**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:**  Record the date of the journal entry. | **Entry:**  1 |
| Description | Initial incident document |
| Tool(s) used | N/A |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   Unethical hackers who are known to target organizations in healthcare and transportation industries   * **What** happened? * Several employees reported that they were unable to access files on their computers, including critical documents such as medical records. As a result, business operations were disrupted and had to be temporarily shut down. In addition, a ransom note was displayed on the affected computers, indicating that the attack involved ransomware. * **When** did the incident occur?   Tuesday morning about 9am   * **Where** did the incident happen?   A small U.S. health care clinic specializing in delivering primary-care services   * **Why** did the incident happen?   The attackers successfully gained access to the company's network through a targeted phishing campaign. Several employees received phishing emails containing malicious attachments. When these attachments were downloaded, malware was installed on the affected employees’ computers, allowing the attackers to infiltrate the network. |
| Additional notes | The company was targeted by phishing emails, a common issue that affects many organizations. To reduce the risk of future attacks caused by human error, it is essential to conduct cybersecurity seminars to train employees on how to recognize and respond to such threats. |