**Incident handler's journal**

| **Date:** July 7, 2023 | **Entry: #1** | | |
| --- | --- | --- | --- |
| Description | Documenting a cybersecurity incident | | |
| Tool(s) used | - | | |
| The 5 W's | **Who**: An organized group of unethical hackers  **What**: A ransomware security incident  **When**: Tuesday 9:00 a.m.  **Where:** At a health care company  **Why**: As 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. Their 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. Should the company pay the ransom to retrieve the decryption key? 2. How would the health care company prevent an incident like this from occurring again? | | |