**Incident handler's journal  
by   
M.Murtaza Soc ANALYST**

|  |  |
| --- | --- |
| **Date:** May 12, 2025 | **Entry:** #1 |
| Description | Documenting a ransomwere incident |
| Tool(s) used | Email client, syslog , windows event viewer. |
| The 5 W's | * **Who**: An organized group of unethical hackers * **What**: A ransomware security incident * **Where**: At a health care company * **When**: Tuesday 9:00 a.m. * **Why**: The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key. |
| Additional notes | 1. How could the health care company prevent an incident like this from occurring again?  *Answer: By implementing phishing awareness training, using advanced email filtering, maintaining secure backups, and enforcing strict access controls.* 2. Should the company pay the ransom to retrieve the decryption key?  *Answer:* *No, paying the ransom is discouraged as it doesn't guarantee file recovery and encourages future attacks.* |