

Review Analysis of Cyber Security in Healthcare System: A Systematic Approach of Modern Development

Venkateswaran Radhakrishnan

Faculty, Cyber and Information Security-IT, College of Computing and Information Sciences,
University of Technology and Applied Sciences, Salalah, Oman

Correspondence should be addressed to Venkateswaran Radhakrishnan; r.venkateswaran2020@gmail.com

Copyright © 2023 Made Venkateswaran Radhakrishnan. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ABSTRACT- The healthcare industry provides medical devices such as pharmaceuticals. The third-party vendor can also pose a risk to the organization. Cyber security if they are not properly vetted and do not have adequate security measures in place. These will help to mitigate and other cyber security risks, healthcare organizations should implement a range of security measures. Regular security assessments in healthcare organizations should conduct a regular security assessment to identify vulnerable in their systems and network. Distributed denial of services attacks where criminals overload the healthcare system. Health care system servers with traffic, causing them to crash and preventive. Lag mate users from accessing the system's network, stealing data, and causing damage to the system. Ensure that these tools are updated regularly to protect against the latest threats. Regularly check the backup data and critical data and store them in a secure location. Monitoring network activity to detect and respond to any potential security incidents conduct regularly.

KEYWORDS- Cyber, Data, Healthcare Security, Malware, Systematic, Technology

I. INTRODUCTION

Cyber security is an increasingly important concern in the healthcare system. Due to the sensitive and confidential nature of the information that is stored and transmitted within this system. Healthcare organization faces numerous modern threats to their systems and network [1]. Ransomware attacks are the type of malware that encrypts a victim's data and demands payment in exchange for the decryption key. Healthcare organization is particularly vulnerable to these attacks due to the critical nature of their data and their potential impact on their patient [3]. Phishing is a social engineering attack that tricks the victim into divulging sensitive information and downloading malware. Healthcare organizations are particularly vulnerable to these attacks because they often deal with a large volume of emails and may be more likely to click on malicious links or attachments [4]. Insider threats refer to the risk posed by employees and others. An insider who has access to sensitive information.

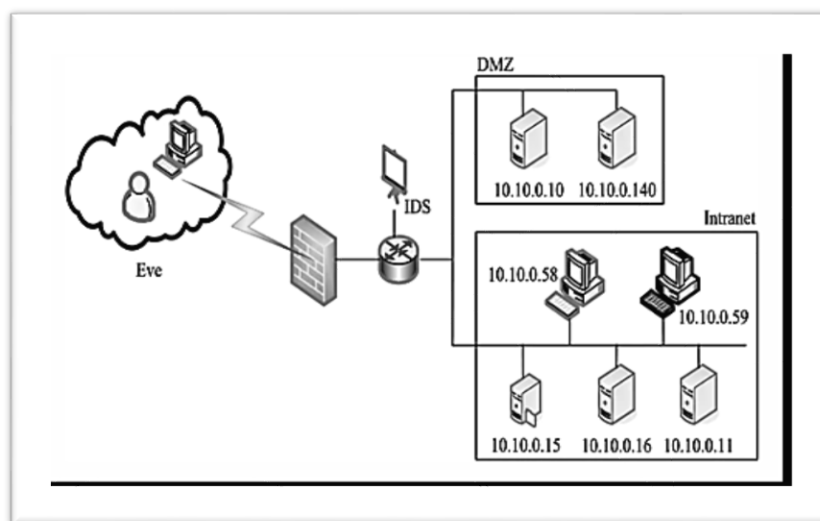


Figure 1: Modern cyber security [10]

These threats can range from accidental data breaches to international theft or sabotage. Third party vendor risks healthcare organizations often rely on third party vendors for

a range of services. In medical industry third party vendors are used to internal networks for catch and remove the data from the systems [5]. These are a very dangerous for the

medical industry to driven out there data without their permissions. In the medical industry, healthcare cyber security is tactical for the organizations and biotechnology [10].

