**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.**

There are many security risks of allowing employees to access work information on personal devices that open the organization up to potential attacks. Then is especially true when there isn’t sufficient training or there’s a lack of cybersecurity education.

One potential attack is that the device could be stolen. Since the organization isn’t providing the device, it’s harder to enforce security requirements like encryption tools or requiring security locks, allowing a thief to have easier access to work information.

A second potential attack is malware since their device will be more vulnerable due to a few different reasons. The first is that employees are free to download whatever they want on their device without the help of an organization’s IT meaning there’s no oversight. The next reason is that there’s no guarantee that the device has any security mitigations such as antivirus scanners or having all their software being updated.

The third potential attack that could be carried out is phishing. While this is already a threat to devices provided by organizations it’s even worse for personal devices. There will be less web filtering and the employee won’t have access to an organization’s anti-phishing software.

1. **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.**

If employees are going to check their work email and communicate through Slack on personal devices, the preferred behavior would be to use two-factor-authentication on Slack and their email login.

1. **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.**

To accurately measure for Slack, I would conduct a survey.

For email, if using Office 365, in the backend you can see which users are using two-factor and can be exported to CSV using PowerShell.

1. **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.**

The goal is to have 100% of the employees having two-factor authentication enabled for Slack and email.

**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.**

**Slack Workspace Owner:** This may be the simplest, but also the most important role in this whole process. The owner of the Slack workspace will be the one to enable two-factor forcing all users to enable it.

**IT Department:** The IT department will oversee rolling two-factor authentication out for work email accounts. They also will be in charge of measuring the number of users that have enabled it.

**CEO:** The CEO will need to be involved by accepting the proposal of adding two-factor authentication. They will also be responsible for helping ensure the seriousness of getting this done.

**Communications Department:** The Communications department’s role would be to create emails or other forms of communications like posters, to help advertise what is being rolled out to the employees and when the deadline or switch is happening. This would be a crucial role because not only will it be informing everyone of what is going on, but it also be a good opportunity to educate everyone on why we would be rolling this out.

**Training Department:** Where I work, we have a training department that handles creating guides or video tutorials on how to do certain tasks. Their role will be pivotal in the early phases to help guide users on how to set up two-factor themselves before it’s switched over for everyone at once.

**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?**

With one of the weakest links in security being employees themselves, training and cybersecurity education is a crucial part of any organization in battling potential threats. My plan to combat this is to have two trainings a month covering one topic, with one being in-person and another online where it will be recorded in case there are those that miss it. In addition to this, I will also hold workshops to help employees set up two-factor authentication for their work email and Slack to achieve my goal of having 100% of the users having two-factor.

While there are many topics that could be covered, I think doing too much at once always has a risk of overwhelming the audience with information. With that in mind, I would narrow each training down to the following topics that I believe will benefit the organization the most.

* Phishing/Vishing
  + With phishing and vishing being two of the most prevalent security risks for everyone, this would explain what they are, how to spot it, and what to do when you spot it. This topic is one that really needs to be stressed because of how common and easy it is to be phished and vished. Learning basic tips on how to spot them and to learn to ask IT when unsure about an email would be a monumental change for the organization.
* Keeping Your Operating System Up to Date
  + With malware being a major security risk while bringing in your own personal device, this would cover how to keep your computer’s operating system up to date. While ideally it would be better to have all software kept up to date, I think isolating it just to keeping employees’ operating systems up to date is a big step in the right direction for the organization while also being a simpler task to tackle and explain. By just patching routinely, this will help with security definitions for malware, patch vulnerabilities, and even help with device performance.
* Encryption and Why You Should Use It
  + With laptops and mobile devices being so prevalent in the workplace, this would help combat the possibility of losing their device or having it stolen. This topic would cover what encryption is, how to do it, and why one would want to do it. This is an important topic because encrypting one’s device is simple and a very effective tool protecting not just work data, but personal data as well.

As these trainings go on, my plan is to also push two-factor authentication for work email and Slack. The main reason I will be pushing this is because you can explain to employees how to do something all you want, but you can’t guarantee they will adhere to it. With two-factor authentication, it can be forced making it very effective.

The way I will go about this is to have a set, and well communicated, deadline to switch it on for the Slack workspace and their work email. With Slack, all it takes is the workspace owner to set it on for everyone to have to set it up and for work email, it should be able to be done in the backend in the same vein (in my experience). However, just doing this all at once may overwhelm IT with issues or employees needing help. Therefore, I would set the deadline 6 months away, but have workshops every 3 weeks leading up to then where employees can come in and have help setting it up beforehand to help alleviate the workload.

After the training and workshops are done, I have a few different ways to measure their effectiveness. For phishing and vishing, a company can be hired to attempt to do them and measure it for IT. For encryption and updating, there really is no way to know besides doing a survey and measuring it that way. For two-factor authentication, this would be the easiest to monitor because it can be looked at in the backend.

**Bonus: Other Solutions**

* **Indicate at least two other potential solutions. For each one, indicate the following:**
  + **What type of control is it? Administrative, technical, or physical?**
  + **What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?**
  + **What is one advantage of each solution?**
  + **What is one disadvantage of each solution?**
* **Require a VPN**
  + Technical
  + Preventive. The goal of this is to help encrypt and verify tunneling methods to enclose data transfers.
  + Pro: It will force people into an encryption tunnel.
  + Con: It will slow internet speeds down.
* **Strong Password Requirement**
  + Administrative
  + Preventive. The goal of this solution is to make the employees create a strong password so that it is harder to crack.
  + Pro: A strong password is harder to figure out.
  + Con: Stronger passwords can be harder to remember and cause employees to write them down in obvious places.