Incident handler's journal

Date: August 24, 2024	**Entry:** #1
Description	Documenting a cybersecurity incident
Tool(s) used	tcpdump
The 5 W's	● **Who**: A group of unethical hackers ● **What**: A ransomware security incident ● **Where**: At a University ● **When**: Thursday 12:00 p.m. ● **Why**: The incident happened because unethical hackers were able to access the company's systems using an unconfigured firewall. After gaining access, the attackers launched their ransomware on the university'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 bitcoin exchange for the decryption key.
Additional notes	1. How could the university prevent an incident like this from occurring again? 2. Should the university pay the ransom to retrieve the decryption key?