Document an incident with an incident handlers journal

Scenario

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.

Incident handlers journal

Date: 05/08/2025	**Entry:** 1
Description	Documenting a cybersecurity incident.
Tool(s) used	None.
The 5 W's	• **Who** – a group of unethical hackers. • **What** – a ransomware attack • **Where** – a small healthcare clinic • **When** – Tuesday at 09:00 AM • **Why –** Unethical hackers want financial gain because they left a ransom note on all infected computers. The incident occurred because the hackers used targeted phishing emails on the employees. After the phishing attack worked, they deployed ransomware on the network.

Additional notes	1) How can the company retrieve their files. Should they pay the ransom? 2) How could an incident like this be prevented in the future?