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.

```
Improper mobile management, data theft, Malware
```

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.)

```
Preferred employee behavior would be to practice safe measures and protect
themselves from cyber threats.
```

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.)

```
I would send phishing emails and document how many out of every employee
fell for the phishing emails and implement training on how to protect
themselves from scams.
```

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.)

```
My goal would be 1 out of every 20 people clicking on the phishing emails.
```

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.

```
The IT department. Their job is to monitor and implement the best practices
for employee training purposes.It would also be their job to keep all
software up to date.The IT department would also be in charge of mitigating
risk. Managers. Their job would be to spread cyber awareness to their team.
For example, it would be the managers job to ask their team to avoid
suspicious emails.The building should also have security officers to monitor
activity inside and outside.Their job would be to guard the building and
make sure that only authorized employees are able to access the facility.The
employees. It would be best practice for the employees to protect themselves
from the dangers of cyber crime and what that could mean for their job
safety.
```

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)?

```
I would run a combination of both training online and in person.
```

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

Keep software and hardware up to date to protect companies from new and existing security vulnerabilities, avoid suspicious emails to avoid someone trying to gain access to information, use anti virus and anti malware to reduce vulnerability, checking links before you click to avoid being targeted, using a VPN to protect personal information, and enable two factor authentication to make sure the right person is accessing the account.

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

The effectiveness will be measured on how many employees can learn and adapt to new changes.

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?

Physical solutions would be key cards to get into the building that only employees can have with security and strict rules on tailgating preventing employees without the key card to get in the building. One advantage would be to make sure only authorized employees enter. A disadvantage would mean even one person slipping in could put the company and employees at some sort of risk.

An Administrative solution would be to implement two factor authentication for every employee, whether it's in office, hybrid, or work from home. Only authorized individuals should have access to protected company information and data. One advantage is making sure only authorized employees have access to work computers. One disadvantage is if someone were to lose their phone, tablet, etc or if the battery dies and not be able to get themselves authenticated.