## Activity Overview

In this activity, you will review an example of a final report.
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.
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 accounts 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.