Week 2 Project: Assessing Security Culture

Step 1: Measure and Set Goals

1-a)Data theft.Hackers would be able to access data and steal it from personal devices
b)Malware infiltration and loss and theft of devices.

2-With the data theft, the company can give the employee the choice of either having their personal device encrypted or using an encrypted company issued device
With the malware infiltration, installing an anti-malware on their personal device would be required.

3-I will conduct a questionnaire survey as my assessment instrument to collect data from employees regarding their beliefs, perceptions, knowledge and practice towards information security.

4-When the acceptance of the reliability and validity of the assessment has been reached,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.

Step 2: Involve the Right People.

a)Chief Financial Officer
b)Chief of Staff or Senior Manager
c)Chief Operating officer
d)Chief Information Officer of the Company Role
e)Chief Executive Officer of the company Role

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.?
-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 emphasize the security policies. More specific topics will be targeted with remote online learning. At the current time, due to COVID even the initially 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.)The topics will include:
-State of the company: The designated officials will share statistics regarding the company's employees and the risk of cybersecurity threats. Any relevant data regarding the past incidents will also be shared.
-Information regarding who to contact and report if an employee suspects a data breach, received a suspicious email etc.

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

Measuring awareness: This will include results of the quizes, 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.