Cybersecurity

Module 2 Challenge Submission File

Assessing Security Culture

Make a copy of this document to work in, and then answer each question below the prompt. Save and submit this completed file as your Challenge deliverable.

Step 1: Measure and Set Goals

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.

These personal devices can be stolen or lost leaving information vulnerable. Also, employees that leave the company or get fired can still have this information. Three types of attacks can be ransomware malware, Phishing attacks and DDoS.

2. Based on the previous 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.)

employees should only use secured and trusted connections. All employees should have proper training(CBTs) and not download anything or click on suspect emails. Should have strong passwords and stick to company training.

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.)

Phishing emails and links can be sent out to individuals to see if they take the bait. Employees that take the bait will need to take additional training classes. Employees who don't can be rewarded with some kind of incentive.

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.)

The goal is to have 0% of Undesired behavior among these employees within a year's time frame. Implementing the proper CBT training on how to mitigate and identify these risks will ensure employees' awareness and abilities to achieve it.

Step 2: Involve the Right People

5. List at least five employees or departments that should be involved. For each person or department, describe in 2–3 sentences what their role and responsibilities will be.

CEO-Manages the company and directs its objective and primary goals. The CEO is above a team of executives that make major decisions, joint ventures, employment decisions , acquisitions and more.

COO-Has a dual role of chief executive and a manager who oversees day to day administrative and operational functions. They make sure operations are on track to keep the business up to par and implement policies.

CFO-Responsible for managing any financial actions of the company. They track and analyze the strengths and weaknesses of the money side to ensure the company's success.

CTO-Oversees the whole information technology department in which is responsible for integrating the needs of the business and requirements of IT operations and planning.

Managers-Organize, plan, direct objectives to reach a specific goal. They allocate resources to employees to achieve a company's plan.

Step 3: Training Plan

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

A large meeting will be held in an area that can accommodate all employees to discuss the training, plan of attack, and what's to be expected. Then employees will complete a series of training modules online during company time. If the training is not complete or individuals fail to comprehend, they will not be allowed access.

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

Topics will be about security threats and the different types of attacks. Also about what to do when you come across these and what to do to avoid them. Explaining the threats and the harm they can do will help them be more defensive and how to report the incidents when they occur.

8. After you've run your training, how will you measure its effectiveness?

Monitor the success rate of individuals that passed the training courses. Also send out Phishing emails to see if the employees follow training. This can be done monthly or quarterly to see if employees remember the training.

Bonus: Other Solutions

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

```
VPN for employees
a.Administrative
b.goal is to be able to use a secure network, it is preventive.
C.its a private network, harder to hack
D.cost and time
```

```
Firewall Systems
A.technical and physical
B.preventive and detective goal
C.provide protection against outside cyber attacks, monitor traffic,
protection against trojans, access control, better privacy
D.cost, user restriction, performance, malware attacks, complex operations
```