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.

   Answer:

   The potential risks of allowing employees to access work information on their devices are having data leakage, possible hacking, vulnerability to malware, the device is lost or stolen, malicious apps, the device can be rooting/jailbreaking, and also the untrustworthy employee.

   The device can be jailbroken after the device is lost or stolen, and all data can be accessed. Also, employees can download any malicious apps or even malware via emails. An employee sharing the company data with others or even competitors.

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.

   Answer:

   - **For the potential risks listed above, the preferred Behaviour is as follows: - Lost or stolen devices correction: Use encrypted devices. Ideally, the company should work on policies and the work environment to such an extent that the employee does not have to work from home. However, this may not be achievable in every situation and some professions necessitate the employees to work from home. The company can then have the policy to issue encrypted secure laptops/computers issued to the employees. Alternatively, the company can have the policy to encrypt an employee's personal laptop or device. The employee can be given a choice whether to use the company issued encrypted laptop or have their own laptop/mobile encrypted**

   - **Increased protection from malware: Installing anti-malware on their personal devices. The company can offer employees to install latest anti-malware software on their personal devices as part of the benefits package for working in the company**

   - **Increasing awareness: The corrective employee behavior would be to be cognizant of the ways they are vulnerable to identity theft by sharing real-world data such as the research conducted by the US Treasury Department**

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.

Answer:

- **I will utilize the Information security culture framework (ISCF) as originally proposed by Alhogail and colleagues which is composed of five dimensions including strategy, Technology, Organization, People, and Environment (STOPE), and will target the 4 main factors of human factor diamond which include: Preparedness, Responsibility, Management, Society and Regulations. My assessment instrument will be a questionnaire to collect data from employees regarding their beliefs, perceptions, knowledge, and practice towards information security. The survey will target two specific components**

- **The demographic information of the employee's e-g, age group, education, background, Job title, information technology use, and experience.**

- **Obtaining assessment regarding the information security behavior, perceptions, and knowledge about IT. Prior studies have demonstrated that the employee's knowledge about IT positively correlates with the**

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.

Answer:

- **The goal will depend on the results of the survey. A robust statistical analysis will be performed to determine the reliability and validity of the assessment instrument. The reliability will be assessed by analyzing the Cronbach alpha as a measure of internal consistency, with a minimum set to at least above 0.6 for acceptability. The validity will be measured using the goodness of fit. (0.9 as acceptable and 0.95+ as good fit)**

- **Once the assessment instrument has been determined to have acceptable reliability and validity. The goal would be to reduce the number of employees using personal devices to initially achieve a 50% reduction in the existing practice and eventually to a rate of less than 5% overall. There will also be an 80% or above pass rate requirement for the employees in the information security quizzes.**

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.

  Answer:
  Five People to involve

  - **Chief Executive Officer** of the company Role:
    - **Providing information regarding the existing state of the company. -Bringing all involved parties to the table including the COO, Chief of staff, Chief financial officer -Providing resources for executing the proposed plan e-g buying anti-malware software, new encrypted laptops for the employees**

  - **Chief Information Officer** of the Company Role:
    - **Implementing the technological aspects of the cybersecurity proposed plan, e-g installing malware, upgrading OS, encrypting employee's phones or laptops**

    - **Conducting surveys for the assessment of security culture, conducting quality control studies for repeat assessment of whether the company is achieving the set milestones and goals for the implementation of the security policy**

  - **Board of Directors**
    - **Incorporating the proposed security culture policies into the company policies and strategy in combating insecure employee practices**

  - **Chief Operating officer**
    - **Communicating the policy changes to the employees**
    - **Training the employees against the security threats by creating awareness courses- such as awareness regarding the mechanisms of identity theft**

  - **Chief of Staff**
    - **Hiring new personnel as needed for implementing the new security culture- such as new IT specialists. Appointing a chief information security officer (CISO)**

  - **Chief Financial Officer**
    - **Determining the financial feasibility in instituting the new company policies. For example, determining whether the company can afford to issue new encrypted phones or laptops to the employees.**

