**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  #1. |
| Description | Documentation of cyber security incidence. |
| 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**: On Tuesday morning, at approximately 09:00am * **Where**: At healthcare company * **Why:** The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded. |
| Additional notes | * How can the health care company prepare for future events ? * Does the company need to pay for ransomware for the decryption key |

### 