**Incident handler's journal**

| **Date:** July 23, 2023 | **Entry:** #1 | | |
| --- | --- | --- | --- |
| Description | Documenting a cybersecurity incident | | |
| Tool(s) used | None. | | |
| 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? 2. Should the company pay the ransom to retrieve the decryption key? | | |

| **Date:** Aug 10, 2023 | **Entry:** #2 | | |
| --- | --- | --- | --- |
| Description | Documenting a cybersecurity incident | | |
| Tool(s) used | VirusTotal | | |
| The 5 W's | * **Who**: A hacker * **What**: A phishing attempt * **Where**: At a financial service company * **When**: Wednesday 9:30 a.m. * **Why**: The alert detected that an employee downloaded and opened a malicious file from a phishing email. The email body and subject line contained grammatical errors. The email’s body also contained a password-protected attachment, “bfsvc.exe,” which was downloaded and opened on the affected machine. The attacker's goal seems to be to gain access to the company's restricted files. | | |
| Additional notes | 1. What improvements should the company make regarding employee security awareness? | | |