II. OBJECTIVES

- To safe from ransomware attacks in the cyber security healthcare system
- To understand from phishing attacks in the cyber security system
- To avoid the insider threat in the cyber security attack in the healthcare system
- To explain third party vendor risks in the cyber security system
- To safe the organizations from the external and internal cyber attack
- To ensure the proper medical system and equipment is safe from the cyber security system

- To analyze the solutions for the healthcare industry from the cyber security networks

III. METHODOLOGY

In this research, researchers could not find any primary data for this is why researchers are researches for using secondary data. Researchers get information from the web site on Google scholar. Researchers know the in cyber security access control should be implement to ensure that only authorized personal have access to sensitive data[5]. In the cyber security, systems data encryption should be use to protect sensitive data from unauthorized access or theft. In the business purposes, cyber security is the crucial for the information security to the today's regular in digital age [15]. In the organization, many healthcare hospitals include the specialized information's such as E-prescribing, EHR system, system of radiology information's, and support system of medical information. IT security involving the cyber threat in healthcare for deals with endangers patient safety.

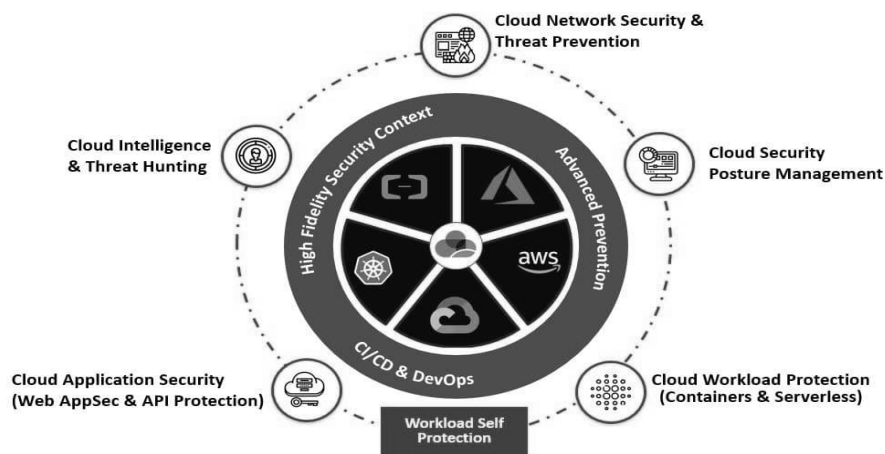


Figure 2: Pillars of Cloud computing cyber security [7]

IV. RANSOMWARE ATTACKS IN THE CYBER SECURITY HEALTH CARE SYSTEM

Ransomware attacks are one of the best malware in the cyber security systems. Healthcare systems are attractive target for the Ransomware system in the cyber security industry [12]. It is attractive target because they store a vast amount of sensitive and personal data, including medical records, financial information, and personal information. In the cyber-Attacks healthcare is the prime target that remove the sensitive information [14]. Ransomware attacks is the Cyber criminals where encrypt and healthcare system data and demand a ransom in exchange for the decryption key [10]. The numbers of data violates and increased by more than five years stated by HHS office in US civil rights. Healthcare organizations enable to use the digital information by reducing complexity, risk, and cost. Cyber criminals send emails and messages that appear to be from a trusted source in order to risk healthcare system employees into receiving sensitive information and clicking on malicious link [5].

