**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:**  03/02/24 | **Entry:**  2 | | |
| --- | --- | --- | --- |
| Description | Major data breach of over one million customers | | |
| Tool(s) used | none | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Unethical hackers * **What** happened? Unethical hackers attacked an e-commerce application vulnerability, where the hackers gained personal data and held it hostage for ransom. * **When** did the incident occur? December 28, 2022, at 7:20 p.m., P.T. * **Where** did the incident happen? Via an employee's email at an e-commerce application company. * **Why** did the incident happen? Because of a vulnerability in an e-commerce application | | |
| Additional notes | 1. Why didn't the employee report it the first time it happened? | | |