Incident handler's journal

Instructions

Date: February 21, 2024	**Entry:** #1
Description	Documenting a cybersecurity incident
Tool(s) used	None.
The 5 W's	• **Who**: Organized group of unethical hackers • **What**: Ransomware attack • **Where**: Health care clinic • **When**: Tuesday 9:00 a.m. • **Why**: The ransomware was deployed because the hackers gained access into the company's network via targeted phishing emails that were sent to several employees of the company. These phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded. As soon as the attackers gained access, they were able to deploy their ransomware and encrypt critical files. The attackers' motivation appears to be financial because they demanded a large sum of money in exchange for the decryption key.
Additional notes	1. What steps can the health care clinic take to prevent an incident like this from occurring again? 2. Should the clinic pay the ransom in order to retrieve the decryption key and resume business operations?