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)

  Answer:

  - **Initially, a survey will be conducted to assess the knowledge base of the existing employees. The results of the survey will be analyzed for reliability and validity. The format of the training will be composed of both in-person interactive sessions and online learning. The Company's leadership will be directly involved. The in-person sessions will include participation by the company's leadership to emphasized the security policies. The more specific topic will be targeted with remote online learning. At the current time, due to COVID, even the initial in-person session will be conducted in the form of live Zoom sessions Every new employee who joins the institution will have to complete the courses/live sessions as a mandatory requirement before starting with duties. Some training courses will be broad-based creating general awareness, others will be targeted by specific areas of vulnerability as outlined below. The general courses will be repeated every year. Specific topic courses will be available every 6 months with updated data.**

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

  Answer:

  - **The live zoom session will be a welcome orientation as well as the 1st mandatory training session regarding the cybersecurity policies of the company. The companies leadership will participate in the live session including the Chief information security officer, chief information officer, chief operations manager, and if feasible the company's CEO. This session will emphasize the company's policies in the cybersecurity culture. The topics will include:**

    - **State of the company: The designated officials will share statistics regarding the companies employees and the risk of cybersecurity threats. Any relevant data regarding the past incidents will also be shared.**

    - **Emphasizing the companies culture that cybersecurity is "everyone's responsibility"**

    - **Information regarding who to contact and report if an employee suspects a data breach, receives a suspicious email, etc.**

    - **Introduction to reward programs for compliance with cybersecurity policies or reporting incidents.**

    - **In addition to the in-person/live sessions, the employees will also take an additional course to create awareness on specific categories of cybersecurity insults**
    - **Phishing scams: Emphasizing not to click unfamiliar links in the external email. Emphasizing the company's administration will never ask the employee's to directly provide password etc**
    - **Information regarding the common types of hacking tricks such as malware, ransomware, formjacking, code injection, the brut force with examples of data breaches with other companies**
    - **Online training with the installation of anti-malware software on the employee's personal devices**
    - **Certain employees may be more vulnerable, especially if they need to routinely perform work-related activities from home. For example, residents who need to obtain access to electronic medical records of patients from home. Such employees may be better off using the company's issued devices with secure encryption at home. An alternative will be encrypting the employee's personal devices (if they are willing) for remote work.**
    - **The employees will be educated regarding the 2-factor identification to prevent identity theft. The online training will inform the employees with examples regarding the mechanisms of identity theft along with videos of how to set this up at the start of their employment**
    - **The employees will be educated about the company's policies of not using external USB, how to obtain encrypted USBs for work that may be issued by the company if needed.**
    - **The training will also include information regarding the alternatives to using personal devices at work such as remote desktop connection, working on the server that is protected against a firewall rather than a personal computer for any data-related activity. Using encrypted USBs issued by the company rather than the external USBs.**
    - **Adopting common sense measures including logging out before leaving a computer, Limiting access to confidential information on a need-to-know basis. Not disclosing protected information on social media. Reporting incidents of potential data breaches e-g lost or stolen laptop**
- After you've run your training, how will you measure its effectiveness?

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

Answer:

- **The effectiveness of the cybersecurity culture framework will be assessed by evaluating the three dimensions**
    - **Measuring awareness:**
        - **This will include results of the quizzes, participation level in the training programs. Testing employee's knowledge by conducting surveys and comparing results for before and after training using the same survey. Another method is by assessing employee feedback**
    - **Measuring behavior:**
        - **This can be achieved by simulating phishing attacks and measuring how many employees fell into the trap.**
    - **Measuring culture:**
        - **Performing qualitative analysis to determine the culture of the institution by reviewing patient's feedback. Identifying recurrent topics and obtaining a sense of how seriously do employees take cybersecurity threats. Determine whether these perceptions have changed with the implementation of new policies. I would conduct these qualitative cybersecurity culture analyses on a yearly basis.**

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?
    - 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?