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: July 23, 2024	**Entry:** #1
Description	Documenting a cybersecurity incident
Tool(s) used	None.
The 5 W's	● **Who**: a well-resourced team of unethical hackers ● **What**: A ransomware security incident ● **Where**: At a health care company ● **When**: Tuesday 9:00 a.m. ● **Why**: Because of a phishing attempt, dishonest hackers were able to gain access to the organization's networks and trigger the incident. The attackers started their ransomware on the company's servers after gaining access and encrypting crucial files. The ransom note the attackers left wanted a sizable sum of money in exchange for the decryption key, suggesting that their goal was financial.
Additional notes	1. How could the health care company prevent an incident like this from occurring again? 2. Should the company pay the ransom to retrieve the decryption key?