Critical Analysis of Attack Landscape and Mitigation Strategies

This report deeply explains the current threat landscape which focuses on actors , threats, trends, and their techniques (Nurse et al., 2011). It is based on the analysis that how to make an attack tree for a fictional healthcare organization and consider which security measures should be taken into account in order to mitigate the identified attack vectors.

a) Organization and Assumptions

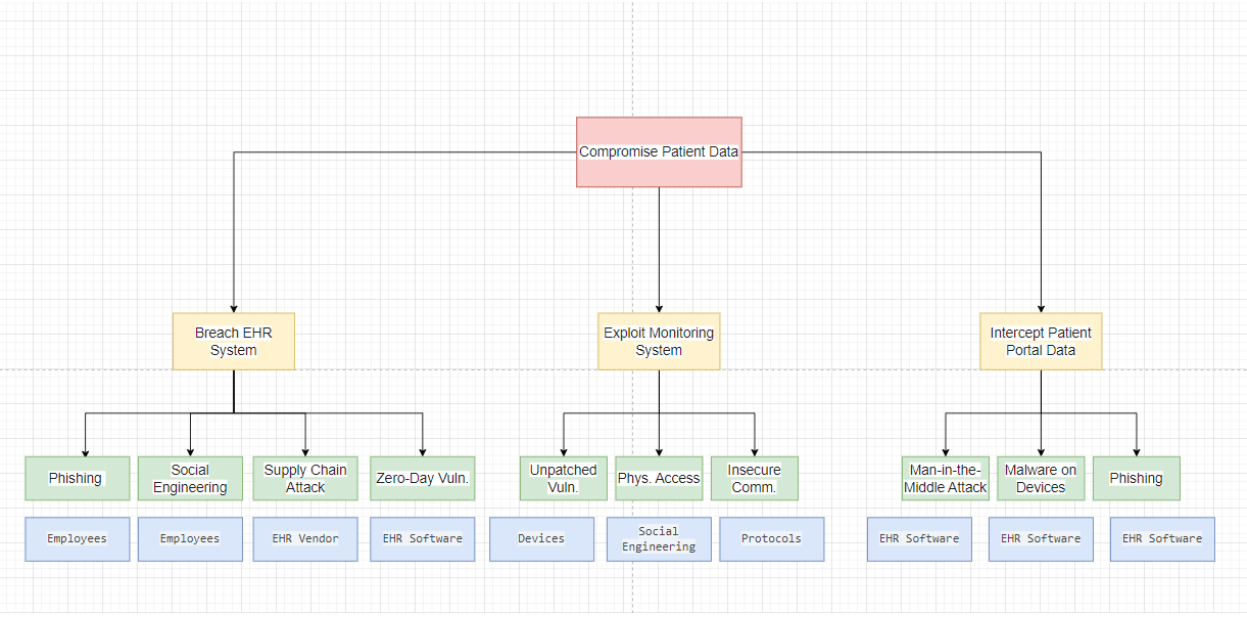
Organization: Any Hospital which is a medium-sized regional hospital having least 200 beds and 500 employees.

Assumptions:

- Acme Hospital uses a machine as EHR systems for storing patient data.
- Some of the hospital uses remote patient monitoring systems for some patients.
- Acme Hospital has an online patient portal for bill payments and appointment scheduling.
- The hospital allow the employees to remotly access the network for administrative tasks .

The above mentioned assumptions create a risk which is vulnerable to cyberattacks targeting data of patient , their finances and interference in operations. This is inlined with the current threat landscape , which focuses on the healthcare as a prime target for financially motivated state-sponsored people and cybercriminals. (Nurse et al., 2011)

b) Attack Tree



Root Node: Compromise Patient Data

Level 1:

- Unauthorized access to EHR system
- Manipulating remote patient monitoring system weaknesses
- Tampering the data which is transmitted through the online patient portal (Lezzi, Lazoi, & Corallo, 2018)
- **Level 2 (Breach EHR System):**
- Phishing attacks against employees with access to the EHR system
- To gain login credentials through social engineering attacks (Veitch et al., 2013)
- The EHR software have zero vulnerabilities
- Attack supply chain attack targeting EHR vendor (Edgar & Manz, 2017)

Level 3 (Exploit Remote Monitoring System):

- Unpatched vulnerabilities in the monitoring devices
- Nonsecure communication protocols between the hospital network and devices
- Unauthorized people gaining physical access to the devices

Level 3 (Intercept Data from Patient Portal):

- Man in the middle attacks
- Phishing attacks to steal the login credentials of patients
- Installing harmful softwares on patient devices for capturing keystrokes

c) Security Recommendations and Justification

To enhance the cyber security of the hospital and eliminate potential cyber security threats it is mandatory to provide some of security recommendations. (Edgar & Manz, 2017) It is also important to understand the significance of these recommendations and implement them efficiently

1. **Multi-factor Authentication (MFA):** This adds an additional layer of security by asking user to provide different forms of verifications before reaching out to the system's sensitive information and data. (Takahashi & Kadobayashi, 2015)The hospitals can significantly reduce the risk of unauthorized access and to the important user credentials , the MFA is implemented on all the user accounts.These recommendations

align with practices that can be helpful to safeguard the patients data like HIPAA Health Insurance Portability and Accountability Act).

2. **Regular Security Awareness Training**: It is very crucial to train the employees to make them capable respond and recognizing potential threats efficiently. The hospitals can train the staff about security threats like social engineering techniques, reinforce cybersecurity and phishing attacks.(Ali et al., 2018) This promote the culture of security awareness all over the organization eliminating cyberattacks and also strengthening the human element of cybersecurity. These trainings can eliminate the likelihood of successful cyberattacks.

