Week 2 Homework: Assessing Security Culture

This week we learned about security culture and how to promote it within organizations.

It’s important that all employees are aware of common security risks and treat security seriously. The majority of cyberattacks aim to exploit human weaknesses with methods like phishing.

For this reason, people are most often the weakest link in an organization’s security defenses.

Scenario

- Employees at SilverCorp are increasingly using their own personal devices for company work.
- Specifically, over half of all employees check their work email and communications via Slack on their personal mobile phones.
- Another 25% of employees are doing other work-related activities using work accounts and work-related applications on their personal phone.
- Allowing sensitive work information to be shared on employees’ personal devices has a number of security implications.
- You must research these security risks and use the security culture framework to develop a plan to mitigate the concerns.

Instructions

Compose the answers to the following four steps in a Google Doc.

Step 1: Measure and Set Goals

Answer the following questions:

1. Using outside research, indicate the potential security risks of allowing employees to access work information on their personal devices. Identify at least three potential attacks that can be carried out.

2. Based on the above scenario, what is the preferred employee behavior?

    - For example, if employees were downloading suspicious email attachments, the preferred behavior would be that employees only download attachments from trusted sources.

3. What methods would you use to measure how often employees are currently *not* behaving according to the preferred behavior?

    - For example, conduct a survey to see how often people download email attachments from unknown senders.

4. What is the goal that you would like the organization to reach regarding this behavior?

    - For example, to have less than 5% of employees downloading suspicious email attachments.

Step 2: Involve the Right People

Now that you have a goal in mind, who needs to be involved?

- Indicate at least five employees or departments that need to be involved. For each person or department, indicate in 2-3 sentences what their role and responsibilities will be.

Step 3: Training Plan

Training is part of any security culture framework plan. How will you train your employees on this security concern? In one page, indicate the following:

- How frequently will you run training? What format will it take? (i.e. in-person, online, a combination of both)

- What topics will you cover in your training and why? (This should be the bulk of the deliverable.)

- After you’ve run your training, how will you measure its effectiveness?

This portion will require additional outside research on the topic so that you can lay out a clear and thorough training agenda.

Bonus: Other Solutions

Training alone often isn't the entire solution to a security concern.

- Indicate at least two other potential solutions. For each one, indicate the following:
  - What type of control is it? Administrative, technical, or physical?
  - What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?
  - What is one advantage of each solution?
  - What is one disadvantage of each solution?

Submission Guidelines

Submit this homework assignment in a Google Doc.

- You can submit all four steps in the same document. Make sure that anyone can view and comment on your document.
- Title your document with the following format: `[Your Name] Unit 2 Homework`
- Submit the URL of the Google Doc in Bootcamp Spot.