Incident handler's journal

Date: July 18th	**Entry: 01**
Description	Provide a brief description about the journal entry. **Documenting a ransomware attack on a U.S health care clinic.**
Tool(s) used	**None**
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Organized group of unethical hackers • **What** happened? The group encrypted all the clinics files and demanded a sum of money for the key to decrypt them. A ransomware attack. • **When** did the incident occur? Tuesday morning, at approximately 9:00 am. • **Where** did the incident happen? At a small U.S health care clinic specializing in delivering primary-care services. • **Why** did the incident happen? The attackers gained access to the company's network using targeted phishing emails that had malware attached to them.
Additional notes	1. How could the health care company prevent an incident like this from occurring again? 2. Should the company pay the ransom to retrieve the decryption key?