| **Date:**  02/28/2024 | **Entry:**  #1 | | |
| --- | --- | --- | --- |
| Description | Documenting a security incident | | |
| Tool(s) used | Nil | | |
| The 5 W's | * **Who** caused the incident? A group of organized unethical hackers who are known to the target organizations in the healthcare and transportation industries. * **What** happened? A ransomware attack has occurred. * **When** did the incident occur? The incident occurred on a Tuesday morning, at approximately 9:00 am. * **Where** did the incident happen? The incident happened in a small U.S. healthcare clinic specializing in delivering primary care services. * **Why** did the incident happen? The incident happened on requesting a large sum of ransom in exchange for decryption keys. | | |
| Additional notes | The incident is first compromised by a phishing attack which is sent to several employees of the company. The phishing email contained a malicious attachment that installed malware on the employee’s computer once it was downloaded. Upon successful compromise, the ransomware attack takes place.   * How can the company safeguard itself from future similar security incidents? * Should the company pay the ransom? | | |