**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:**  05/09/2025 | **Entry:**  1 |
| Description | A small U.S. health care clinic experienced a serious cybersecurity incident involving ransomware, which disrupted their operations. |
| Tool(s) used | None specified |
| The 5 W's | **Who caused the incident?** An organized group of unethical hackers.  **What happened?** A phishing email was sent to the clinic. Once a malicious attachment was downloaded, ransomware was deployed and encrypted the organization's files.  **When did the incident occur?** Tuesday at 9:00 a.m.  **Where did the incident happen?** A small health care clinic in the United States.  **Why did the incident happen?** Because an employee downloaded a malicious attachment from a phishing email, leading to the deployment of ransomware. |
| Additional notes | This incident highlights the critical importance of employee training and email security. What email security solutions could have prevented this? Was there a lack of endpoint protection or network segmentation? |