Incident handler's journal

Date: July 23, 2024	**Entry:** #1
Description	Documenting a cybersecurity incident
Tool(s) used	None.
The 5 W's	• **Who**: An organized group of unethical hackers • **What**: A ransomware security incident • **Where**: At a health care company • **When**: Tuesday 9:00 a.m. • **Why**: The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key.
Additional notes	1. How could the health care company prevent an incident like this from occurring again? Employee Training, Implement Multi-Factor Authentication (MFA),Backup and Disaster Recovery Plan 2. Should the company pay the ransom to retrieve the decryption key? No, the company should not be supporting criminal activity and could potentially violate laws or regulations in some jurisdictions. Additionally, paying the ransom does not guarantee that the attackers will provide a decryption key or that they won't launch future attacks. the company should explore alternative solutions, such as restoring data from backups or seeking assistance from cybersecurity professionals to decrypt the files.