Step 1: Measure and Set Goals

Answer the following questions:

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.
    - Lost or stolen devices - if a device is found by a threat actor, they can mine the device for PII or other information relating to the business.
    - Unsecure networks - if an employee uses public wifi to log into their work, they are risking their company's information if the network is not secure. Hackers can use a middle-man approach to siphon data as it comes through.
    - Malware - malware can be in apps that users download to their personal devices such as a smartphone. I was listening to a podcast that mentioned how hundreds to thousands of apps were found to have back doors in them. Most users would never know to look or how to look for that embedded in the code.

2. Based on the above 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.
    - It would be advised that if employees are allowed to use their personal devices, that they not connect to public wifi when logging into their work.
    - To make sure they are setting up strong passwords and using multi factor authentication where it is available.
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 would have MDM software installed on any personal device that will be used for work purposes. Along with installing the MDM software, it would be a requirement that employees use a strong password and logout whenever they are not accessing the work information.
    - Using specific apps that have multi factor authentication to control how the employees are accessing the data.
    - I think monitoring the internet traffic on individual devices would be the best option for monitoring security while also not infringing too much on privacy. It would also be possible to monitor the GPS on individual devices but I think that might be too much, considering it is a personal device.
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.
- One goal would be to have 0% of employees connecting to public wifi when accessing work information.
- Another goal is to have 100% of employees using a strong password.

Step 2: Involve the Right People

Now that you have a goal in mind, who needs to be involved?

> Indicate at least five employees or departments that need to be involved. For each person or department, indicate in 2-3 sentences what their role and responsibilities will be.

1. The CEO will need to work with the board to cover the risks and assume responsibility for the activities of their employees. The CEO will also be involved in writing the policy.
2. The CISO is responsible for ensuring the data privacy is secure. They will also be responsible for making sure the company is in regulatory compliance.
3. The IT department will be responsible for installing the necessary software on the personal devices. They will also need to be available to help troubleshoot issues with the devices when they occur.
4. The CFO will be responsible for making sure everything will be under budget. They will also play a big role in assessing the financial damages that could occur if a cyber attack were to happen.
5. Lastly, the employees will play a large role in making sure they mitigate risks by following protocol. Employees will also play a role in giving feedback to their supervisors if they suspect something is not right.

Step 3: Training Plan

Training is part of any security culture framework plan. How will you train your employees on this security concern? In one page, indicate the following:

- How frequently will you run training? What format will it take? (i.e. in-person, online, a combination of both)
- What topics will you cover in your training and why? (This should be the bulk of the deliverable.)

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

Training will be conducted over the course of a week, every quarter so that the information and expectations are consistent and up to date. Taking one week each quarter will allow smaller groups and will also increase the number of employees that will receive the training. There will always be a few people who are out sick or out of town, so extending the training will accommodate these absences. The format will be both online and in person. Having the training accessible both in person and online will also increase the chance that it will be available for everyone and will also accommodate any employees that are remote so that the company does not have to expense travel.

Topics will include the following: acceptable devices, how to create a strong password, utilizing multi factor authentication, what safe apps are vs. suspicious apps, how to recognize phishing emails, how to prevent a device from being stolen or lost, education of what can happen when connecting to unsecured networks, and lastly it would make the employees aware that they will be losing some privacy due to using a personal device for work.

Going over acceptable devices will cover the type of device, whether it is a cell phone, laptop/desktop, tablet and so on. This will be important because if an employee is not aware what type of device is acceptable, they may use a certain type of computer that is not formatted correctly or is not able to download the necessary software to keep the information protected. Teaching employees what is considered a strong password is extremely important because this can be an easy way for a threat actor to gain access to a device or a system. While teaching them how to create a strong password is important, it is also important to show them how to set up a multi factor authentication in case a password were to be compromised. Most users do not pay attention to the type of apps they are downloading onto their personal devices and if they are not taking precautions while downloading them to a personal device with access to company data, it can risk a threat actor gaining access through a backdoor. I think it would be important to show employees that many apps have been found to have back doors embedded in the code which can allow someone access who does not have the credentials. Along with showing them how to spot trusted apps vs. suspicious ones, it is extremely important to educate employees on phishing emails. Although you cannot teach them how to spot every phishing email, teaching employees certain things to look out for, will greatly increase the chance that your employees will spot suspicious emails. Although it may seem silly to educate employees on how to protect their devices from being stolen or lost, a lot of people do not think about simple

things like leaving their phone sitting on top of their desk while they step away. With the number of employees working remotely increasing more and more, it is important to teach employees the importance of not using public wifi when accessing sensitive company data. Even when not accessing company data, it is important to not connect to public wifi, because you always run the risk of a threat actor stealing information that passes through. Lastly, it is important to make sure your employees understand that they will be giving up some privacy while using their own devices to access company data. Although it sounds obvious, some employees will not understand that using their own device means sacrificing some privacy so it is important to tell them up front.

To ensure the employees are retaining the information taught to them, a short “quiz” will be given to them at the end of the training and a survey will follow. This will give some qualitative data to the employers on what their employees learned and will also give a chance for the employees to provide feedback which will enhance the experience for everyone. Once a month, a phishing email will be sent out to everyone in the company including the executives which will measure how many people are clicking on suspicious emails. The goal would be to have a 5% or less click rate with the expectation that this will decline until they reach a 0% click rate. I think with consistent training, surveys, and phishing emails, this will ensure that the employees are protecting their devices and the data on them.

This portion will require additional outside research on the topic so that you can lay out a clear and thorough training agenda.

Bonus: Other Solutions

Training alone often isn't the entire solution to a security concern.

- Indicate at least two other potential solutions. For each one, indicate the following:
    - What type of control is it? Administrative, technical, or physical?
        - Mobile device management - technical control
        - Intrusion preventive systems - technical
    - What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?
        - I believe MDM would be preventive control because the software is there to mitigate risks when using personal devices.
        - Intrusion preventive systems would be preventive control
    - What is one advantage of each solution?
        - MDM software can erase data remotely in the case of a stolen device.
        - Intrusion preventive systems are great because they not only detect the intrusions but also prevent them actually occurring.

- What is one disadvantage of each solution?
  - MDM can be very expensive especially for an enterprise.
  - Intrusion preventive systems are fairly new and are still evolving but the chance or false positive/negatives due to the system noticing unusual activity and assuming it is malicious.