Incident handler's journal

Scenario 1

Date: **July 23, 2024**	**Entry: # 1**
Description	**Documenting a cybersecurity incident** Investigation into a security event involving ransomware used against a small U.S. health care clinic specializing in delivering primary-care services.
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**: Thursday 24th October 2024 at 9:00 a.m., JST. ● **Why**: The incident occurred because of malicious threat actors successfully compromising the company's systems through a phishing attack. Once access was obtained, the attackers deployed ransomware, encrypting critical files within the organization's infrastructure. The primary motivation for the attack appears to be financial, as evidenced by the ransom note, which demanded a significant sum of money in exchange for the decryption key.
Additional notes	1. **Preventative Measures:**

	• Enhance employee training programs focused on phishing awareness and prevention to improve their ability to identify and avoid such attacks. • Implement routine phishing simulations to test employee readiness and reinforce secure email practices. 2. **Ransom Payment Consideration:** • The organization should not pay the ransom as it does not guarantee the recovery of encrypted data and may incentivize further malicious activities by the attackers. • Instead, focus on having robust backup systems, incident response plans, and collaborating with cybersecurity experts to recover from such incidents effectively.

Reflections for Scenario 1	• **Number of Entries:** One entry has been documented for this scenario. • **Type of Security Incident:** The organization was affected by a ransomware attack, initiated through a phishing email. • **Root Cause of the Incident:** The root cause was phishing emails containing malicious attachments. When a recipient clicked on the attachment, ransomware was deployed, encrypting critical data. • **Preventive and Mitigative Actions:** ○ Conduct regular training and education to help employees recognize and avoid phishing emails. ○ Ensure secure backups are maintained to prevent data loss due to ransomware encryption.

	○ Isolate infected systems from the network promptly to prevent further spread of ransomware. ○ Consult cybersecurity firms for potential decryption tools tailored to the specific ransomware variant. ○ Maintain clear communication with relevant stakeholders regarding the incident and mitigation steps. ○ If appropriate, report the incident to the relevant authorities to comply with regulatory requirements and assist in potential investigations.