Incident handler's journal

Date: June 20, 2023	**Entry:** #1
Description	Documenting a cybersecurity incident (Ransomware)
Tool(s) used	None.
The 5 W's	• **Who**: An organized group of unethical hackers that target healthcare and transportation industries. • **What**: A ransomware security incident • **Where**: At a healthcare company • **When**: Tuesday 9:00 a.m. • **Why**: 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 and gave access to all important files. The attackers were demanding a large amount of money to give them the decryption key to stop the ransomware.
Additional notes	1. What future security measures can take this company to not suffer this attack again? 2. Should the company pay the ransom to retrieve the decryption key? Or should they look for a security team or company that helps them decrypt the files?