3. **Vulnerability Management:** Some of the measures must be taken to prevent the cyber attacker from accessing the systems like prioritizing, identifying and reducing the security vulnerabilities in the software applications.(Veitch et al., 2013) The risk of exploitation can be minimized by regularly updating the software and firmware on all the devices including the employees' workstations, monitoring devices and EHR systems.(Takahashi & Kadobayashi, 2015) The hospitals can eliminate the risk of cyber threats by knowing the vulnerabilities by implementing potential vulnerability management practices.

4. **Network Segmentation:** To limit the scope of potential cyberattacks and restrict the flow of traffic the network must be divided into smaller and isolated segments.The Hospital can minimize the impact of the successful breach and the lateral moments by attackers by implementing network segmentation to isolate critical systems like patient portals and EHRs.Network segmentation is particularly related to the healthcare sector as the integrity and confidentiality of patient data are important.

5. **Data Encryption:** It is a method to protect sensitive information from unauthorize access by apply to different encoding techniques to the data in such a way that only authorized users can access it.(Nurse et al., 2011) Encrypt the sensitive data of patients can ensure that even if the security is compromised, the unauthorized users can not be able to exploit the confidentiality and integrity of the patients information(Ali et al., 2018). The hospital can ensure compliance with regulatory environments and safeguard the data against unauthorized access by implement data encryption measure. These technique are followed in systems like GDPR and HIPAA.

6. **Endpoint Protection:** This involves securing the endpoint devices like desktops, laptop and mobile devices from cyber security threats.(Lezzi, Lazoi, & Corallo, 2018) The hospital can monitor the devices for suspicious activities and prevent the malware in their software by developing endpoint detection and response solutions (EDR).This

approach can enhance the overall security of the hospital and reduce the risks of cybersecurity threats and attacks targeting the end devices which are the entry point of the dangerous attackers.(Nurse et al., 2011)

7. **Penetration Testing and Vulnerability Assessments:** This kind of testing can enable the organizations to recognize and identify the address system security weaknesses before being exploited by the cyber attackers and dangerous people.(Ralston et al., 2007) The Hospital can strengthen the defense against the number of cyber attacks, identify potential vulnerabilities in the systems and the networks and prioritize remediation efforts by regularly conducting the vulnerability assessments and penetration testing. These are helpful in validating the overall security of the organizations and provide valuable insights into the effectiveness of existing security control systems.(Lezzi, Lazoi, & Corallo, 2018)

Justification: The above mentioned recommendations are very significant to mitigate the identified attack vectors and strengthen the Hospital's security resilience.(Veitch et al., 2013)The hospital can efficiently address the vulnerabilities highlighted in the attack tree, regulate the requirements and in line the cyber security strategies with its best practices.These proactive measures enhance the organizations' security and also ensure operational continuity of the organization, demonstrate the hospital's dedication to protecting patient's data and encompass confidence and trust among stakeholders.(Ralston et al., 2007) Implementing these recommendations can give rise to an empowered and secure environment aligned with prevailing expectations and standards.

Conclusion:

The current threat landscapes pose a significant risk to the healthcare sector like Acme hospital. (Yang et al., 2011)The healthcare sector can significantly reduce the risk profile and protect patient data, financial information and the operational integrity by understanding the common attack vectors and implementing the appropriate security controls to prevent the attacks(Veitch et al., 2013). Consequently, this report demonstrates the importance of analyzing the threat landscape, implementing the evidence based security recommendations and constructing attack trees to create a comprehensive cyber security strategy. (Ralston et al., 2007) This multifaceted approach is very important in formulating a comprehensive cybersecurity strategy to ensure the defense against evolving cybersecurity threats and address potential vulnerabilities in the system.(Takahashi & Kadobayashi, 2015)

References:

1. Von Solms, R. and Van Niekerk, J., 2013. From information security to cyber security. *computers & security*, *38*, pp.97-102.
2. Lezzi, M., Lazoi, M. and Corallo, A., 2018. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry*, *103*, pp.97-110.

3. Veitch, C.K., Henry, J.M., Richardson, B.T. and Hart, D.H., 2013. *Microgrid cyber security reference architecture* (No. SAND2013-5472). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).
4. Takahashi, T. and Kadobayashi, Y., 2015. Reference ontology for cybersecurity operational information. *The Computer Journal*, *58*(10), pp.2297-2312.
5. Priyadarshini, I., 2019. Introduction on cybersecurity. *Cyber security in parallel and distributed computing: Concepts, techniques, applications and case studies*, pp.1-37.
6. Yang, Y., Littler, T., Sezer, S., McLaughlin, K. and Wang, H.F., 2011, December. Impact of cyber-security issues on smart grid. In *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies* (pp. 1-7). IEEE.
7. Nurse, J.R., Creese, S., Goldsmith, M. and Lamberts, K., 2011, September. Guidelines for usable cybersecurity: Past and present. In *2011 third international workshop on cyberspace safety and security (CSS)* (pp. 21-26). IEEE.
8. Ali, S., Al Balushi, T., Nadir, Z. and Hussain, O.K., 2018. *Cyber security for cyber physical systems* (Vol. 768, pp. 11-33). Berlin/Heidelberg, Germany: Springer.
9. Ralston, P.A., Graham, J.H. and Hieb, J.L., 2007. Cyber security risk assessment for SCADA and DCS networks. *ISA transactions*, *46*(4), pp.583-594.
10. Edgar, T.W. and Manz, D.O., 2017. *Research methods for cyber security*. Syngress.