Date: 5/30/2024	**Entry:** 1
Description	At 9:00 a.m. on Tuesday morning, our team received reports from several employees that they were unable to access their computers and critical files necessary for daily operations. Upon investigation, it was discovered that a ransom note was displayed on their screens, indicating that all company files had been encrypted by a group of hackers known for targeting healthcare and transportation industries. The attackers gained entry through targeted phishing emails containing malicious attachments, which, when opened, installed malware on the employee's computers. Subsequently, the attackers deployed ransomware, encrypting critical files, including patient data, resulting in severe disruptions to our business operations.
Tool(s) used	1. Endpoint Detection and Response (EDR) tools were used to detect and respond to the presence of malware on affected endpoints. 2. Intrusion Detection Systems (IDS) were utilized to identify and alert on suspicious network activity. 3. Backup and Disaster Recovery (BDR) solutions were employed to restore encrypted files from backup copies. 4. Email filtering and security solutions were implemented to prevent future phishing attacks. 5. Incident Response Plan (IRP) was activated to coordinate the organization's response efforts and mitigate the impact of the incident.
The 5 W's	**Who:** The incident was caused by an organized group of unethical hackers known for targeting organizations in healthcare and transportation industries. Their method of entry was through targeted phishing emails sent to several employees of our company. **What:** The attackers gained unauthorized access to our network and deployed ransomware, encrypting critical files and demanding a large sum of money in exchange for the decryption key. **When:** The incident occurred on Tuesday morning at approximately 9:00 a.m. Where: The event took place at our small U.S. healthcare clinic specializing in primary-care services. **Why:** The attackers executed this cyber attack with the intention of extorting money from our organization by encrypting critical files and demanding a ransom for their release.

Additional notes	- Immediate actions were taken to isolate affected systems from the network to prevent further spread of the ransomware. - Law enforcement agencies and cybersecurity experts were notified to assist in the investigation and recovery efforts. - Employee training and awareness programs will be reinforced to educate staff on identifying and avoiding phishing attempts in the future. - Post-incident analysis will be conducted to identify gaps in security measures and enhance our cybersecurity posture against future attacks.