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: Tuesday morning, approx 9am Record the date of the journal entry.	**Entry:** On a Tuesday morning at approximately 9:00 a.m, a small U.S. health care clinic experienced a major disruption when several employees reported being unable to access medical records and other critical files. Shortly after, a ransom note appeared on their screens, stating that all company files had been encrypted by a known cybercriminal group. Investigation revealed that the attackers had gained initial access through targeted phishing emails sent to employees, containing malicious attachments that, once opened, installed malware and allowed the attackers to infiltrate the network and deploy ransomware. Journal Entry No. 2025-07-21-001
Description	Initial journal entry documenting the ransomware incident that affected the clinic's network and disrupted operations. Incident response was initiated following employee reports of file inaccessibility and ransom messages on their computers.
Tool(s) used	Email monitoring tools (preliminary review of phishing emails) Endpoint detection and response (EDR) – pending further investigation Antivirus/anti-malware software logs – being collected Manual network segmentation (temporary shutdown of systems)

The 5 W's	**Who caused the incident?** An organized group of cybercriminals known for targeting healthcare and transportation sectors. Initial access was achieved through phishing emails sent to employees. **What happened?** A ransomware attack occurred. Employees were locked out of systems and files, including medical records. A ransom note was displayed, demanding payment in exchange for a decryption key. **When did the incident occur?** Tuesday morning, 9:00 a.m. **Where did the incident happen?** At a small U.S.-based health care clinic specializing in primary-care services. The attack affected multiple systems across the clinic's internal network. **Why did the incident happen?** The attackers exploited human vulnerabilities through targeted phishing emails. At least one employee opened a malicious attachment that installed malware, allowing attackers to deploy ransomware and encrypt critical systems.
Additional notes	**Initial Infection Vector Confirmed:** Phishing emails appear to be the origin. Sample messages have been preserved for analysis. **Unclear if Data Was Exfiltrated:** Need to determine if Protected Health Information (PHI) was accessed or exported prior to encryption (potential HIPAA breach). **Ransom Note Analysis Pending:** Forensics will examine the note's content for

	identifying indicators of which ransomware group is responsible. **Backup Integrity:** It is not yet confirmed whether recent backups exist or are viable for restoration. **Employee Awareness Gap:** Early indication suggests limited phishing awareness among staff. A training gap likely contributed to the success of the social engineering attack. **Next Steps:** • Conduct full forensic investigation • Verify and test system backups • Notify appropriate regulatory bodies (HHS, OCR) • Begin internal review of incident response policies and user access controls • Initiate crisis communication plan (patients, legal, partners)