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.

```
Employers that use their own devices for work purposes can cause a list of
potential security threats. These threats include:

Malware: Many employees have anti-malware security programs on their laptop,
few employees are aware that smartphones can be infected by malware. If a
mobile device has an outdated operating system, that device may be at major
risk of a breach. Many users do not read the fine print on applications, and
a user with unlimited ability to download applications may download a game
or file that contains malware.

Lost or stolen device: A lost or stolen device is one of the biggest threats
to an employer that allows BYOD.

Unsecure Network: Most mobile devices are set up to automatically connect to
any public wifi in range. These public access points could be insecure and
allow anyone to intercept traffic coming to and from an employee's mobile
device. If that mobile device is still connected to the company's network,
that could cause a security breach.
```

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 should be clearly defined in a company
security policy. This policy should include, but not be limited to:

Install a company application that allows control of the personal device in
relation to company data. This application can be used to wipe data from the
personal device if needed.

Ensuring that employees keep their personal devices up to date in regards to
operating system software is key to maintaining device integrity.

All company data should be encrypted in order to avoid the impact of a
potential breach. Using a VPN to secure the company network on the device
should allow more secure incoming and outgoing data.
```

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.)

```
Their are a variety of methods that could be used to measure employee
behavior:

One, hire a security firm to perform phishing campaigns on employee company
and personal emails that are likely to be accessed on a personal device.

Two, task the IT department to run tests on employee personal devices in
order to check if they are properly updated and encrypted. The department
will note how many devices are not meeting company policy.

Three, set up your company network to only allow devices to connect through
a VPN. Monitor all devices that attempt to connect to the company network
without the VPN.
```

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.)

```
By the end of a phishing campaign, the goal for employee click rate of
malicious emails and files would be less than 7%.

The company should expect 100% data encryption and VPN usage on all personal
devices.
```

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. Chief Executive Officer (CEO): All security policies would need
   clearance from the CEO for implementation and funding. The CEO has all
   power to allow or deny any policy that affects the company.
2. Chief Information Officer (CIO): A company's CIO will need to be
   involved with the IT and security department in order to develop and
   implement all cybersecurity policies. The CIO would most likely report
   to the CEO.
3. Chief Audit Executive (CAE): The CAE is responsible for auditing
   employees after the implementation of company policies. The CAE
   reports their findings to the CEO and CIO.
4. Chief Financial Officer (CFO): The CFO would approve all funding
   required for the implementation and running of new or existing
   policies. The CFO adjusts company budgets to assure that funding can
   be secured and allocated to implement, maintain, and enforce company
   policy.
5. The IT Department: The IT department researches and reports the
   programs needed to effectively enforce company policies. The IT
   department is also essential in monitoring and auditing employee
   personal devices to ensure that they are abiding by company policy.
```

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)?

```
Employees will be trained quarterly, with 25% being trained each time. Training will be a combination of both online and in-person. Online training will consist of informational videos and online questionnaires to ensure proper training.
```

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

```
Training topics will cover a variety of security procedures:
   1. Training will cover how to install and use a VPN to connect to the
      company server. This training will also explain why using a VPN to
      secure your connection is important.
   2. Training will inform employees about the potential danger of phishing
      attacks and the significant impact of that can result from a
      successful breach.
   3. Training will inform employees about the employer app that will be
      able to monitor and delete company data from personal devices. The
      training will emphasize the importance of these applications.
   4. Employee training will also cover why maintaining an updated personal
      device is required for security.
```

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

```
The company will run quarterly checks on employee devices in order to ensure it is properly updated and encrypted. The company will contract a security company to run phishing services to measure the effectiveness of online training. A penetration testing service can be utilized to attempt to access personal devices and breach company data. The company will also trach who is logging in to the company servers and who is attempting to log in without the VPN.
```

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?

Compartmentalize data company data vs personal data

a. Technical control
b. This is a preventive control that will allow a company to wipe all company data off of a personal device without that device losing any personal data.
c. An advantage of compartmentalizing data will make it easier to wipe and restore a personal device to the employee without having to completely wipe the device of all data.
d. A disadvantage of compartmentalizing data may be that some devices have a hard time setting up the ability to do so.

Creating a whitelist/blacklist of allowed/unallowed applications

a. Administrative control
b. This is a preventive control. It aims to prevent employees from compromising their devices by restricting applications they are allowed to download on their personal devices.
c. An advantage of creating a whitelist/blacklist is that it is a reliable way of blocking new threats, such as malware and unauthorized software. Whitelists are more effective than blacklists because they are extremely effective at preventing zero-day attacks.
d. A disadvantage of whitelist/blacklist is that both lists are very time consuming to create and maintain.