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 21	**Entry: #1**
Description	Document a ransomware incident
Tool(s) used	None:
The 5 W's	Capture the 5 W's of an incident. • **Who**: an organized group of unethical hackers • **What**: a ransomware incident • **When**: Tuesday 9:00 am • **Where**: At a small health care clinic • **Why**: the attackers gained access into the company network using phishing emails. Once they gained access, they deployed ransomware which encrypted critical files. Their purpose must be financial as they note demanded a large sum of money in exchange for decryption key.
Additional notes	Should we pay money for the decryption key? What is the solution for preventing this problem happens again?