Activity Exemplar: Score risks based on their likelihood and severity

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 following link and select *Use Template*.

Link to exemplar:

Risk register

OR

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

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 possible way to complete the activity. Yours will likely differ in certain ways. What’s important is that you've considered how likelihood and impact affect how organizations approach risk management.*

Next, you can review the results of a completed risk register:

Notes

Some risk factors to have considered might have been the number of other companies that interact with the bank. These sources of risk might introduce incidents beyond the bank's control. Also, the risk of theft is important to consider because of the number of customers and the operational impact it could have to the business.

Likelihood

A range of likelihood scores were estimated based on factors that could lead to a security incident. Each risk was scored as a 1, 2, or 3 on a risk matrix, meaning the chances of occurring were rare, likely, or certain. A supply chain attack caused by natural disaster was scored with a 1, meaning it was regarded as unlikely due to the unpredictability of those events. On the other hand, compromised data events were scored a 2 because they are likely to occur given the possible causes.

Severity

No risk received a severity score less than 2 because risks that involve data breaches such as business email compromise, can have serious consequences. Customers at a bank trust the businesses to protect their money and personal information. Also, the bank's operations could be terminated if they fail to comply with regulations.

Priority

A financial records leak received the highest overall risk score of 9. This indicates that this risk is almost certain to happen and would greatly impact the bank's ability to operate. Such a high overall score signals the security team to prioritize remediating, or resolving any issues related to that risk before moving on to risks that scored lower.

Key takeaways

Risk assessments are useful for identifying risks to an organization’s information, networks and systems. Security plans can benefit from regular risk assessments as a way of highlighting important concerns that should be addressed. Additionally, these assessments help keep track of any changes that can occur in an organization's operating environment.