Project

In this project, I wrote an incident handler's report on a ransomware attack at a small U.S. primary care clinic. The incident occurred on a Tuesday at 9am when employees were unable to access critical medical records due to ransomware displayed in ransom notes. Attackers gained access through phishing emails containing malicious attachments, leading to the encryption of vital patient data and a shutdown of operations. My report analyzed the attack vector, its impact, and the clinic's response actions.

Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: 12/04/24	**Entry: 1**
Description	Ransomware attack disrupts clinic operations, demands payment
Tool(s) used	Encryption
The 5 W's	Capture the 5 W's of an incident. ● **Who** attacker/hacker ● **What** Ransomware attack, encrypted files, demands payment ● **When** Tuesday 9:00am ● **Where** US health care clinic ● **Why** Employee clicked a malicious email link which allowed an attacker to encrypt the data for financial gain
Additional notes	More employee training on phishing e-mails Can data be recovered or pay ransom? Are there backups of the data?