Incident handler's journal

Scenario

Review the following scenario.

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.

Date: July 23, 2024	**Entry:** #1
Description	Documenting a cybersecurity incident
Tool(s) used	None.
The 5 W's	● **Who**: An organized group of unethical hackers ● **What**: A ransomware security incident ● **Where**: At a health care company ● **When**: Tuesday 9:00 a.m. ● **Why**: The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's

	systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key.
Additional notes	To prevent future incidents like the one experienced, the health care company should implement a comprehensive cybersecurity strategy. This includes conducting regular employee training on identifying and avoiding phishing emails and social engineering tactics. Robust email filtering and security measures should be employed to detect and block phishing attempts. Keeping all software, operating systems, and applications up to date with the latest security patches is crucial to minimizing vulnerabilities. Regularly backing up critical data to a secure, offsite location ensures the ability to recover files without resorting to paying ransoms. Network segmentation should be implemented to isolate sensitive systems and data, limiting potential damage if a breach occurs. Multi-factor authentication should be enforced to enhance access security. Furthermore, an incident response plan must be developed and regularly updated, outlining the steps to be taken in case of a security breach. By combining these measures, the health care company can bolster its defenses and reduce the likelihood of falling victim to such cyber-attacks in the future.