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.

```
Man in the Middle attacks, Spear Phishing, Malware or 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.)

```
I'd say that the preferred behavior for employees would be to not to open
suspicious email attachments. Also that they should only be using work
approved apps while connected to the network. Also to ensure that their
security features are updated regularly to the most recent versions.
```

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'd send out a company wide email with a link to a site that I created to track how many times the site is visited.

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 should be 0%, but the reality is that the goal should be something attainable, so I'd say 5% or less of the total staff visited the site.

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.

- Chief Executive Officer- Their role would be to provide support for the above stated audit. Also to ensure that the audit is taken seriously.

- Chief Information Officer- To be informed of the audit taking place. Also they are to help ensure that the information is true and accurate.

- Director of HR- Their role would be to ensure staff in their department is aware of the audit. Also they must stand behind the results to help make new guidelines.

- Person involved in training- This person will have to be informed, so they can begin to evaluate current training strategies. To see what else they can do to improve the training

- Information and Security Department- This department will have a heavy role in this task since they will have to draw up the email. They will also have to ensure that the email is sent to only employees, so as to not create faulty 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'd perform quarterly training with 25% of the staff coming in each quarter until we were at 100% of the staff being trained. I'd do this in person to help ensure the staff sees how serious the issue is being taken. In addition I'd be doing quarterly online refresher courses to keep the topic fresh in the staff's minds.
```

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

```
My topics for the training will be Phishing and data security. My main topic would have to be Phishing. I'd make sure that employees know that it may simply take a click or tap of your finger to invite unauthorized users into your personal devices, and the companies networks. So the best policy would be to not open emails or links from unknown senders. Though the emails don't necessarily have to be from unknown senders, so to always be vigilant in any and all tasks done on personal devices.
Also I'd cover training on data theft. Which can be done quite easily, so to protect your information both within the company and on your personal devices. Don't just blindly give permissions to websites to accept cookies or even to save your passwords to sites.
```

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

```
I will do another email with a link to a website we created to track the traffic. If the traffic has decreased from the previous test then we will have increased our effectiveness.
```

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?

```
You could not allow employees to access public networks for confidential
work.
   A. This would be a Technical control
   B. The goal for this control is to prevent the employees from putting
      private/confidential information from less secure networks.
   C. The main advantage for this is that it helps to keep information on
      protected networks. So long as you keep your hardware up to date and
      scanned regularly.
```

```
You could install an Intrusion Detection System.
   A. This would be a Technical control
   B. The goal for the Intrusion Detection System would be to notify you of
      potential breaches, and help you to know where the intrusion was
      detected. This would be a detective control.
   C. The advantage of the Intrusion Detection System would be so you were
      alerted of any breaches. So you can notify the proper staff and work
      on removing the breach as quickly as possible.
```