Step 1: Measure and Set Goals:

1. Potential security risks of allowing employees to access work information on their devices:
    - Data Theft/Leakage
    - Legal Problems
    - Lost or Stolen Devices
    - Poor Mobile Management
    - Sketchy Apps

    Three Potential Attacks:
    - Malware Infiltration
    - Phishing
    - Man In the Middle/Router Spoofing

2. The preferred employee behavior would be cautious for spam emails, won't download apps for personal use, and is always connected to the VPN when accessing work files.

3. To measure the behavior above, sending artificial emails with spam-like attachments to the entire organization would be a good method to determine which employees are more likely to download. Another method would be monitoring which users attempt to access work files outside the virtual private network.

4. The goal for the organization is to have remote users rely solely on the VPN, and to have less than 4% of employees downloading email attachments from untrusted sources.

Step 2: Involving the Right People

1. Executive Management Team's (CEO, CIO, CISO) role is to discuss with the Security team about their plan of action for a secured VPN and the results from the artificial emails. The Executive team then implements a budget that's deemed profitable for the business.

2. The Security Operations' role is to assess all potential risks and implement an artificial email strategy for pen testing. They will create a training plan to educate all employees and departments. They will also secure the organizations data by restricting work information to only be accessible when connected to the VPN.

3. The Director of HR's role is to determine training dates and time frames for each department. They will also relay the importance of avoiding suspicious emails and VPN usage to their team.

4. The Communications Team will determine the most beneficial approach to educate the entire organization. They will discuss the effectiveness of applied training, and possibly implement incentive strategies.

5. The Marketing Team's role is to create quarterly reminders about training schedules companywide via email and text. They will also understand the importance of VPN usage and suspicious activity as they often communicate with outside sources.

Step 3: Training Plan

To execute the preferred employee behavior, on site training will take place quarterly in person, followed by an assessment. The assessment will be thorough to confirm employee understanding. With the help from the Communications and Marketing team, there will be effective videos and demonstrations of potential security risks and attacks for employees to be cautious of. The training will cover how spam emails can lead to Phishing attacks, as well as how downloading attachments from untrusted sources can lead to Malware Infiltration. Trainers will stress the importance of email usage and downloads from unfamiliar origins to prevent these potential attacks. Also, we will cover what the VPN is and why we use it. Training materials will demonstrate the possibilities and risks of a Man in the Middle attack. Making sure employees understand that accessing work files outside the VPN is prohibited. Trainees and supervisors will be very clear on VPN usage and should implement incentives for proactive behaviors. Along with the assessments, the security team will measure effectiveness through testing with artificial emails and attachments, determining how many employees interact and download unfamiliar files. We will also be able to monitor which devices and logins attempt to access work files outside of the VPN.

Bonus: Other Solutions

Another possible solution would be for the company to purchase an Anti-Virus software for the entire company to download on personal devices. This solution would be a technical control as it will require a specific software for remote use. The goal from this control is preventative as it creates a technical barrier to avoid potential future hacks. The advantage of an Anti-Virus is the company's proactive measures to secure its data, making it one step harder for an attack to be successful. However, the disadvantage is the cost of the software and subscription, the executive team may decline if it's not within budget.

Additionally, requiring a two-factor authentication login for remote users would be an ideal solution. This solution would fall into both administrative and technical controls. It requires employees to create an additional verification and the security team must implement the restricted login. This control is considered Deterrent, as it discourages unauthorized users to attempt a login. The advantage of the two-step authentication login promotes the secured access for authorized employees. One disadvantage could be an employee no longer having access to their secondary source (phone, email, app, etc.) and having to contact IT.