Incident handler's journal

Scenario 1

Date: **July 24, 2024**	**Entry: # 1**
Description	A ransomware attack targeted a small U.S. health care clinic specializing in primary care services. The attack was initiated via a phishing email that successfully compromised the organization's systems. Once access was obtained, the attackers deployed ransomware, encrypting critical files within the clinic's infrastructure. The ransom note demanded payment in exchange for a decryption key.
Tool(s) used	No specific tools were actively used during this incident. This highlights a gap in the clinic's preparedness.
The 5 W's	• **Who**: An organized group of cybercriminals. • **What:** A ransomware attack encrypting critical files. • **Where**: The incident occurred within the IT infrastructure of a U.S.-based health care clinic. • **When**: Monday, July 24, 2024, at 9:00 a.m. JST. • **Why**: The attack leveraged a phishing email containing malicious attachments. The attackers sought financial gain by demanding a ransom for the decryption key.
Additional notes	**Preventative Measures:** • **Phishing Awareness Training:** Regular training programs for employees to recognize and report phishing emails.

	• **Phishing Simulations:** Routine exercises to test employee readiness and reinforce secure practices. • **Data Backup Protocols:** Maintain secure, regular backups to ensure business continuity in the event of ransomware attacks. • **Incident Response Planning:** Develop and test a comprehensive incident response plan for handling ransomware attacks. • **Report to Authorities:** Report such incidents to law enforcement and regulatory bodies as required.

Reflections for Scenario 1	This incident underscored critical vulnerabilities in the organization's cybersecurity defenses, particularly in employee awareness and technical safeguards. The absence of phishing awareness training allowed the attackers to exploit human error as the primary vector of compromise. Key takeaways include: • The need for regular training programs and simulations to enhance phishing awareness among employees. • The importance of maintaining secure, off-site backups to prevent significant data loss. • A structured incident response playbook is essential for quick containment and recovery. To prevent recurrence, the organization should invest in robust email filtering systems and endpoint detection tools. Involving cybersecurity experts during the recovery phase will ensure that comprehensive measures are implemented to address any remaining gaps.

Follow-Up Actions	1. Implement a phishing awareness training program within the next 30 days. 2. Deploy advanced email filtering solutions to prevent phishing emails from reaching employees. 3. Create and test an incident response playbook tailored to ransomware incidents. 4. Report the incident to relevant authorities and share findings with industry partners to improve collective resilience.