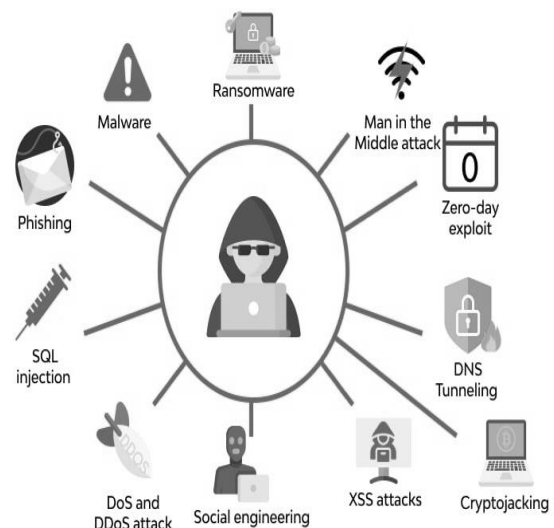


Figure 3: Types of cyber security [17]

Access control access to sensitive data and system to be restricted to authorized personal only. Therefore, access should be granted on a need to know basis. Auditing system

in the company to detect suspicious activity and identified potential insider's threats.

V. INSIDER THREAT IN THE CYBER SECURITY ATTACKS

Insider threats are the legitimate to access the network for harm to the organizations. Most of the cases inside threat is detect can be difficult for this is why it is go unnoticed in the month or years [5]. Malicious insiders are individuals who intentionally use their access to steal the data and cause damage or disrupt the organizations [6].

They may be motivated by financial gain, revenge, and ideology. Careless insiders who accidentally exposed sensitive data or information [9].

It is introduced to security vulnerabilities into the organizations system. They may lack awareness of security of best practices or fail to follow established products [1]. Compromise insiders those who are access credential information from taken out from the systems. Hackers may use these credentials to gain access to the organizations' systems and data [2].

Industries and corporate sectors should provide regular training and awareness program to educate employee on security best for the organizations.

VI. THIRD PARTY VENDOR RISK IN THE CYBER SECURITY SYSTEM

Third party vendor risk is a significant concern in the cyber security system. It can create vulnerabilities that can be exploited by malicious sectors [5]. A third party vendor is any external entities that provide goods and services to organizations, such as cloud computing services[2], software, or hardware. According to the source [7] Cloud security is a responsibility that is shared between the cloud provider and the customer. This diagram (figure 2) shows that the 6 pillars of cloud security. It can potentiality provide an entry point for cybercriminals to access an organizations? Therefore, it is an essential to manage third party vendor risks as part on overall cyber security strategy [9].

One way to manage third party vendor risk is to conduct due diligence before engaging with a vendor. This include the accessing the vendors posture.

It is as well as their record of accomplishment with order organizations [10]. It is also important to ensure that the vendor has appropriate security controls in place

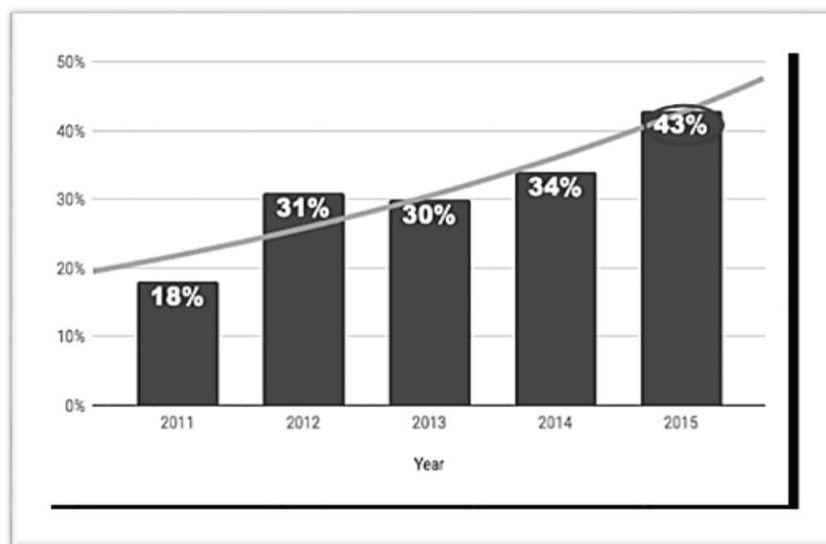


Figure 4: Third party vendor risk increasing [11]

The place is such as multiple sectors, multifactor authentication, and encryptions. Once a third party vendor is engaged is a crucial to monitor there activity and performance. It is ensure that they are adhering to security standards and contractual obligations [11]. Regular security assessment and audits can help identified and address any vulnerabilities or potential risk. In security managing third party vendor risk (figure 4) is a critical component of a robust cyber security [12]. According to elandcables.com studies, it requires proactive due vigilance, ongoing monitoring, and effective risk mitigation strategies to ensure the third party vendors do not comprise an organizations security.

