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: 5/9/2023	**Entry: 1**
Description	Documenting the cybersecurity incident.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A group of unethical hackers • **What** happened? Ransomware security incident • **When** did the incident occur? Tuesday at 9:00 am • **Where** did the incident happen? A small U.S. health care clinic • **Why** did the incident happen? 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?