Incident Handler's Journal Entry

Date: October 29, 2023	Entry: 1
Description	A security incident has occurred at a small U.S. health care clinic, where ransomware encrypted critical files, severely disrupting business operations. A ransom note was left by the attackers demanding payment in exchange for the decryption key.
Tool(s) Used	• Email Security Gateway – For analyzing the phishing email source and preventing such attacks in the future. • Endpoint Protection Platform – To detect and quarantine the malicious attachment. • Network Monitoring Tool – To track any abnormal network activities after the download of the malicious attachment. • Ransomware Decryption Tools – Attempted to decrypt the affected files without paying the ransom. • Backup and Recovery Tool – To restore the encrypted data if available and valid backups exist.
5 W's	Who caused the incident? • An organized group of unethical hackers known to target organizations in healthcare and transportation industries. What happened? • Ransomware was deployed onto the company's network, encrypting critical files. Employees found a ransom note on their computers demanding payment for the decryption key. When did the incident occur? • Tuesday morning, at approximately 9:00 a.m. Where did the incident happen? • At a small U.S. health care clinic specializing in delivering primary-care services. Why did the incident happen? • Attackers used targeted phishing emails sent to employees. These emails contained malicious attachments, which when downloaded, installed malware, leading to the ransomware attack.
Additional Notes	Immediate system shutdown may have minimized further damage. The company should reassess its cybersecurity policies and employee training. The decision to pay the ransom or restore from backups must be carefully weighed. Collaboration with external cybersecurity firms could be beneficial for recovery and future prevention.