**Incident handler's journal**

| **Date:**  Record the date of the journal entry. | **Entry: 1** | | |
| --- | --- | --- | --- |
| Description | Documenting a cyber security incident | | |
| Tool(s) used | none | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: An organized group of unethical hackers known for targeting healthcare and transportation industries. * **What**: Ransomware was deployed via a phishing email, encrypting critical files and demanding a ransom for the decryption key. * **When**: Tuesday 9:00 a.m. * **Where**: small U.S. healthcare clinic specializing in primary-care services. * **Why**: The incident occurred because employees fell victim to targeted phishing emails containing a malicious attachment that, once downloaded, installed malware leading to a ransomware attack. | | |
| Additional notes | Concerns about the potential impact on patient care and data privacy.  Importance of enhancing employee training to recognize phishing attempts.  Possible need for better security measures, such as multi-factor authentication (MFA) and email filtering solutions. | | |