**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:** Oct 14, 2025 | **Entry:** #1 |
| Description | A small U.S. health care clinic suffered a ransomware attack that shut down their operations. Employees couldn’t access medical records or files, and a ransom note appeared on their screens. The attack started from phishing emails that carried a malicious attachment. Once opened, ransomware encrypted all the company’s important files, blocking access to patient data and forcing a full system shutdown. |
| Tool(s) used | None. |
| The 5 W's | * **Who:** An organized group of unethical hackers known for targeting healthcare and transportation sectors. * **What**: A ransomware security incident that encrypted the company’s data and demanded ransom in return for the decryption key. * **Where**: At a small U.S. health care clinic specializing in primary care services. * **When**: 9:00 am Tuesday. * **Why**: The attackers sent phishing emails with a malicious attachment. When opened, the file installed malware that gave the hackers access to the system. They deployed ransomware to encrypt critical files. Their main goal was financial, to extort money in exchange for data recovery. |
| Additional notes | 1. Should the company pay the money to the hackers? 2. What will they tell their customers and patients and how will they amend the breach? |