1. Summarize the recent history of adversarial behavior and attacks for your chosen sector.

In recent years, the health sector has witnessed a significant surge in adversarial behavior and attacks. This sector is particularly targeted due to its crucial need for uninterrupted service delivery. For instance, a ransomware-induced lockdown could have catastrophic consequences for the health sector. Threat actors understand this vulnerability and exploit it to exert pressure on their victims, thereby increasing the likelihood of a ransom payment. Moreover, the digitalization of the health sector has opened up a lucrative opportunity for threat hackers seeking to steal sensitive data. When we visit a healthcare provider, we entrust them with a wealth of personal information, including Social Security Numbers, email addresses, physical addresses, dates of birth, and even credit card details. This makes the health sector an attractive target for threat actors, offering a high potential payoff. Threat actors employ various methods to breach this sector, including social engineering, phishing, distributed denial-of-service (DDoS) attacks, botnets, zero-day vulnerabilities/exploits, man-in-the-middle attacks, malware, and ransomware. While cybercriminals and script kiddies may target the sector for financial gain, other threat actors have different motivations. Hacktivists, national actors, and cyberterrorists may aim to disrupt critical infrastructure for political and espionage purposes. Disrupting the health sector can have profound implications for a country's stability, making it an enticing target for certain nation-states like China, North Korea, Iran, and Russia. These countries have been known to deploy national actors and cyber terrorists to conduct espionage, given the sector's pivotal role in a nation and its repository of crucial citizen information. In 2022, an IBM study revealed a 45% increase in the average ransom demand from 2020 to 2021. In November 2021, an astounding $240 million was requested in the Hive Attack. Many hospitals impacted by ransomware attacks cannot admit new patients, putting lives at risk. However, hackers are not the sole threat. Regrettably, the 2022 Ponemon Institute Inside Report disclosed a nearly 50% rise in incidents from insider threats. Over half of these incidents were attributed to negligence, while one in four had malicious intent. Credential theft emerged as a primary avenue for insider theft, with 75% of respondents reporting using corporate email for this purpose, and other methods included downloading sensitive data onto external hard drives. Recognizing that insider threats pose a significant risk alongside external threats is crucial.

References:

Academy Page. Palo Alto Networks. (n.d.). https://www.paloaltonetworks.com/services/education/academy

Healthcare cybersecurity 2020 year in review, and a 2023 look-ahead. (n.d.-a). https://www.hhs.gov/sites/default/files/2022-retrospective-and-2023-look-ahead.pdf?lv=true

Health Industry Cybersecurity Practices: Managing threats and ... (n.d.-b). https://405d.hhs.gov/Documents/Five-Threat-Series-Loss-or-Theft-of-Data-R.pdf

Palo Alto Networks VMware Workstation 10.0 Academy Labs Deployment Guide. (n.d.).

2. Evaluate the emerging threat climate for the sector of your choice. Identify two or more areas of vulnerability where the sector will be at future risk.

The emerging threat landscape in the health sector is characterized by rapidly evolving cybersecurity risks and vulnerabilities. Among these, ransomware is a prevalent threat due to its potential to lock down critical systems. However, before ransomware, other vulnerabilities and threats have exposed the sector to these types of breaches. One significant threat is the Zero-day exploit, which can be particularly menacing for the health sector, as they might not have as specialized staff as some big tech companies to patch their systems on time. According to Unit 42's Palo Alto Attack Surface Threat report of 30 common vulnerabilities, 3 of them were exploited within hours of the CVE disclosure, and 19 were exploited within 12 weeks of the public disclosure, emphasizing the need for swift response from IT professionals in the health sector. Another area of vulnerability lies in Supply Chain Risks. The health sector's procurement of goods and services is managed through its supply chain. However, evolving cybersecurity risks have made this chain susceptible to cyber exploitation. This can originate from various third-party sources within the supply chain, such as medical devices, cloud applications, and aging legacy technology. While highly effective, integrating AI and machine learning into the healthcare system introduces a new dimension of vulnerability. Hackers can exploit concerns over potential biases and misconfigurations. This includes using biases in AI for fraudulent access, insurance fraud, and manipulation. Some Nation Actors may seek to exploit misdiagnoses and medical errors to create chaos and destabilize a country. Additionally, AI and machine learning, integral cybersecurity tools, can be repurposed for malicious intent. These technologies can be leveraged to automate tools and expedite exploitation within the health sector. Furthermore, the health sector faces Data Privacy and Compliance challenges, where compliance rules designed to protect users can inadvertently work against the sector. HIPAA, for instance, is a U.S. federal law aimed at safeguarding the privacy and security of individuals' medical information. Threat actors can exploit HIPAA compliance through social engineering, impersonating healthcare professionals to gain unauthorized access. Additionally, if a breach occurs and patient data is accessed by unauthorized parties, it leads to HIPAA violations, potentially resulting in fines and penalties from the Office for Civil Rights. These, combined with ransomware demands, can lead to significant financial repercussions for organizations in the health sector.

References

Academy Page. Palo Alto Networks. (n.d.-a). https://www.paloaltonetworks.com/services/education/academy

Health Industry Cybersecurity practices: Managing threats and ... (n.d.-b). https://405d.hhs.gov/Documents/Five-Threat-Series-Email-Phishing-405d-R.pdf

Health and Human Services. (2022). FACT SHEET: Ransomware and HIPAA. https://panacademy.net/CourseFiles/sbo/HHS_RansomwareFactSheet.pdf

Industry Cybersecurity Supply Chain Risk Management Guide. (n.d.-d). https://healthsectorcouncil.org/wp-content/uploads/2019/10/Health-Industry-Cybersecurity-Supply-Chain-Risk-Management-Guide-v1-2.pdf

Rajagopal, A. (2023, August 29). *Incident of the week: Malware attack exposes patient data*. Cyber Security Hub. https://www.cshub.com/attacks/articles/incident-of-the-week-malware-attack-exposes-patient-data

Xhofleer, T. (2023, October 2). *Ai helps hackers steal data. Healthcare Providers Must Get Ready now*. ICT&health. https://ictandhealth.com/ai-helps-hackers-steal-data-healthcare-providers-must-get-ready-now/news