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 bring their own devices presents a myriad of potential threats.

Of these possibilities is the event of a lost or stolen device. Lost and stolen devices make up a very large percentage of data breaches yearly.

Another potential threat is Malware. An employee with an out of date operating system can be seriously at risk if they are infected with malware. Many employees either skim or skip the fine print of apps and downloads onto their personal devices which can also lead to potential breaches of their device.

Finally a large risk is the use of unsecured networks on the device. Whether at a coffee shop, the airport, or even potentially their own home network, the potential targets.

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 should be laid out clearly in company policy.

Encryption of data as well as having remote wipe capabilities is good practice to secure data on a personal device. If the device is compromised, notification of the respective team to lock and wipe a device.

Making sure employees keep up to date devices is critical to maintaining device integrity. As well as potentially limiting downloads and application installation on the device.

Using a VPN to secure the network of the device. Securing your incoming and outgoing data is key. Encryption of messages and emails.

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.)

Hiring a security firm to perform testing on employees by running phishing campaigns against the employees on their personal devices.

Having the IT department run random tests on employees personal devices to check if they are properly updated and encrypted and noting how many are not up to standard.

Ensuring that a personal device cannot connect to the main company network without the aforementioned VPN, and monitoring how many devices attempt to.

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.)

Having less than 10% click through on malicious phishing emails would be good for contracted tests. Getting under 5-7% would be the final goal for malicious emails and files.

As for the encryption and VPN on personal devices that would need to be 0% with a zero tolerance 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.

1. Chief Executive Officer - All of the aforementioned security policies would have to be run by the CEO and cleared for implementation and funding. They would have the final word on if the policies affect the overall direction of the company.

2. Chief Information Officer - The CIO would need to be involved with the IT department to oversee the development and implementation of the policies. They would likely be the one to report to the CEO and inform them of new policy procedures and implementation.

3. Chief Audit Officer - Would be responsible for running auditing after the implementation of the policies. Report their findings to the CEO and CIO so that adjustments can be made to policies and enforcement.

4. Chief Financial Officer - Would be needed to approve funding to the new policies. Would adjust budgets to assure that funds can be secured and allocated to implement, maintain, and enforce the new policies.

5. IT Department - The IT department would be key in researching the programs needed to effectively enforce the new policies. They would also be essential in monitoring and auditing employees to ensure that they are following protocol and maintaining security.

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 be run quarterly with 25% of the staff. A combination of online and in-person will be used. Online training will consist of informational videos to ensure employees are adequately informed on potential risks to their personal devices. In-person would consist of IT specialists training, updating, and auditing personal devices.

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

Online training topics will cover how and why using the VPN to connect to the company servers is important. It will also inform employees about potential phishing techniques and the importance of making sure that you can remotely lock and wipe your phone. In-person training will cover why maintaining an updated device is important, as well as the installation and training on how to use the VPN and encryption of device data.

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

Quarterly checks on employee devices to ensure it is updated and properly encrypted. Running contracted phishing campaigns to measure the effectiveness of the online training. Potentially contracting a security firm to attempt to steal and access information off of a personal device of an employee to ensure encryption and remote access is enabled. Tracking who is attempting to connect to the main company server without a VPN or from a public internet connection.

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?

1. Compartmentalize data on a personal device
    a. This is a technical type of control for the device.
    b. This is a preventative control for the device, if an employee decides to leave a company the corporate data should easily be able to be wiped without losing any of their personal data.

```
      c. One advantage is making it easy to restore a personal device to
         its owner without having to completely wipe it.
      d. One disadvantage is some devices could prove difficult to set up
         compartmentalization on the device.
```

```
2. Using over-the-air configuration for devices
      a. This is a technical type of control.
      b. This would be a preventative or compensating solution.
         Preventative in making sure that updates and essential apps are
         able to be sent to the device without relying on the employee
         seeking help from the correct department, and Compensating for
         employees that might be negligent in updating and securing their
         devices.
      c. One advantage is that you can easily set up emails, calendars,
         VPNs, updates and all kinds of other things to a personal device
         for the employee.
      d. One disadvantage is that it could prove difficult to get
         employees to enroll in the program.
```