As the healthcare industry continues to rely heavily on digital systems, it faces a growing number of cyber threats that can have severe consequences for patient care and hospital operations. The most common cyber threats in the sector include ransomware, phishing, insider threats, and IoT vulnerabilities. The frequency and sophistication of these attacks are on the rise, with numerous high-profile breaches in recent years. These incidents can lead to disrupted patient care, operational challenges, and significant financial losses for healthcare organizations.

Cybercriminals employ various modes of attack to target healthcare systems, such as malware and ransomware, which involve encrypting data, locking systems, and demanding ransom payments. Phishing and social engineering attacks focus on manipulating employees into divulging sensitive information or accessing malicious links. Insider threats pose another risk, with unauthorized access, data theft, and intentional sabotage being potential outcomes. Moreover, emerging threats like IoT vulnerabilities, supply chain attacks, and Advanced Persistent Threats (APTs) further challenge the healthcare industry's cybersecurity measures. To address these threats, it is crucial for healthcare organizations to implement robust security protocols, invest in employee training, and remain vigilant against evolving cyber threats.