Activity Exemplar: Improve authentication and authorization for a small business

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

Completed Exemplar

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

Link to exemplar: Access control worksheet exemplar

OR

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

Assessment of Exemplar

Compare the exemplar to your completed asset inventory. 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 possible way to complete the activity. Yours will likely differ in certain ways. What’s important is that your review of the security incident considers effective access controls that can be implemented and how a lack of controls can put information at risk.*

Let's review the details of the completed access control worksheet:

Note(s) about the user:

- The event took place on 10/03/23.
- The user is Legal/Administrator.
- The IP address of the computer used to login is 152.207.255.255.

Event logs can often help you identify the who, what, and why of a security incident.

Access control issue(s):

- Robert Taylor, Jr. is a contractor with admin access.

- His contract ended in 2019, but his account accessed payroll systems in 2023.

Oftentimes, incidents like this occur because systems are misconfigured or misused. That is the case with how this business is sharing information among its employees.

Recommendations:

- User accounts should expire after 30 days.
- Contractors should have limited access to business resources.
- Enable multi-factor authentication (MFA).

It appears as though a former employee is potentially the threat actor. However, it's possible that they were not the person responsible for this security incident.

It is common for people to reuse login credentials across many services. And if those credentials are compromised on one platform then an attacker can use them to gain access to others. In this case, implementing access controls, like password policies, limited file permissions, and MFA can protect the business from incidents like this.

Key Takeaways

This activity highlights how easy it can be to lose track of users, which can leave a business open to unnecessary risk if effective access controls are not in place. The activity also demonstrates the risk of operating a business with open, shared access to resources. Setting boundaries around who can access information and what they are allowed to do should be the starting point of any security plan.