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.

```
Risks:
Some risks include the fact that employees' personal devices do not have the same security protection that a work specified device would have. Because of this, employees can either knowingly or unknowingly leak sensitive data through accessing public networks or downloading malware knowingly or unknowingly.

3 Potential Attacks:
   -  Malware infections
   -  Phishing emails
   -  Data interception through unsecure networks
```

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.)

```
Based on the three attacks that I listed; for malware infections, employees would have to install some security software to protect against them, for phishing emails, employees would only click on trusted emails, for data interception they would make sure any network they connect to is secure.
```

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.)

```
For malware infections, a survey could be done of whether or not they have security measurements installed on their personal devices. For phishing, a survey could be done on how many emails they click on from unknown senders. For data interception, how many public networks an employee connects to could be tracked.
```

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.)

```
For malware infection, the goal would be to have all employees have at least some sort of security program installed on their devices. For phishing, ideally no employees would be clicking on emails from any unconfirmed source, at least half since about that many employees use their work emails on personal devices. For data interception, employees would have to be trained and not be comfortable connecting to random or unsecured public networks, at least 25%.
```

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 - The role of the CEO is to make the big important decisions. The CEO is responsible for communicating with the stakeholders and being in charge of any crisis response.
```

CIO - The CIO is to be in charge of any incidence responses. The CIO also has to communicate with the information technology to provide any support needed.
Director of HR - HR is in charge of creating and implementing security policies for the employees. They are also the one who communicates with the training and information technology teams with developing and training employees for the necessary procedures.
Training Team - The role includes actually training the employees. As well as keeping up incident reports and tracking the progress of the new security training the employees undergo.
Information Technology Team - They are in charge of vulnerability management with assessing any potential weaknesses in the framework. They are also in charge of securing the network and hardware and regularly accessing security protocols.

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)?

It is hard to say how frequent training will run depending on how needed the security protocols need to be implemented, how it will affect the company's workforce, and how many employees there are. I believe in-person training would work best. If the job is fully remote then an online training would have to be done. It would work as long as it is live training and continuously engaging for the employee. Ideally the training would be done for about 1-2 weeks, then tests and analysis can be run to test the effectiveness of the training and see what else needs to be fixed.

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

For malware infection, the topics to be covered would be what security software would need to be installed on an employee's personal device, as well as being trained on how to ensure these security programs are working properly. For phishing, there would be training to ensure employees do not click on emails from unauthorized senders, and do not click on any unknown links. For the data interception, first an employee must be trained on why exactly connecting to any public network is unsafe. Then they would be

```
debriefed on how to spot an unsecure network, and how to protect their data
from these unsecure network attacks.
```

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

```
For malware infections, employee's devices could be scanned for any
malicious software that could have been installed. For phishing, any clicked
links could be tracked or a survey could be done on how many unauthorized
emails were clicked on or a planned phishing email by the security team
could be sent and tracked that way. For data interception, another survey
could be sent out on how many public network employee's join and which ones
are random and unsecured.
```

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?

```
Give employees work devices.
   a. Administrative
   b. Preventive
   c. The advantage ensures that employees cannot be attacked on their
      personal time or leak sensitive data either knowingly or unknowingly
   d. The disadvantage would be the cost of giving everyone new devices
```

```
Limit access so work applications can only be used when connected to a
specific network.
   a. A combination of technical and administrative
   b. Preventive
   c. The advantage of this is that employees can only access sensitive
      information so they cannot lose or give up sensitive information when
      not at work
   d. The disadvantage would be employees would not be able to conduct work
      or have access to work emails or applications unless at work
```