#### **Step 1: Measure and Set Goals**

#### SOLUTION

1. **Potential Risk are**:

***Opportunities for Data Theft*** - the use of a mobile device to send files over an unsecured wi-fi network, such as in the airport could expose company’s information to hackers.

***Malware infiltration*** - employees downloading files containing hidden malware or viruses that compromised employee mobile devices, could be passed to the company’s network.

***Device loss or Theft*** - a device theft could pose a huge disaster to the company if the employee does not follow recommended company security protocols.

***Poor Mobile Management*** - former employees having access to the company network is a poor security setup leaving the company to the mercy of the former employee.

***Potential Legal Issues*** - security breach through an employee’s device that leads to leaks of customer’s credentials might result in a series of litigations which might damage company’s reputation.

***Shadow IT*** - this is where the information technology is handled outside the company’s IT department. Outsourcing of information technology from third parties with vulnerable networks could also expose the company’s network to malware attacks.

***Lack of Employee Training*** - inadequate training of employees on the company security policy can lead to mistakenly compromising the security of the company’s network.

**Potential Attacks are**:

***Phishing*** - a type of social engineering attack that involves an attacker deceiving a victim into opening an email, instant message, or text message often used to steal user data, including login credentials and credit card numbers.

***Advanced Persistent Threat APT*** - typically a nation state or state-sponsored group, which gains unauthorized access to a company’s network and remains undetected for an extended period.

***Malware*** - codes specifically written to gain unauthorized access to computer systems, disrupt, or damage operation.

2. **Preferred Employee Behavior.**

* Employees should always download attachments from trusted sources.
* Employees should use strong passwords.
* Employees should not use the same password and username across multiple sites.
* Employees should ensure that they do not use unsecured wi-fi networks to send files.
* Employees should separate personal devices from company’s mobile devices.

3. **Methods to measure how employees are not currently behaving according to the preferred behavior.**

* The use of Mail Campaign within a specified period of time to conduct a survey to see how often employees download email attachments from unknown senders.
* The use of Password Meter to check how strong is the employee password
* Using off-the-shelf tools to test if employee password use on one account has been used on another site. Example of such a tool is ‘Shard’ by Philip O’Keefe.
* Taking inventory of all employees devices accessing the company’s network.
* Conduct periodic audit of company’s mobile devices (Bring Your Own Device - BYOD) policy

4. **Goals to reach regarding the Employee behavior:**

* Our goals for the organization regarding all the preferred Employee behavior is to reach **0** **percent**.