**Step 1: Measure and set goals:**

1. Three potential attacks that can be carried out from allowing employees to access work information on their personal devices are downloading malicious apps, data leakage (stolen device/phone theft), public exposure (unsecured network can cause data theft), and phishing emails.
2. The preferred employee behavior is:

Downloading malicious apps:   
Download only trusted apps and use only well respected websites  
  
Phishing emails:  
Click links and download attachments from only trusted senders  
  
Data leakage/ phone theft:  
Enable location on at all times and tracking.   
Enable phone to automatically erase after 10 attempts of login.   
Require 6 character pw, fingerprint recognition, and face recognition

Public exposure:  
Log into VPN when in public. Opt for personal hotspot when secure network isn't available

1. Methods that are used to measure how often employees are currently not behaving accordion to the preferred behavior are:  
     
   Phishing emails:  
   Conduct quarterly phishing test to gather information

Data leakage/phone theft:  
Conduct a survey to see if location is enabled.  
Take screenshots and send email for confirmation

Public exposure:  
Conduct a survey to see how often people use VPN when in public locations.

1. The goal that I would like the organization to reach regarding this behavior are:  
     
   Data leakage (phone theft):  
   100% of employees have their phones enabled 90% of the time.

Public exposure, unsecured network can cause data theft:  
Use of VPN in public places 75% of the time.  
  
Phishing emails:   
Under 5% of downloading suspicious emails

#### **Step 2: Involve the Right People**

The people who needs to be involved are:

* 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) Human Resources- The roles and responsibilities of HR is to create and deliver training materials for all employees/staff. HR should create documentation like policies for staff/current and new hires to sign. Another important role of HR is to make sure employees understand the importance of rules and policies of the company. HR should also report to the CEO for updates regarding any issue or problems.

2)Management control- Management control is like an administrative control, they have access to confidential files, have more authority. Their role is to help regulate staff regarding updated policies and procedures. Management’s job is to also lead a team by example. Be supportive and help encourage. Management will also have to report anything unusual to HR.   
  
3) Technical control- IT is responsible for conducting surveys and phishing tests. In addition to gathering information and creating reports to see if procedures are being followed and met. Their job is to also help mitigate risk and keep the company safe, making sure everything is flowing correctly and smoothly. In other words, help manage and report to other departments.  
  
4) Employees- Employees are responsible for obeying new policies and procedures. It is also their job to attend training and stay updated with new policies. Employees are to address any issues or concerns to upper management.

5) CEO- The CEO is to stay up to date with all problems about the company. The Ceo is responsible to review, approve, and fund all aspects of the business. Mainly Ceo’s goal to maintain and overlook the business.

#### 

#### **Step 3: Training Agenda**

How frequent will training occur? How will training take place?

* For new hires: training will take place during orientation and in person.
* All employees: training is quarterly for the first year and every six months (may be in person or online).
* Training must be completed within one month

Training topics:

1. Phishing emails

* Click links and download attachments from only trusted senders

1. Data leakage (phone theft)

* Enable location on at all times
* Enable phone to automatically erase after 10 attempts
* Require 6 character pw, fingerprint recognition, and face recognition

1. Public exposure

* Use VPN when in public
* Opt for personal hotspot when secure network isn't available

Why is it important?

* To mitigate risks
* Increase knowledge
* Save company money
* Protect company

How to measure effectiveness:

* Reaction- Observe reactions during training. Are trainee’s engaged?
* Learning- Test what they learned  
  - Provide questionnaires, surveys, quizzes, and tests
* Behavior- Will employees make the same mistakes?  
  -Phishing emails:  
  Conduct quarterly phishing test to gather information

-Data leakage/phone theft:  
Conduct a survey to see if location is enabled.  
Take screenshots and send email for confirmation   
-Public exposure:  
Conduct a survey to see how often people use VPN when in public locations.

* Interviews with peers are encouraged
* Impact- Did they pass the test? Results!

Work Cited

“Measuring Training Effectiveness: A Practical Guide.” *AIHR*, 21 June 2021, [www.aihr.com/blog/measuring-training-effectiveness/](http://www.aihr.com/blog/measuring-training-effectiveness/).

“BYOD Security: What Are the Risks and How Can They Be Mitigated?” *Comparitech*, 26 Sept. 2020, www.comparitech.com/blog/information-security/byod-security-risks/.