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.***
    - From a company policy perspective, allowing employees to use their personal devices is in itself a poor policy and opens the entire network security/data open to vulnerabilities/attacks and should be addressed immediately.
    - Potential security risks include: poor filter applications allowing employees the ability to download data is a security risk. Accessing work email and communications via slack on personal mobile phones is a security risk, and

allowing employees access to sensitive data that is not critical to their job and allowing them to share that data on their personal phone is also a security risk. Most of these examples can be addressed with training and improving/updating company policy.

- Three potential attacks that could be carried out are:
  i. Ransomware Attack
  ii. Internet of Things (IoT) Attack
  iii. Phishing Attack

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

The preferred behavior would be to only access the network using secure devices and reducing the number of employees who can access the network via personal devices to those who have been approved and established a more secure/encrypted connection. IT is important to reduce the number of phishing attacks as well, and last, limiting employees' access to data is another behavior that would be beneficial to network security.

- 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?

- Provide monthly training to employees on new policies
- Provide monthly training on phishing attacks
- Perform random phishing email tests. Record the name of each employee who clicks on the phishing attachment. Provide retraining as needed for 3 months. After three months, begin the progressive discipline process.

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

- The overall goal is to prevent employees accessing sensitive data and having the ability to share that data to their own personal devices.

Step 2: Involve the Right People

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

1. <u>Chief Executive Officer (CEO):</u> The CEO is responsible for plotting the overall direction of the company and conceiving and communicating a corporate mission or ultimate goal,

determining what the business should focus on in order to meet those goals, assessing risks, and setting standards of social responsibility for the organization.

2. Chief Financial Officer (CFO): The CFO is responsible for charting and monitoring the company's financial trajectory, in other words, they are ultimately responsible for budgeting, which helps ensure that the company uses its funds wisely.
3. Chief Operating Officer (COO): The COO is responsible for ensuring business functions operate effectively day-to-day, monitor day-to-day operations, keeps the CEO aware of significant achievements and setbacks, and oversees people management (hiring, promotion, firing).
4. Chief Information Officer (CIO):The CIO is responsible for developing IT systems that support the business including setting up corporate networks, provisioning services like VPN, setting up and recycling employee devices, and ceasing servers for data storage and internal application development.
5. Chief Information Security Officer (CISO): The CISO is responsible for managing risk to an organization's data throughout its lifecycle. This means they are responsible for ensuring that the company's data is safe from the time it's collected to the time it's stored and retrieved.

- 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)
    - .The overall training curriculum and format will be conducted monthly and in-person. Training will be performed by the IT Department Manager and or designees.
    - Tests will be given and scores recorded at the completion of the training. Employees will also sign updated notifications of the new policies.
    - Training will be provided to all employees and will be the primary focus for the first three months of the company's already established employee engagement/training program.
    - Monthly vulnerability tests will be performed by the IT department to monitor employee behavior.
    - After three months, employees who are in violation of policy may be subject to the progrssive discipline policies of the company.

- What topics will you cover in your training and why? (This should be the bulk of the deliverable.)
    - **Network Security:** provide training on basic security. Inform employees of new changes/updates to the security network
    - **Email: do's and dont's:** This will go over email topics like malware,phishing and other security risks
    - **Network access:** This will go over changes to network access and why the need to improve security. Will demonstrate how to navigate to public folders so all employees are aware of where company policies are located.

    - **Personal Devices:** This topic will go over the new policies regarding personal devices
    - **Help Desk:** This topic will privy employees with ways to contact help desk, resolve andy issues and or answer questions

- After you've run your training, how will you measure its effectiveness?
    - The IT department will monitor traffic and determine if phishing/malware/and other attacks have been reduced.
    - The IT department will monitor log in access and determine how successful the training was in reducing the use of personal devices.
    - The IT department will provide random phishing tests to all employees and document employee behavior
    - The IT department will also provide follow up training on a as needed basis as well as continue to provide regular Security training at all monthly Employee Engagement Trainings as well as at Employee Annual In-Service Trainings.

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.