VII. SAFE THE ORGANIZATION FROM EXTERNAL AND INTERNAL CYBER ATTACKS

Protecting organizations from internal and external cyber-attacks requires a multifaceted approach (see figure 5). Here the some steps that can help improve the organization in cyber security posture. Conduct a cyber-security risk assesses is the organizations vulnerabilities and potential impact of a cyber-attack [5]. Identified the assists of that need to protect the possible attack vectors. Develop a comprehensive cyber security policy to establish a clear set of guidelines and procedures [9].The organizations employee and contractors must follow to ensure cybersecurity. This policy should include password management, remote access software installation an employee training. Implement cyber security training all employees on cyber security [12]. The

cyber security is the best practices including how to identify and report suspicious activity.

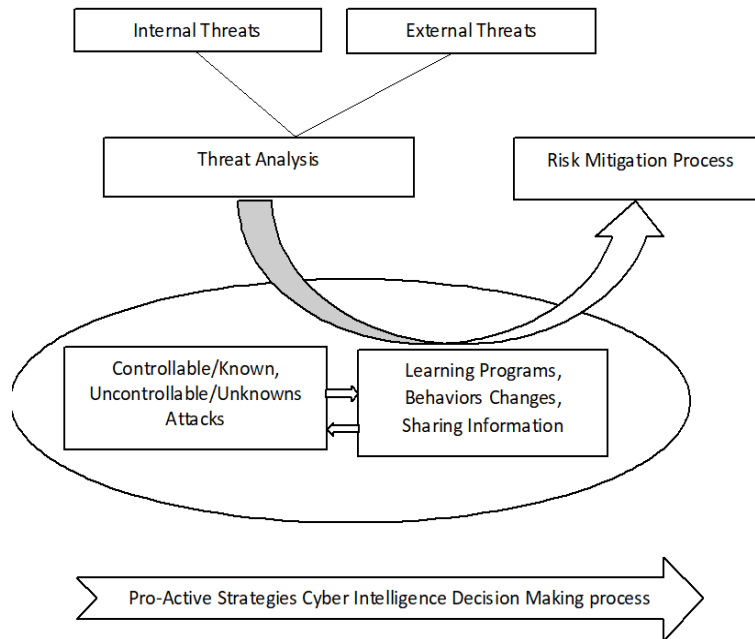


Figure 5: Internal and external cyber-attack [11]

How to use strong password and how to recognize the phishing emails and social engineering attacks. Developing cyber security such as firewalls, intrusion detection, preventive system, antivirus software, and data encryption.

VIII. PROBLEM STATEMENT

The problem statement of the cyber security industry is the need to protect digital systems network. It is protect the device from unauthorized system and protect the system malware. As the world become increasingly reliant on technology [5]. It is the risk of cyber-attacks has grown exponentially according to this source [9]. Cyber threats include malware, phishing attacks, and social engineering. Now day's cyber security is a big problem of many organizations. It is not too secured from the many of hackers to driven out files and information's in the organizations.

IX. CONCLUSION

Present day's cyber security is the biggest problem in the world. Cybersecurity is a constantly involving field that encompasses a wide range of technologies, practices, and politics. Cyber security aimed at protecting computer systems, networks, and data from unauthorized access. The rapid advancement of the technology and the increasing reliance on digital services and online platforms have made for cyber security.

