Incident handler's journal

RANSOMWARE IN HOSPITAL

Date: Record the date of the journal entry.	**Entry:** June 20, 2025
Description	A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job. Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that all the company's files were encrypted by an organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key. The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded. Once the attackers gained access, they deployed their ransomware, which encrypted critical files. The company was unable to access critical patient data, causing major disruptions in their business operations. The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ Ransomware actors ○ organized group of unethical hackers who are known to target organizations in healthcare and transportation industries ● **What** happened?

	○ Ransomware was installed by clicking on phishing email ○ It Encrypted all critical files ○ Ransom note displayed on computers demanded large sum of money in exchange for decryption key ● **When** did the incident occur? ○ Tuesday, June 17 morning 9:00 am ● **Where** did the incident happen? ○ US healthcare clinic ● **Why** did the incident happen? ○ Someone clicked link in phishing email
Additional notes	Include any additional thoughts, questions, or findings. **Observations:** ● This attack hampered business continuity ● Clearly, the clinic was unprepared for this event ● No procedures or policies in place to handle such events **Questions**: ● What are the hospital policies and procedures in the event of this attack ? ● Isn't there any backup of employee data that can be accessed in such an event? ● How this attack can be avoided **Recommendations**: ● Train employees to identify phishing emails ● Train employees to not click links from unknown sources ● Email filters must be in place to block known attacker sources