Incident handler's journal

Date: November 28, 2024	**Entry: 1**
Description	Operations were disrupted by a major security incident that occurred at a small primary-care clinic in the United States. Workers saw a ransom message on their computers and complained that they couldn't access important information, such as medical records. According to the message, the company's files were encrypted by an organized cybercriminal organization that targets the transport and healthcare industries, and they wanted a large ransom for the decryption key.
Tool(s) used	Based on the scenario there were no cybersecurity tools used by the clinic.
The 5 W's	• **Who** caused the incident? The incident was caused by an organized group of unethical hackers. • **What** happened? A ransomware was deployed by the unethical hackers with critical files of the clinic. • **When** did the incident occur? The incident happened on a a tuesday morning at approximately 9:00am • **Where** did the incident happen? The incident happened at a health care clinic in the US that specializes in delivering primary care services. • **Why** did the incident happen?

	The incident happened because unethical hackers were able to gain access to the company's network by using a social engineering technique called Phishing emails, after gaining access to the clinic networks they then encrypted files whereby the clinic was unable to access critical files like patient data. The hackers' purpose was said to be a financial gain because a ransomware note appeared to the systems demanding a large sum of money.
Recommendations	• The Clinic should ensure that employees are well trained and aware by conducting phishing awareness programs. • The Clinic should ensure they have an active and appropriate incident response plan tailored to ransomware attacks. • The Clinic should strengthen their email security enhancement by making use of multifactor authentication (MFA) to add defense in depth for them and also email filtering solutions to block phishing attempts. • The Clinic should implement Intrusion detection system (IDS) and Intrusion prevention system (IPS) to detect, prevent and eliminate any malicious activity.