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: August 22, 2023	**Entry: 1**
Description	Documenting a cybersecurity incident
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. • **Who:** Organized group of unethical hackers • **What**: Ransomware security incident • **When**: At a small U.S. health care clinic • **Where** : Tuesday 9:00 a.m. • **Why**: The incident happened when unethical hackers were able to access the company's systems using targeted phishing attack. After gaining access to the system the attackers launched their ransomware software, encrypting the company's critical files. The attacker's motivation is strictly financially due to ransom note demanding large sum of money in exchange for a decryption key.
Additional notes	• How the company could prevent this type of incident occurring in the future. • Should the company pay the ransom in exchange of decryption key