**Incident handler's journal**

| **Date:** July 6, 2023 | **Entry: #1** | | |
| --- | --- | --- | --- |
| Description | A cybersecurity incident occur to a small U.S. health care clinic which severely disrupted their business operations. | | |
| Tool(s) used | There were no tools used | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? A group of unethical hackers targeting healthcare and transportation industries * **What** happened? Several employees were unable to access files because they were encrypted, and could only be decrypted by the hacker group. * **When** did the incident occur? This incident occurred on Tuesday at 9:00 a.m. * **Where** did the incident happen? It happened in a small U.S. health care clinic specializing in delivering primary-care service. * **Why** did the incident happen? The incident occur because The attackers were able to gain access into the company's network by using targeted phishing emails | | |
| Additional notes | It looks like there aren’t any Phishing preventive training in place, the company should apply the training to spread awareness of these types of incidents. | | |