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.

```
The biggest hurdle for an IT department to overcome with regards to a BYOD
policy is lack of control. Depending on the size of SolverCorps, there are
potentially hundreds of personal devices, with un-uniform OS's (apple v
android), as well as some devices may already be infected and in various
states of being secure (ie: strong/weak passcodes),  that will be able to
access company data from anywhere. From here, we can begin to outline the
potential risks facing Silvercorps vis a vis a BYOD policy.
   1) A lost/stolen device - an insecure lost/stolen device can grant
      unauthorized access to SilverCorp data.
   2) Insider threat - An employee who was fired or quit may still have
      access to SilverCorps data.
   3) Malware - an employee downloaded malicious software from an insecure
      source that IT was not aware of.
   4) Compliance - A data leak may put SilverCorp into non-compliance and
      they may face fines or legal repercussions.
After outlining the potential risks or threat vectors inherent in a BYOD
policy, we can now explore some potential attacks.
```

```
   1) An employee decides that they want to download a new game onto their
      phone from an insecure source. The download has resulted in Malware
      being installed on the employee's device. On Monday, the employee goes
      to work at SilverCorps and connects to the company intranet. The
      malware is now able to infect the company network.
   2) An employee goes out for a night of drinking and loses their phone at
      the bar. They haven't enabled biometrics and their password is
      weak/not enabled. The person who finds the phone is able to unlock it
      and access sensitive SilverCorps data through the lost phone.
   3) The employee receives a phishing email to their personal account and
      clicks through, infecting their device with malware. Once again, when
      they connect to the SilverCorps network, they infect it.
   4) A disgruntled employee has been approached by a competitor and is
      offered money to exfiltrate sensitive data for them. There is no least
      privilege policy in place so the employee is able to access high level
      data from their phone and easily share it with the competitor.
   5) The employee goes to a cafe and connects to the open public network to
      do work. Little do they know that there is a malicious threat
      monitoring all devices that connect to the wifi and is gathering
      credentials using a man in the middle attack. They are able to steal
      their login credentials for SilverCorps.
```

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 behavior for employees is as such.
   a) Lock your personal device using a strong password and biometrics
   b) Only download software/apps/games from trusted sources.
   c) Employ anti-virus/vpn software on your device.
```

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.)

```
When an employee enters into the BYOD program, whether they are new to the
company or an existing employee, they must demonstrate that their device is
in compliance with company policy. They must demonstrate that they have
   a) A strong password, MFA and biometrics enabled
```

```
   b) Anti-virus/vpn software installed and a scan has been run on it.
   c) All apps on the device have been downloaded from trusted sources.
If the device meets this criteria, it will be added to a safe list of
devices allowed to connect to and access the SilverCorps network. All
devices that are not in compliance will not be granted access. IT should
note the devices that came in in a state of non compliance. Then through an
NAC (Network Access Control), IT can track how many non-compliant devices
are attempting to connect to the SilverCorps network. This, however, is not
enough to gauge how many employees are adhering to the company's preferred
behavior outline. A phishing pentest should be conducted every 3 months to
see how many employees do not adhere to download policies. And then every 6
months, employees must re-demonstrate to IT that they still have
anti-virus/vpn software and that their biometrics and MFA are enabled.
```

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.)

```
SilverCorps would like to see no less than 95% of personal devices be in
compliance with the BYOD policy.
```

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.

```
Outlined here are the 5 employees/departments that are essential to creating
a BYOD policy and training program.

   a) CEO: Because this is a business-wide policy that affects all
      departments of SilverCorps, it is imperative to involve the CEO as
      they are in charge of setting the overall direction of the company.
      They would have to approve any new training and policies as a result.
      Furthermore, they will be subject to the new policy themselves if they
      approve it. The CEO is the one who will disseminate the new policy
      among the other department executives, ensuring that the rest of the
      company is up to speed with.
```

