Step-By-Step Instructions

Follow the instructions and fill in the sections to complete the activity.

Step 1: Access the template

To use the template for this course item, click the link and select *Use Template*.

Access the template (Incident handler’s journal)

Step 2: Review the scenario

Review the details of the scenario. Consider the following key details:

- A small U.S. health care clinic experienced a security incident on Tuesday at 9:00 a.m. which severely disrupted their business operations.
- The cause of the security incident was a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files.
- An organized group of unethical hackers left a ransom note stating that the company's files were encrypted and demanded money in exchange for the decryption key

Step 3: 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.

What to Include in Your Response

Be sure to include the following in your completed activity:

- The journal entry date and number
- A description of the journal entry
- 1-2 sentences addressing each of the 5 W's of the scenario:
    - Who caused the incident?
    - What happened?
    - When did the incident occur?
    - Where did the incident happen?
    - Why did the incident happen?
- 1-2 sentences on any additional thoughts or questions about the scenario.