Kevin Hamzaj 2687959

Cybersecurity II

Module 3 assignment

24 September 2023

In today's digitally connected world, cybersecurity is of utmost importance, especially in the healthcare sector, where patient data must be safeguarded. HIPAA (Health Insurance Portability and Accountability Act) provides guidelines and controls to protect sensitive healthcare information.

Cyber Attack Method (CAM): Financial Compromise (Payment Method)

A. Control 1: Access Control (HIPAA Control #164.312(a)(1))

Access Control is a crucial aspect of HIPAA that involves implementing technical policies and procedures to restrict access to patient data.

Control Description (short): Access Control ensures that only authorized individuals can access sensitive healthcare information. This control includes user authentication, role based access, and encryption of data.

How it would stop, eradicate, thwart, prevent, or mitigate your CAM: Financial compromise often involves unauthorized access to payment information or sensitive patient data. Implementing strong access controls can prevent cybercriminals from gaining access to such information. With proper access control measures in place, even if an attacker breaches the perimeter defenses, they would find it extremely challenging to access payment data or compromise financial information.

B. Control 2: Audit Controls (HIPAA Control #164.312(b)) Audit Controls are essential for monitoring and recording system activity to detect and respond to suspicious or unauthorized activities.

Control Description (short): Audit Controls involve the continuous monitoring of system activities, recording of logs, and regular reviews of these logs to identify anomalies or potential security breaches.

How it would stop, eradicate, thwart, prevent, or mitigate your CAM: Financial compromise cyber attacks often leave traces in system logs. By implementing robust audit controls, healthcare organizations can quickly identify any unusual or unauthorized access attempts related to payment methods. This early detection can lead to a prompt response, preventing or mitigating potential financial losses.

C. Control 3: Encryption and Decryption (HIPAA Control #164.312(a)(2)(iv)) Encryption and Decryption are vital for protecting data in transit and at rest.

Control Description (short): Encryption involves converting data into a format that is unreadable without the appropriate decryption key. This control ensures that even if data is intercepted, it remains confidential.

How it would stop, eradicate, thwart, prevent, or mitigate your CAM: Financial compromise attacks often target data during transmission, such as payment transactions. Encrypting sensitive payment data ensures that even if intercepted, the attacker cannot decipher it without the encryption key. This control prevents unauthorized access to financial information and adds an additional layer of security.

Conclusion: In conclusion, the three HIPAA Technical Controls discussed Access Control, Audit Controls, and Encryption and Decryption play a crucial role in thwarting financial compromise cyber attacks, specifically those targeting payment methods. By implementing these controls effectively, healthcare organizations can enhance their cybersecurity posture and protect patient data from unauthorized access and financial loss. It is essential for healthcare entities to continuously assess and update their security measures to stay ahead of evolving cyber threats in the digital age.