Incident handler's journal

Date: January 1, 2024	**Entry: #1**
Description	Documenting a cybersecurity incident
Tool(s) used	None.
The 5 W's	• Who caused the incident? An organized group of unethical hackers, known for targeting healthcare and transportation industries, initiated the security breach. • What happened? The clinic's computer files were encrypted by ransomware following the successful deployment of malware through a phishing email, rendering essential systems inaccessible. • When did the incident occur? The security incident took place on a Tuesday morning at 9:00 a.m. • Where did the incident happen? The incident occurred at a small U.S. health care clinic specializing in primary-care services. • Why did the incident happen? The attackers gained access to the clinic's network through targeted phishing emails, exploiting employees who unknowingly downloaded a malicious attachment. The attackers demanded a ransom in exchange for the decryption key.
Additional notes	The scenario highlights the critical need for robust cybersecurity measures and employee training to mitigate the risks associated with phishing attacks. Additionally, it raises questions about the clinic's existing security infrastructure and incident response plan. How promptly and effectively the organization responds to this incident will be crucial in minimizing the impact on patient care and business continuity.

Scenario

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