```
b) COO: The Chief Operating Officer is the person who is in charge of the
   daily operations of SilverCorps and works closely with the CEO. They
   are also responsible for the management of people at the company so
   their involvement in implementing any new policies will be essential.
   They will be tracking the successes and failures of such a policy in
   order to report them to the CEO.
c) CFO: The cost of creating a training program for a new BYOD policy
   would have to be constructed within the financial budgeting set by the
   CFO. Budget will play a factor in how extensive and frequent training
   for the BYOD policy will be.
d) CISO: The Information Security department is going to be at the center
   of creating the new BYOD policy and responsible for relaying this
   information to the other departments. Their department will construct
   the policy and then be responsible for administering the training to
   all employees.
e) HR: In order to set the policy into action, HR needs to be involved
   for the purposes of scheduling the training sessions, distributing any
   company wide information regarding the policy and ensuring that
   employees actually attend the training.
```

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)?

```
Training will initially be conducted in person, with a target of 25% of the
employees every quarter. Therefore, every year, the entire staff will go
through an in-person training session. Every quarter, an online quiz will be
sent out to test employees' information retention from the in-person
sessions. All new employees will be required to join an in-person session
ASAP.
```

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

```
1) Outline the privacy practices in effect regarding personal and
   corporate use of a personal device. This should be done to ease
   concerns that the company is “just trying to spy on them”.
2) Outline acceptable uses of public wifi, if any. Insecure public
   networks pose a severe risk of a threat actor eavesdropping on a
```

```
   personal device, potentially granting them access to sensitive
   SilverCorps data.
3) The dangers of phishing - How to identify and avoid being a victim of
   phishing and the risks of introducing malware onto a personal device.
4) What is Malware and what can it do to a corporate network? Employees
   need to be aware of how destructive a malware attack can be.
5) How to secure your personal device using MFA, biometrics and the
   importance of strong passwords.
6) Patching policy. SilverCorps needs to outline its standards for having
   a personal device up to date with regards to any security patches. An
   unpatched device can be open to an OS exploit, making it not secure.
7) Role based access. Outline how only information pertaining to your
   role at the company will be made available on a personal device.
   Explain how this can contain the severity of a data breach.
8) Outline a clear procedure to follow in the event of a security breach.
   Employees need to know exactly what to do in order to mitigate the
   breach.
9) What authorization methods are in place to allow access to secure
   company data. Explain if there is a corporate VPN in place and how it
   securely connects the user to company data and outline any MDM
   software that will be used to keep all corporate apps or software
   secure.
10)    Clear outline of the on-boarding and off-boarding policies. When
   can an employee start using their device to access company data and
   when and how does that privilege end upon termination or quitting.
11)    Outline the importance of only using vetted applications by the
   Apple App Store or Google Play. This can be tied into the discussion
   about Malware.
```

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

```
Quarterly phishing pentests coupled with a quarterly security quiz.
Employees that do well will be incentivized to continue their preferred
behavior whereas those that do poorly will be subject to another in person
training session and further follow up assessments.
```

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?

a) Another solution can be that employees may only access company data from their personal device when they are on the secure corporate network and physically on site.This would be a preventative/compensatory control.
b) This is a preventative measure that cuts down on possible data theft by physically requiring employees to be on the secure corporate network before they can access work materials, however, this does not ensure that an employee device has not accessed an insecure network when not at work. This is why it is also compensatory as it only mitigates or limits the device's vulnerability.
c) The advantage of this is that employees cannot access SilverCorps data from an unverified network, making their data more secure.
d) The disadvantage of this policy is that it almost defeats the purpose of having a BYOD policy if employees can only use it on site.Furthermore, employees can still connect to an insecure network outside of work and infect their device that way.

a) Another control we can employ is a stricter password policy that requires all employees to generate a new strong password every quarter. This is a procedural/administrative control.
b) The control is both preventative and compensating. Having password access is already a preventative control.Requiring employees to regularly update this control helps to mitigate any unauthorized access if that password is compromised as it is changed on a regular basis.
c) Ensures all employee passwords are no more than 3 months old and are strong. In the event that a password is compromised, it will only be effective for a shorter period of time.
d) A disadvantage is that enforcing a quarterly password change takes time and may be seen as "annoying" by the employees.