**Incident handler's journal**

This document contains incident response journal entries completed as part of the Google Cybersecurity Certificate. Each entry is based on a simulated scenario designed to demonstrate incident handling, documentation, and analysis skills.

| Date: July 1, 2025 | Entry: 1 | | |
| --- | --- | --- | --- |
| Description | A ransomware attack targeted a small healthcare clinic in Western Australia, causing a complete shutdown of operations after staff reported they couldn’t access medical records or systems. A ransom note was displayed on employee computers demanding payment to decrypt the files. | | |
| Tool(s) used | None at this stage. Tools to be considered for incident investigation may include antivirus software, email security tools, backup systems, and forensic analysis platforms. | | |
| The 5 W's | * Who: An organized group of unethical hackers known for targeting healthcare and transportation sectors. * What: Attackers sent phishing emails with malicious attachments. Once opened, ransomware encrypted critical files and demanded payment. * When: The incident occurred on Tuesday, July 1, 2025, at approximately 9:00 a.m. * Where: At a small healthcare clinic located in Western Australia. * Why: The incident happened due to a successful phishing campaign exploiting employee action, allowing ransomware to be deployed and critical systems to be encrypted. | | |
| Additional notes | This incident highlights the critical need for phishing awareness training, email filtering, and reliable data backup systems. A formal incident response plan should be implemented and tested regularly. | | |

| Date**:** July 21, 2025 | Entry: 2 | | |
| --- | --- | --- | --- |
| Description | A data leakage incident occurred at a WA healthcare clinic due to a misconfigured cloud storage bucket. Sensitive patient information was inadvertently made publicly accessible, prompting an urgent response from the IT security team. | | |
| Tool(s) used | Cloud Security Posture Management (CSPM), Azure configuration scanner, and data loss prevention (DLP) tool. | | |
| The 5 W's | * Who: The Internal IT team unintentionally misconfigured a cloud storage setting. * What: A cloud bucket containing sensitive patient records (including personally identifiable information) was exposed to the public internet without authentication. * When: The exposure was discovered during a routine security audit on the morning of July 21, 2025. * Where: The issue occurred in the cloud infrastructure used by a WA-based healthcare provider. * Why: A lack of automated misconfiguration detection and poor access control policies led to the accidental data exposure. | | |
| Additional notes | This incident emphasizes the importance of cloud security audits, automated configuration monitoring, and regular staff training. Implementing Infrastructure as Code (IaC) with security guardrails could prevent similar incidents. | | |