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. Scenario is at the bottom.

Date: May/9/2024	**Entry:** 1
Description	A U.S. health care clinic had its operations interrupted by a security incident that kept them from accessing their files and necessary software. A ransom note was found that was left by a group of unethical hackers that demanded a large amount of money to release their assets. The hackers got in via phishing emails with an attachment that installs malware which multiple employees opened.
Tool(s) used	none
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A group of unethical hackers • **What** happened? They got into the network of a clinic and locked all of the digital assets until they are given a lot of money (ransomware incident). • **When** did the incident occur? Tuesday morning about 9 am • **Where** did the incident happen? U.S. health care clinic

	• **Why** did the incident happen? Employees opened phishing emails containing malware that launched on their computers and locked all their files and software until a ransom is paid.
Additional notes	Employees should be trained/taught how to spot suspicious emails

---

A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job.

Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that all the company's files were encrypted by an organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key.

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.

Once the attackers gained access, they deployed their ransomware, which encrypted critical files. The company was unable to access critical patient data, causing major disruptions in their business operations. The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance.