Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: September 10, 2024	**Entry:** #1
Description	• A small U.S. health care clinic experienced a security incident on Tuesday at 9:00 a.m. which severely disrupted their business operations. • The cause of the security incident was a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files. • An organized group of unethical hackers left a ransom note stating that the company's files were encrypted and demanded money in exchange for the decryption key.
Tool(s) used	None.
The 5 W's	• **Who**: An organized group of unethical hackers • **What**: A ransomware security incident • **When**: Tuesday, approximately at 9:00 a.m. • **Where**: At a small U.S. health care company • **Why**: An organized group of unethical hackers were able to access the company's systems using a phishing attack. The cause of the security incident was a phishing email that contained a malicious attachment. Once it was downloaded, the ransomware was

	launched on the company's system, encrypting critical files. The attackers' motivation appears to be financial because they left a ransom note stating that the company's files were encrypted and demanded a large sum of money in exchange for the decryption key.
Additional notes	- The health care company could educate employees and staff to prevent an incident like this and ensure it will not occur again. - Should the company pay the ransom to retrieve the decryption key?