Incident handler's journal

Instructions

Date: Record the date of the journal entry.	**Entry:** 1
Description	First journal entry documenting a security incident.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	**Who caused the incident?** An organized group of unethical hackers targeted the small U.S. health care clinic specializing in primary-care services. **What happened?** The clinic experienced a security incident where employees were unable to access files and software due to encryption caused by ransomware deployed by the hackers. **When did the incident occur?** The incident occurred on a Tuesday morning at approximately 9:00 a.m. **Where did the incident happen?** The incident occurred within the small U.S. health care clinic. **Why did the incident happen?** The incident happened because the hackers gained access to the clinic's network through targeted phishing emails, which contained a malicious attachment that installed malware on the employee's computer.
Additional notes	The ransom note demanded a large sum of money in exchange for the decryption key. The clinic had to shut down its computer systems and seek

	technical assistance after major disruptions in business operations caused by the inability to access critical patient data.

Reflections/Notes: It is crucial for organizations to enhance their cybersecurity measures, including employee training to detect and avoid phishing attacks. Regular backups and incident response plans are essential for effective incident handling and minimizing the impact on business operations.