REFERENCES

[1] Wanasinghe, T. R., Wroblewski, L., Petersen, B. K., Gosine, R. G., James, L. A., De Silva, O., ... & Warriar, P. J. (2020). Digital twin for the oil and gas industry: Overview, research trends, opportunities, and challenges. *IEEE access*, 8, 104175-104197. Retrieved from: <https://ieeexplore.ieee.org/iel7/6287639/8948470/09104682.pdf> [Retrieved on: 28/03/2023]

[2] Taimoor, N., & Rehman, S. (2021). Reliable and resilient AI and IoT-based personalised healthcare services: A survey. *IEEE Access*, 10, 535-563. Retrieved from: <https://ieeexplore.ieee.org/iel7/6287639/9668973/09658494.pdf> [Retrieved on: 28/03/2023]

[3] Guzmán, J. A., & Núñez, F. (2021). A cyber-physical systems approach to collaborative intersection management and control. *IEEE Access*, 9, 99617-99632. Retrieved from: <https://ieeexplore.ieee.org/iel7/6287639/9312710/09480804.pdf> [Retrieved on: 28/03/2023]

[4] Rodriguez, E., Otero, B., Gutierrez, N., & Canal, R. (2021). A survey of deep learning techniques for cybersecurity in mobile networks. *IEEE Communications Surveys & Tutorials*, 23(3), 1920-1955. Retrieved from: https://upcommons.upc.edu/bitstream/handle/2117/355516/survey_DL_cyber%2B-%2Bfinal.pdf?sequence=3 [Retrieved on: 28/03/2023]

[5] Mullet, V., Sondi, P., & Ramat, E. (2021). A review of cybersecurity guidelines for manufacturing factories in industry 4.0. *IEEE Access*, 9, 23235-23263. Retrieved from: <https://www.ideals.illinois.edu/items/126167/bitstreams/413034/object?dl=1> [Retrieved on: 28/03/2023]

[6] Mullet, V., Sondi, P., & Ramat, E. (2021). A review of cybersecurity guidelines for manufacturing factories in industry 4.0. *IEEE Access*, 9, 23235-23263. Retrieved from: <https://ieeexplore.ieee.org/iel7/6287639/9312710/09345803.pdf> [Retrieved on: 28/03/2023]

[7] Chkadmin (2022) what is cloud security? understand the 6 pillars, Check Point Software. Check Point Software. Available at: <https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/> (Accessed: April 22, 2023).

[8] Marques, G., Pitarma, R., M. Garcia, N., & Pombo, N. (2019). Internet of things architectures, technologies, applications, challenges, and future directions for enhanced living environments and healthcare systems: a review. *Electronics*, 8(10), 1081. Retrieved from: <https://www.mdpi.com/2079-9292/8/10/1081/pdf> [Retrieved on: 28/03/2023]

