HANDOUT 15.1: GAP ANALYSIS SCENARIO ACTIVITY

Purpose: To identify the steps of the gap analysis process in a given scenario
Duration: 40 minutes (30-activity; 10-discussion)
Group composition: Table groups
Debrief: Large group discussion

Directions

1. Read the following fence sensors scenario with your team.
2. Discuss the questions as a group and record your answers in the space provided after Option 3.
3. You will have 30 minutes to complete this activity.
4. Be prepared to share your answers with the class.

Gap Analysis Process: Fence Sensors Scenario

Management requested a gap analysis to ensure that the physical protection system at their critical infrastructure was meeting the needs of the organization. As part of this analysis, the team examined the perimeter fence that includes installed sensors to detect any intruder who climbs over the fence. The information the team documented about the fence at each step in the gap analysis process follows.

Step 1: Determine Expected Standard Requirements

While determining expected standard requirements, the team found that the physical protection system design requires that each section of the fence have sensors appropriately spaced to ensure full coverage and detection, regardless of the fence location the intruder selects to climb over. It is management's expectation that alarm activation will occur every time (100% of the time) regardless of where an intruder attempts to breach the fence.

Step 2: Assess Existing Performance Level

While examining the testing strategies, the team documented that security force members conduct weekly tests of different fence sections by climbing the fence at randomly selected locations. They also found that during a recent security force attempt to climb the fence, one section of the fence (approximately four meters in length) did not produce sensor activation.

Since there was a failure in the system — the physical protection system as previously described (in Step 1) did not function as expected — the team must ask additional questions to determine the existing performance level. The team required immediate answers to the following series of questions:

- Is the design of the sensor on the fence preventing the sensor from activating?
- Did the vendor install the sensor properly?
- Has the sensor activated before, during similar types of testing?
- Does the sensor problem appear localized to only that area or is the issue occurring at several sections, requiring all fence sensors to be tested?

- Is management's expectation that the fence sensors operate 100% of the time without failure a realistic expectation?
- What can the organization do to mitigate the situation, in both the short and long term?

Answering these questions helped the team assess the gaps between the expected outcome requirements and actual performance of the sensors. The next stage in the scenario identifies the gap that will lead to the plan that is the outcome of the gap analysis.

Step 3: Identify Gaps

After a thorough review and evaluation of the physical protection system (as it related to the perimeter fence sensor problem), the results of the analysis indicated that the failure was restricted to one four-meter perimeter fence section and was the result of a bad segment of sensors.

In this scenario, we have seen an application of the first three steps in a gap analysis:

- The expected outcome requirement for the sensor is 100% functionality.
- The weekly security force tests measured and assessed the existing performance.
- The team identified the gap: 100% failure of one four-meter fence section.

Next, we can see how to complete the process by examining how the team defined the risk management plan in Step 4.

Step 4: Define Risk Management Plan

Once the team identified the gap, the next step was to decide how to manage the identified risk. This included defining the action needed to address the risk management of the critical infrastructure. As part of this process, the team examined three options for the organization:

- Option 1: Accept the risk and do nothing.
- Option 2: Transfer the issue to another organization, such as an insurance company.
- Option 3: Accept responsibility and attempt to mitigate the risk through implementation of new or enhanced physical protection system strategies.

Risk Management Options

Decision-makers construct the risk management plan for their organization by evaluating three basic choices to mitigate risk.

Option 1: Accept the Risk and Do Nothing

The first option for an organization is whether to choose to accept the risk and do nothing. This choice would only be appropriate in situations where the risk may be so minimal that selecting not to act would fall within acceptable safety guidelines as set down by the management of the critical infrastructure.

For example, an organization discovered they could change the lighting type in the facility parking lot from older vapor lighting bulbs to new high intensity bulbs, which would increase the amount of light in the parking lot significantly.

- After conducting an analysis, they decided to accept the risk and delay changing out all the bulbs. In this case, the cost and benefit associated with the new light type did not justify a total change out.
- The existing lights were still sufficient to light the area according to standard operating procedures.
- Instead, the organization decided to replace the light bulbs, as they naturally burn out, with the new high intensity bulbs.

This option is not to be confused with avoidance, which is typically not an acceptable alternative.

- Avoidance alludes to an identified problem that has a higher level of risk associated with it and does not represent a viable and productive solution.
- To avoid the problem is to knowingly assume an extreme liability to the overall protection strategy of the critical infrastructure, possibly rendering the entire strategy ineffective.
- Avoidance is not considered an option in this course.

Option 2: Transfer the Issue to another Organization

The next option available to decision makers is to transfer the issue to another organization.

- There may be another organization responsible for paying for security upgrades, but it is usually an insurance company.
- An insurance company can provide assurance so that if a loss occurs, the insurance company will reimburse the organization for expenses associated with the loss.
- Insurance companies will typically require you to provide an appropriate level of security for any insured items.
- If you do not meet the level of security prescribed by the insurer, the insurance company may assign the liability of loss to the organization.

Additionally, losses that cybersecurity is meant to prevent — theft of critical information or disruption of critical processes — are often difficult to insure due to the often undefined nature of the information and the consequences associated with the loss of information.

Option 3: Accept Responsibility and Mitigate Risk

The last choice is for the organization to accept responsibility and attempt to mitigate the risk through the implementation of new or enhanced physical protection strategies. This choice involves decision makers rendering a number of decisions that can affect personnel, finances, and other resources, both internal and external to the organization.

Discussion Questions for the Fence Sensors Scenario:

1. **Is the option to accept the risk and do nothing acceptable? Why or why not?**

2. **Is the option to transfer the problem to another organization acceptable? Why or why not?**

3. **Is the option to accept responsibility acceptable?**

4. **How could the organization mitigate risk?**

Gap Analysis Process: Fence Sensors Scenario, Continued

Step 4: Define Risk Management Plan

The team recommended Option 3 — for the organization to accept responsibility.

- As a result, in the short term (while arrangements were being made to replace the sensors), a security force member was to be posted at the damaged fence section until sensor repairs and replacements were completed.
- In the long term, the team asked the organization to consider replacing all sensors if the problem turns out to be systemic.

This choice involves a number of decisions that affect other areas internal and external to the organization.

- For example, the organization will issue a contract and use an external contractor to replace the fence section.
- In addition, the allocation of security force members to the fence location may require additional personnel or overtime expenses.
- In the future, the organization must consider finances and security force requirements again as sensors are replaced in other areas.