Scenario

You're the first cybersecurity professional hired by a growing business.

Recently, a deposit was made from the business to an unknown bank account. The finance manager says they didn't make a mistake. Fortunately, they were able to stop the payment. The owner has asked you to investigate what happened to prevent any future incidents.

To do this, you'll need to do some accounting on the incident to better understand what happened. First, you will review the access log of the incident. Next, you will take notes that can help you identify a possible threat actor. Then, you will spot issues with the access controls that were exploited by the user. Finally, you will recommend mitigations that can improve the business' access controls and reduce the likelihood that this incident reoccurs.

Steps

Step 1: Review the event log of this payroll incident

Event logs contain information related to the operation and usage of a system. They can be utilized to identify suspicious activity, detect vulnerabilities, and track users.

Find the **Event log** tab of the Accounting exercise spreadsheet. Carefully review the event log of this incident to start your investigation. Notice the Event Type, Date, Time, and IP Address of the user in the log details.

Make **1-2 notes** of information that you learned about the user from reviewing the Event log details. Add your notes to the **Notes** column of the access control worksheet.

Step 2: Identify access control issues that led to the incident

Log details tell you a lot about a specific moment in time. You can find other useful details about an event by cross referencing that information with other sources.

This business has a range of different employees. They all currently manage company resources using a shared cloud drive.

Find the **Employee directory** tab of the Accounting exercise spreadsheet. Compare the information found in the Employee directory tab with the information in the Event log tab. Notice any similarities between the details in the Event log and the details in the Employee directory.

Then, list **1-2** issues that you discover with how the business handles employee access in the **Issues** column of the Access control worksheet.

Step 3: Recommend mitigations that can prevent a future breach
You've completed your accounting of the strange payment and discovered flaws with how the business handles their information.

Find the **Recommendation(s)** column of the Access control worksheet. Make **at least 2** recommendations of mitigations the business can implement to prevent incidents like this in the future.

For example, one recommendation might be to have procedures in place to revoke access to files when an employee is no longer with the company.