0 Architecture was proposed in the European Union to safely transfer patient information within National Health Systems (NHS) [4].

Similarly, the Personal Data Protection Act (PDPA) and National Electronic Health Record (NEHR) in Singapore provide protection of personal data, including health information, set a baseline of security compliance, and impose fines on failure to comply with the law [5]. While developed countries like the US and EU already have robust laws to protect user health information, developing countries like India do not have explicit healthcare data protection laws [5].

The study suggested low awareness regarding the importance of cyber security in the healthcare industry [6]. The author conducted telephone interviews with 99 healthcare executives. Fifty-three executives confirmed that their organizations have a budget for their cyber security program, and 33 responded that they did not have a cyber security budget [6].

Modern problems need modern solutions. Researchers are implementing and testing Machine Learning (ML) and Artificial Intelligence (AL) to optimize predictive cyber risk analytics on healthcare entities during a future pandemic [7]. The author proposed using open-source intelligence (OSINT) to gather public domain data, including public repositories like Shodan, to collect training data used to train the ML models [7]. Healthcare entities should adopt a defense-in-debt approach to secure Information Technology (IT). Mechanisms should implemented to detect, contain, and respond to a cyber threat at all stages of the cyber-attack kill chain. Healthcare entities should train users to identify phishing mechanisms and help improve users' cybersecurity hygiene practices, like using strong passwords and avoiding password reuse. Networks should be segregated by creating Virtual Local Area Networks (VLAN). Users in the billing and administrative department do not need access to the other part of the network where sensitive servers supporting medical equipment are hosted and Patient Health Information (PHI) is stored. Thus, the segregation of the network and use of zero trust network architecture limits the TA's access to the part of the network and helps to contain the compromise. Implementing a complex password policy, password rotation, password expiration policy, and a Multifactor Authentication mechanism minimizes the attack surface. Implement the principle of least privileges access control mechanism. This mechanism ensures that the users do not have overly permissive permissions to access the computer resources. If a user account gets compromised, the TA will have limited access through the computer network, limiting the scope of the breach. Deployment of Endpoint detection and response tools enables the security teams to detect and respond to threats efficiently. Network firewall and endpoint telemetry logging allows the investigator to retail long-term historical data valuable during a cyber incident. Studie by Kruse et al. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends, and Welch, S. S. (2015). Five things providers need to know about cybersecurity, summarized similar methods to protect the organization from cyber threats. Furthermore, healthcare providers should implement a cybersecurity program that follows the NIST framework, focusing on the continuous improvement methodology to secure networks. The cybersecurity program should implement mechanisms to identify and patch weaknesses, build a robust detection, response, and recovery mechanism, and implement lessons learned from previous incidents in identifying, protecting, detecting, and responding to future cyber threats.

3. CONCLUSION

Although healthcare entities worldwide have low cybersecurity awareness, government and regulatory bodies are becoming aware of the risk of cyber-attacks on the healthcare industry. They are creating laws for healthcare entities to protect their citizens from such incidents. Implementing modern tools, techniques, and proposed cyber procedures to defend against cyber threats can mitigate the risk.

ABBREVIATIONS AND ACRONYMS

AI: Artificial Intelligence
CIA: Confidentiality, Integrity, and Availability
EU: European Union
GDPR: General Data Protection Regulation
HITECH: Health Information Technology for Economic and Clinical Health
HIPAA: Health Insurance Portability and Accountability
IT: Information Technology
ML: Machine Learning
NEHR: National Electronic Health Record
NHS: National Health Systems
NIST: National Institute of Standards and Technology
OSINT: Open-Source Intelligence
PHI: Patient Health Information
PDPA: Personal Data Protection Act
US: United States
USD: United States Dollar
VLAN: Virtual Local Area Networks

Funding

The authors had no institutional or sponsor backing.

Conflicts Of Interest

The author's disclosure statement confirms the absence of any conflicts of interest.

Acknowledgment

The authors extend appreciation to the institution for their unwavering support and encouragement during the course of this research.

References

[1] National Institute of Standards and Technology (NIST). (December 2020). Detecting and Responding to Ransomware and Other Destructive Events. https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html

[2] D. Y. Huang, M. M. Aliapoulios, V. G. Li, L. Invernizzi, E. Bursztein, et al., "Tracking Ransomware End-to-end," In IEEE Symposium on Security and Privacy (SP), pp.1-6, July 2018. https://doi.org/10.1109/SP.2018.00047

[3] What is the HIPPA Act? (n.d.). The HIPAA Journal. https://www.hipaajournal.com/what-is-the-hitech-act/

[4] X. Larrucea, M. Moffie, S. Asaf, and I. Santamaria, "Towards a GDPR compliant way to secure European cross border Healthcare Industry 4.0," *Computer Standards & Interfaces*, vol.69, pp.103408, March 2020. https://doi.org/10.1016/j.csi.2019.103408

[5] D. Jain, "Regulation of Digital Healthcare in India: Ethical and Legal Challenges," *Healthcare*, vol.11, no.6, pp.911, March 2023. https://doi.org/10.3390/healthcare11060911

[6] A. Garcia-Perez, J. G. Cegarra-Navarro, M. P. Sallos, E. Martinez-Caro, and A. Chinnaswamy, "Resilience in healthcare systems: Cyber security and digital transformation," *Technovation*, vol.121, pp.102583, March 2023. https://doi.org/10.1016/j.technovation.2022.102583

[7] E. G. Spanakis, S. Bonomi, S. Sfakianakis, G. Santucci, S. Lenti, et al., "Cyber-attacks and threats for healthcare – a multi-layer thread analysis," In Proceedings of International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), pp.1-6, August 2020. https://doi.org/10.1109/EMBC44109.2020.9176698

[8] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technology and Health Care*, vol.25, no. 1, pp.1-10, February 2017. https://doi.org/10.3233/THC-161263

[9] S. S. Welch, "Five things providers need to know about cybersecurity," *Journal of the Medical Association of Georgia*, vol.104, no.1, pp.40-42, January 2015.