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.

```
Allowing employees to access work information on their personal devices
could put that at risk, vulnerability to malware, data leakage, and
malicious apps.
```

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.)

```
The preferred employee behavior would be to only access work information on
a device that is approved by the company itself to limit the possibilities
of these scenarios
```

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 monitor emails and which devices are used to access work information on personal devices.
```

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.)

```
I would like for the organizaion to reach 0% of employees but a realistic goal would be 3%-5%
```

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.

```
1 department that should be involved is HR they are the who the people go to for a lot of questions so if they aren't practicing the same security measures they teach they shouldn't be working there. Another would be the security team, they are the biggest on security so they should all be aware of the risks. Another department would be the IT team or whoever is incharge of websites, they are working behind the scenes a lot so they should be aware of all the safety precautions. The 4th department should be anyone in administration, they have access to a lot more data so they should be well aware of all the risks. And finally the CEO,COO,CISO, etc should be involved and aware of all the risks because they have the most access to sensitive data.
```

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 use a combined in person training followed by homework
```

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

```
The topics i would cover in the training are the risks of accessing work
info on a personal device and the risk of phishing emails
```

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

```
We can measure the effectiveness by monitoring what devices access what and
and sending out phishing emails to see who clicks on it.
```

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?

```
Another solution would be to restrict access on non administrative confirmed
devices, this would be administrative, technical and preventive control. It
an advantage would be that noone would be able to access data on their
personal devices and a disadvantage would be that you have to manually
select what devices are allowed.
```

```
Another solution would be creating a separate server where any data you
wouldn't want getting out to be stored. This would be Administrative and
physical control. That would be preventative and deterrent control. One
advantage would be if someone hacks into a device that does not have access
to this server it would still be secure a disadvantage would be having to
move all of the data over to that server along with the price of another
server and installation.
```