- [9] Tidjon, L. N., Frappier, M., & Mammari, A. (2019). Intrusion detection systems: A cross-domain overview. *IEEE Communications Surveys & Tutorials*, 21(4), 3639-3681. Retrieved from: <https://arxiv.org/pdf/2302.14536> [Retrieved on: 28/03/2023]
- [10] Zambrano, P., Torres, J., Tello-Oquendo, L., Jácome, R., Benalcázar, M. E., Andrade, R., & Fuertes, W. (2019). Technical mapping of the grooming anatomy using machine learning paradigms: An information security approach. *IEEE Access*, 7, 142129-142146. Retrieved from: <https://ieeexplore.ieee.org/iel7/6287639/8600701/08845626.pdf> [Retrieved on: 28/03/2023]
- [11] Lopez, T., Tun, T., Bandara, A., Mark, L., Nuseibeh, B., & Sharp, H. (2019, May). An anatomy of security conversations in stack overflow. In 2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Society (ICSE-SEIS) (pp. 31-40). IEEE. Retrieved from: <https://oro.open.ac.uk/59243/1/PID5783059-CRC.pdf> [Retrieved on: 28/03/2023]
- [12] Langehaug, T. J., Graham, S. R., Kabban, C. M. S., & Borghetti, B. J. (2022). MADFAM: MicroArchitectural Data Framework and Methodology. *IEEE Access*, 10, 23511-23531. Retrieved from: <https://ieeexplore.ieee.org/iel7/6287639/9668973/09718324.pdf> [Retrieved on: 28/03/2023]
- [13] Liu, Y., Hassan, K. A., Karlsson, M., Pang, Z., & Gong, S. (2019). A data-centric internet of things framework based on azure cloud. *IEEE Access*, 7, 53839-53858. Retrieved from: <https://ieeexplore.ieee.org/iel7/6287639/6514899/08698762.pdf> [Retrieved on: 28/03/2023]
- [14] Ashenden, D., Ollis, G., & Reid, I. (2022, October). Dancing, not Wrestling: Moving from Compliance to Concordance for Secure Software Development. In 37th IEEE/ACM International Conference on Automated Software Engineering (pp. 1-9). Retrieved from: https://yuxi-wu.github.io/pubs/sp22_sok_socialcybersecurity.pdf [Retrieved on: 28/03/2023]
- [15] Jiang, B., Li, J., Yue, G., & Song, H. (2021). Differential privacy for industrial internet of things: Opportunities, applications, and challenges. *IEEE Internet of Things Journal*, 8(13), 10430-10451. Retrieved from: <https://www.academia.edu/download/96834000/2101.10569v3.pdf> [Retrieved on: 28/03/2023]
- [16] FAQ: In Oil & Gas What is upstream and downstream?: Eland Cables (no date) FAQ: In Oil & Gas what is upstream and downstream? |Eland Cables. Available at: <https://www.elandcables.com/the-cable-lab/faqs/faq-what-are-upstream-and-downstream-works-in-the-oil-gas-industry> (Accessed: April 14, 2023).
- [17] Wallarm (2023) what is cyber-attack meaning? types and examples, RSS. Available at: <https://www.wallarm.com/what/what-is-a-cyber-attack> (Accessed: April 14, 2023).
- [18] Kruse, C.S. et al. (2017) "Cybersecurity in Healthcare: A systematic review of modern threats and Trends," *Technology and Health Care*, 25(1), pp. 1-10. Available at: <https://doi.org/10.3233/thc-161263>.
- [19] McKeon, J. (2023) Quantifying the financial impact of healthcare ransomware attacks, HealthITSecurity. HealthITSecurity. Available at: <https://healthitsecurity.com/news/quantifying-the-financial-impact-of-healthcare-ransomware-attacks> (Accessed: April 20, 2023).
- [20] Basic level certification - international association for ... - IAHSS (no date). Available at: <https://www.iahss.org/page/basic> (Accessed: April 20, 2023).
- [21] Ambulatory tracks selections (no date) The Healthcare Security Institute. Available at: <https://www.thehealthcaresecurityinstitute.com/new-page-2> (Accessed: April 20, 2023).
- [22] Michali (2023) Cyberattacks on the healthcare sector, Check Point Software. Check Point Software. Available at: <https://www.checkpoint.com/cyber-hub/cyber-security/what-is-healthcare-cybersecurity/cyberattacks-on-the-healthcare-sector/> (Accessed: April 20, 2023).
- [23] Biggest cyber threats in healthcare (updated for 2023): Upguard (no date) RSS. Available at: <https://www.upguard.com/blog/biggest-cyber-threats-in-healthcare> (Accessed: April 20, 2023).
- [24] 9 reasons healthcare is the biggest target for cyberattacks (2022) Swivel Secure. Available at: <https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/> (Accessed: April 20, 2023).
- [25] HealthITSecurity (no date) Home, Healthcare Information Security. Available at: <https://healthitsecurity.com/topic/latest-health-data-breaches> (Accessed: April 20, 2023).