Incident handler’s journal

**Activity Overview**

In this activity, you will review the details of a security incident and document the incident using your incident handler's journal. Previously, you learned about the importance of documentation in the incident response process. You've also learned how an incident handler's journal is used to record information about security incidents as they are handled.

Throughout this course, you can apply your documentation skills using your incident handler's journal. With this journal, you can record information about the experiences you will have analyzing security incident scenarios through the course activities.

By the time you complete this course you will have multiple entries in your incident handler's journal that you can use as a helpful reference to recall concepts and tools. Later, you'll add this document to your cybersecurity portfolio, which you can share with prospective employers or recruiters. To review the importance of building a professional portfolio and options for creating your portfolio, read [Create a cybersecurity portfolio](https://www.coursera.org/learn/detection-and-response/resources/H3ujO).

**Scenario**

Review the following scenario. Then complete the step-by-step instructions.

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.

## Step 1: Access the template

**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.

|  |  |
| --- | --- |
| **Date:** 11/20/2023 | **Entry:**  Record the journal entry number.  # 1 |
| Description | Provide a brief description about the journal entry.  Security Incident at U.S. Healthcare Clinic |
| Tool(s) used | List any cybersecurity tools that were used. None |
| The 5 W's | Capture the 5 W's of an incident.  **Who** caused the incident? An organized group of unethical hackers.  **What** happened? A phishing email with a malicious attachment was used to deploy ransomware, encrypting critical files.  **When** did the incident occur? Tuesday morning at approximately 9:00 a.m.  **Where** did the incident happen? At a small U.S. healthcare clinic specializing in primary-care services.  **Why** did the incident happen? The attackers gained access through targeted phishing emails, aiming to extort money by encrypting the company's files. |
| Additional notes | Include any additional thoughts, questions, or findings.  The impact on business operations was severe, leading to a shutdown of computer systems. It's crucial to investigate the phishing email source and enhance employee training on identifying such threats. |

### 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

Be sure to include the following elements 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.

### Step 4: Assess your activity

# Portfolio Activity Exemplar: Document an incident with an incident handler's journal

Here is a completed exemplar along with an explanation of how the exemplar fulfills the expectations for the activity.

## Completed Exemplar

To review the exemplar for this course item, click the link and select Use Template.

Link to exemplar: [Incident handler's journal entry exemplar](https://docs.google.com/document/d/1NdqPmIeVDjRMzVmOz_puj2Vw7YGZTyd_yrdcPqLTVYc/template/preview?usp=sharing)

OR

If you don’t have a Google account, you can download the exemplar directly from the following attachment.

[Incident handler's journal entry exemplar](https://d3c33hcgiwev3.cloudfront.net/c3BfRpn4Tjajvi1CSwIwsQ_d37e89552c6a41b58442364bb43970f1_Incident-handler-s-journal-entry-exemplar.docx?Expires=1702080000&Signature=ctEGpnmM~QrdqD9ZVDCC2apmXB1lNGupgeMaenodaXtDVbskpqFUymRnQVDDAPZcz~5Xe2AhZUuRqsvaGgIyddEndMbid1HiQ4J1f-~jGQLFVQRqKJBZkWYeylMxw5zKbx~vSf2YPIis3BpDYtb~pR0wCMmarGELf1q~6xgNjww_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/c3BfRpn4Tjajvi1CSwIwsQ_d37e89552c6a41b58442364bb43970f1_Incident-handler-s-journal-entry-exemplar.docx?Expires=1702080000&Signature=ctEGpnmM~QrdqD9ZVDCC2apmXB1lNGupgeMaenodaXtDVbskpqFUymRnQVDDAPZcz~5Xe2AhZUuRqsvaGgIyddEndMbid1HiQ4J1f-~jGQLFVQRqKJBZkWYeylMxw5zKbx~vSf2YPIis3BpDYtb~pR0wCMmarGELf1q~6xgNjww_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

## Assessment of Exemplar

Compare the exemplar to your completed activity. Review your work using each of the criteria in the exemplar. What did you do well? Where can you improve? Use your answers to these questions to guide you as you continue to progress through the course.

***Note:*** The exemplar represents one of many possible ways to complete this activity. Yours will likely differ in certain ways. What’s important is that your incident handler's journal records the details of the scenario. Knowing how to use an incident handler's journal to record notes and additional details during an incident investigation is important because it can be used as a reference for future incident response efforts.

The exemplar contains one completed journal entry. The journal entry is dated, numbered, and provides a brief description of the scenario. Additionally, in the **The 5 W's section**, the journal entry addresses the following about the scenario:

* Who caused the incident?
* What happened?
* When did the incident occur?
* Where did the incident happen?
* Why did the incident happen?

Lastly, the journal entry includes additional questions about the scenario in the **Additional notes** section.

