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: November 8, 2024	**Entry:** 1
Description	Initial journal entry documenting a ransomware attack incident affecting a small U.S. healthcare clinic specializing in primary care services.
Tool(s) used	None utilized at this stage. Awaiting further instructions for technical response.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? An organized group of unethical hackers, who are known to target healthcare and transportation sectors, conducted the attack. They gained access through a phishing campaign targeting clinic employees. ● **What** happened? A phishing email containing a malicious attachment was sent to clinic employees. Upon downloading the attachment, ransomware was deployed, encrypting critical patient files and business-related data. A ransom note was left, demanding a sum of money in exchange for a decryption key.

	● **When** did the incident occur? The attack was identified on Tuesday morning, at approximately 9:00 a.m., when employees reported that they could not access files or medical records ● **Where** did the incident happen? The incident occurred at a small healthcare clinic in the United States, impacting the clinic's computer systems and essential files. ● **Why** did the incident happen? The attack was possible due to employees interacting with a targeted phishing email. The email tricked users into downloading a malicious attachment, which then initiated the ransomware, leading to widespread data encryption and operational shutdown.
Additional notes	● Investigate the full extent of the encryption to understand which systems and data are impacted. ● Review phishing defense mechanisms within the clinic to identify potential improvements. ● Confirm if the clinic has data backups that could potentially be used for recovery without paying the ransom. ● Evaluate the clinic's current incident response plan, if one exists, to ensure appropriate actions are in place for ransomware scenarios.