1. There are huge security risks for allowing an employee to access work information on their personal devices. The first potential attack is the physical device being stolen. There are some cases where it may not be at the fault of the employee, however there are times where the employee carelessly leaves their personal belongings unattended. The second potential attack could be malware, the employee could be using the browser on their device and receive pop ups that may or may not contain malicious code that steals the information from the device. The third potential attack is communication interception, also known as man-in-the-middle attacks, employees could have work on their personal devices and think that it is okay to work in public areas, using the free Wi-Fi around, the potential of a hacker monitoring the Wi-Fi, they could use the people logging into their corporate database and attempt to steal information.

2. For the preferred employee behavior, if you are doing work related activities on your personal devices, do not work on company related documents in public areas where the Wi-Fi is free and not protected or secured. Another is preferably purchasing another phone to utilize specifically for work, that way you can separate junk emails that potentially contain malware and those that are for work related items and people.

3. One way to view if employees are following preferred behavior is by setting up weekly meetings to keep everyone in check and remind them of best practices as well as provide them with a checklist. Another is also potentially providing the said employee with a device solely for work purposes and monitoring their work so that you can see if there are any intrusions, and data is being copied somewhere else.

4. One goal for this company is to have less than 15% of employees doing work-related activities, using work accounts and work-related applications on their personal phone. If possible, to limit work related items to another device that is secure solely for work.

5. **HR Department:**

   - Within HR, they can overview and have communications with the employees to see if they are following best practices. As well as set the best practices for countering these habits and setting up posters around the office to remind employees of the risks.

   Supervisor:

- Each supervisor of each department should approve of any major changes within the database before the employee submits it so that they can check whether a file has been changed. Set up alerts if it seems like the employee may be trying to access a file that they may not have access to, that maybe something is wrong.

IT Department:

- Within the IT department, they can monitor and distribute company devices so that they can control what comes in through the phone. The department may setup alerts and countermeasures in the case that information is altered without the approval of the supervisor or manager.

Product manager:

- As the product manager oversees the process during a product development, they may be targeted for email phishing, they should be taught the risks of putting their personal email on the same device as their work email. They can inform those below them of the dangers and aid in encouraging best practices.

SOC manager:

- As the SOC manager, they employ SOC analysts, those analysts have the job in the event that there is malware that entered the system due to an employee, they can reinforce the security around certain directories, files, departments.

6. For the training, I believe that it should be in-person, for the reason being that when it is in-person, I believe that people would be a lot more focused on it as well as having a small quiz at the end to make sure the employees remember as well as for the frequency of it, I believe that every 9 months would be sufficient.

7. During the training, the topics covered will be preventative methods, unattended devices, Public Wi-fi and the possible hacker, email phishing scams.

Unattended devices:

- For the employees that do work-related activities on their personal devices, sometimes they may lose or forget where they put their devices, other times they may be working on their computers in public and are so focused that they may be distracted and go buy food or go to the bathroom and think that it is safe to leave their devices unattended, anyone can come up and take the phone or put malware on the device without them even knowing.

Public Wi-Fi and hackers:

- When using personal devices in public, most places have public Wi-fi nowadays, however it is not secure and because it can be accessed by anyone, the probability of having your information stolen is very high. With public Wi-Fi, hackers can use spoofers to emulate a hotspot and when you log into the company database or the company email, they can log the username and password and use that to access the company and steal data.

Email phishing scams:

- For the reason being that half the employees in the company use their personal devices for emails, some may encounter junk and phishing emails on their other email accounts, some of these emails in their personal accounts may contain malware, or similar to a three-question quiz phishing scheme to win a prize. These emails may contain a keylogger software that may tell the hacker the username or password of any company related material.

Preventative methods:

- While half the employees in the company use their personal devices for work related items, it is best to teach them about the dangers of email phishing and the examples of different schemes and scam emails that they could come across on their personal devices. For the reason being that the employees use their personal devices for work emails, some may think that it is not a problem, however assuming that they have their work email on their device, it is most likely that they also have their personal email as well, and some of those emails may have been used to sign up for different websites and those websites may have limited security and have been hacked.

- Another is reused username and passwords; most people nowadays use virtually the same username and passwords due to comfortability and less memory of constantly trying to remember what username and passwords were used for what site.

8. After the training, I believe that a small quiz to review the best practices as well as maybe some posters around the office to remind employees of the risks of doing work-related activities on their personal devices. As well as, potentially setting up a cyber security division that would hire Pen Testers to possibly test some of the employees with emails that may contain minimal malware that steals information specific to their job.