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.

Record a journal entry

Use the incident handler's journal to document your first journal entry about the given scenario. Ensure that you fill in all of the fields:

1. In the **Date** section, record the date of your journal entry. This should be the actual date that you record the entry, not a fictional date.
2. In the **Entry** section, provide a journal entry number. For example, if it is your first journal entry, enter 1.
3. In the **Description** section, provide a description about the entry.
4. In the **Tool(s) used** section, if any cybersecurity tools were used, list them here.
5. In the **The 5 W's section**, record the details about the given scenario.
    a. Who caused the incident?
    b. What happened?
    c. When did the incident occur?
    d. Where did the incident happen?
    e. Why did the incident happen?

6. In the **Additional Notes** row, record any thoughts or questions you have about the given scenario.