**Note**: The exemplar contains the first entry in the incident handler's journal. As you progress through the course, you'll complete the subsequent journal entries in your incident handler's journal template.

**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.

|  |  |
| --- | --- |
| **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 | 1. How could the health care company prevent an incident like this from occurring again? 2. Should the company pay the ransom to retrieve the decryption key? |

**Review a final report**

## Activity Overview

In this activity, you will review an example of a final report and answer a series of quiz questions.

So far, you've learned about the actions involved in the Post-incident Activity phase of the NIST Incident Response Lifecycle. This includes the development of the **final report**, which is documentation that provides a comprehensive review of an incident. It includes essential details of all events related to the incident and recommendations for future prevention.

## Scenario

Review the following scenario. Then complete the step-by-step instructions.

You recently joined the security team as a level-one security operation center (SOC) analyst at a mid-sized retail company. Along with its physical store locations, your company also conducts operations in e-commerce, which account for 80% of its sales.

You are spending your first week of training becoming familiar with the company's security processes and procedures. Recently, the company experienced a major security incident involving a data breach of over one million users. Because this was a recent and major security incident, your team is working to prevent incidents like this from happening again. This breach happened before you began working at the company. You have been asked to review the final report. To gain an understanding of the incident's life cycle, your goals for your review are as follows:

* Goal 1: Identify exactly what happened.
* Goal 2: Identify when it happened.
* Goal 3: Identify the response actions that the company took.
* Goal 4: Identify future recommendations.

**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.

|  |  |
| --- | --- |
| **Date:**  12-1-2023 | **Entry:**  # 2 |
| Description | Started reviewing the final report of a recent security incident at the retail company. |
| Tool(s) used | N/A |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? An individual * **What** happened? Unauthorized access to customer PII and financial information due to a vulnerability in the e-commerce web application. * **When** did the incident occur? Dec 28, 2022 at 7:20 P.m, PT (initial email on Dec 22, 2022) * **Where** did the incident happen? in the e-commerce web application * **Why** did the incident happen? Due to a vulnerability in the e-commerce web application, leading to unauthorized access and data exfiltration |
| Additional notes | . The incident involved unauthorized access to customer data.  . The timeline of events is crucial for understanding the incident’s progression.  The root cause seems to be a vulnerability in the e-commerce web application.  . The response actions include collaboration with the PR department and offering identity protection services.  . Future recommendations involve routine vulnerability scans and penetration testing, along with an access control mechanism. |

# **Step 1: Access supporting materials**

## INCIDENT FINAL REPORT

### **Executive summary**

The organization experienced a security incident on December 28, 2022, at 7:20 p.m., PT, during which an individual was able to gain unauthorized access to customer personal identifiable information (PII) and financial information. Approximately 50,000 customer records were affected. The financial impact of the incident is estimated to be $100,000 in direct costs and potential loss of revenue. The incident is now closed and a thorough investigation has been conducted.

### **Timeline**

At approximately 3:13 p.m., PT, on December 22, 2022, an employee received an email from an external email address. The email sender claimed that they had successfully stolen customer data. In exchange for not releasing the data to public forums, the sender requested a $25,000 cryptocurrency payment. The employee assumed the email was spam and deleted it.

On December 28, 2022, the same employee received another email from the same sender. This email included a sample of the stolen customer data and an increased payment demand of $50,000.

On the same day, the employee notified the security team, who began their investigation into the incident. Between December 28 and December 31, 2022, the security team concentrated on determining how the data was stolen and the extent of the theft.

### **Investigation**

The security team received the alert and traveled on-site to begin the investigation.

The root cause of the incident was identified as a vulnerability in the e-commerce web application. This vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. This vulnerability allowed the attacker to access customer purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated.

After confirming the web application vulnerability, the security team analyzed the web application access logs. The logs indicated that the attacker accessed the information of thousands of purchase confirmation pages.

### **Response and remediation**

The organization collaborated with the public relations department to disclose the data breach to its customers. Additionally, the organization offered free identity protection services to customers affected by the incident.

After the security team reviewed the associated web server logs, the cause of the attack was very clear. There was a single log source showing an exceptionally high volume of sequentially listed customer orders.

### **Recommendations**

To prevent future recurrences, we are taking the following actions:

* Perform routine vulnerability scans and penetration testing.
* Implement the following access control mechanisms:
  + Implement allow listing to allow access to a specified set of URLs and automatically block all requests outside of this URL range.
  + Ensure that only authenticated users are authorized access to content.

# Step 2: Please answer these questions.

1. What type of security incident was the organization affected by?

. Data breach

2. Which section of the report included an explanation of the root cause of the incident?

. Investigation

3. what did the attacker use to exploit the e-commerce web application vulnerability?

. Force browsing

4. What recommendation did the organization implement to protect future re-ocurrence?

. Perform routine vulnerability scans and penetration testing

. Implement access control mechanism, including allow listing and ensuring authenticated user access to content