Incident handler's journal

Date: Aug 17, 2024	**Entry:** 1
Description	There was a cybersecurity incident where employees reported that they were unable to access files and software they needed to do their jobs. A ransom note was left by a group of unethical hackers demanding money in exchange for the decryption key.
Tool(s) used	N/A

The 5 W's	Capture the 5 W's of an incident.
	• **Who** caused the incident?
	  ○ An organized group of unethical hackers.
	• **What** happened?
	  ○ A ransomware incident
	• **When** did the incident occur?
	  ○ Tuesday at around 9am.
	• **Where** did the incident happen?
	  ○ In a small U.S health care clinic.
	• **Why** did the incident happen?
	  ○ Attackers' motivation was money because they intentionally installed a ransomware that demands a large sum of money in return for the decryption key.

Additional notes	Include any additional thoughts, questions, or findings. • Should they pay the ransom to retrieve the decryption key?