**Incident handler's journal**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

| **Date:** July 23, 2024 | **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?   To prevent future incidents like the ransomware attack, the healthcare company should implement a comprehensive cybersecurity strategy. This includes providing regular security awareness training to help employees recognize phishing emails and suspicious attachments. The company should also deploy advanced email filtering tools and maintain up-to-date antivirus and anti-malware software to block threats before they reach users. Network segmentation and strict access controls should be enforced to contain any potential breaches. Additionally, using Endpoint Detection and Response (EDR) tools can help monitor and respond to unusual activity in real time. Regular, encrypted, and offline backups of critical data must be maintained and tested to ensure recovery without relying on ransom payments. Keeping all systems patched and up to date reduces exploitable vulnerabilities. Finally, the company should develop and regularly update an incident response plan and conduct exercises to ensure preparedness in the event of future attacks.   1. Should the company pay the ransom to retrieve the decryption key?   The company should not pay the ransom to retrieve the decryption key. Paying the ransom offers no guarantee that the attackers will actually provide the key or that the data will be fully restored, and it may lead to further harm if the attackers exploit the company again. Additionally, making such payments encourages and funds criminal activity, potentially increasing the likelihood that similar organizations will be targeted in the future. There are also legal and ethical concerns, as paying ransoms may violate regulations related to financing sanctioned entities or terrorist organizations. Instead of paying, the company should focus on recovery through secure backups and collaborate with cybersecurity professionals and law enforcement agencies to investigate the incident and strengthen defenses against future attacks. | | |