# Week 2 Homework: Assessing Security Culture

## 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.

- **Unsecure data transfer (data to-and-from a user's device can be intercepted)**
- **Malicious Apps (downloading apps infiltrated with malicious malware code)**
- **Network breach (due to lost or stolen device)**

2. Based on the above scenario, what is the preferred employee behavior?

- **Setting up a PIN code or password on their mobile. For Apple users it will automatically activate data encryption. Android users can access their security settings to enable encryption.**
- **Do not install unapproved apps or make unauthorized customizations on your devices.**
- **In Addition to setting up PIN codes and complex passwords for all used devices it would be preferred to use additional security features which include fingerprint recognition or if applicable facial recognition technology.**

3. What methods would you use to measure how often employees are currently _not_ behaving according to the preferred behavior?

- **By implementing BYOD policy which includes a single Enterprise Mobility Management (EMM) which contains Mobile Content Management (MCM), a Mobile Application Management (MAM) system and Mobile Device Management (MDM).**

4. What is the goal that you would like the organization to reach regarding this behavior?

- **One goal is to register, track and control which personal devices are accessing company resources and data.**
- **Another goal would be to control what software is installed on the devices.**
- **Finally, and most importantly, is to manage what kind of company data is allowed to be stored or accessed on the device.**

Step 2: Involve the Right People

Now that you have a goal in mind, who needs to be involved?

- **Chief Executive Officer (CEO) of the company Role:**
    - **Providing information regarding the existing state of the company.**
    - **Bringing all involved parties to the table including the COO, CoS & CFO**
    - **Providing resources for executing the proposed plan**
- **Chief Operating officer (COO)**
    - **Communicating the policy changes to the employees**
    - **Training the employees against the security threats by creating awareness courses**
- **Chief of Staff (CoS) or Senior Manager**
    - **Hiring new personnel as needed for implementing the new security culture, such as new IT specialists.**
    - **Appointing a chief information security officer (CISO)**
    - **Communicating the security risks to the lower managers and setting up VPNs for employees**
- **Chief Financial Officer (CFO)**
    - **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.**
- **Chief Information Officer (CIO) :**
    - **Implementing the technological aspects of the cybersecurity proposed plan, e-g installing malwares, 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.**

Step 3: Training Plan

How will you train your employees on this security concern?

**Training will be run quarterly and be a mix of in person training and where industry specialists will come and hold presentations about threads and online training will be provided.**

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

**BYOD training will start with an introduction explaining what BYOD brings to the company. This leadoff to the training will hopefully sell the initiative to the employees while relating the effort to what it offers the overall business and your customers.**

**Onboarding devices into a BYOD program will be done in conjunction with BYOD training. Employees need to know exactly what software the organization is installing on their personal device(s).**

**Breaking down a typical BYOD device and showing how MDM affects the device features and security and describing MDM features and how they benefit the BYOD user.**

**Defining the responsibilities of BYOD device users**

**How to access corporate resources from BYOD devices**

**BYOD device password policies**

**BYOD device loss or theft policies**

**Corporate WiFi network security**

After you've run your training, how will you measure its effectiveness?

**After implementing the BYOD policy the Enterprise Mobility Management (EMM) will be able to give the company all user related data, since it is a new policy the employees have to stick to it and will not be allowed to use unsafe devices for work.**