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: April 26, 2025	**Entry:** #1
Description	Documenting a cybersecurity incident
Tool(s) used	None.
The 5 W's	• **Who**: An organized group of unethical hackers • **What**: A ransomware security incident • **Where**: At a health care company • **When**: Tuesday 9:00 a.m. • **Why**: The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key.
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?

Key takeaways

This activity enabled me to practice applying my documentation skills to complete a journal entry about a ransomware scenario. Accurate and thorough documentation is a critical aspect in incident response because it helps to ensure that important information is not lost or overlooked, and it also allows me to capture aspects of an incident for future use. I should continue practicing my documentation skills by creating additional journal entries as I complete the course activities. By the end of the course, I should add this document to my cybersecurity portfolio.