**Week 2 Homework: Assessing Security Culture**

**Step 1:Measure and Set Goals**

1. Silvercorp has gathered possible threats that can happen from employees accessing SilverCorp data on personal devices go as follows, devices being stolen and an outsider has access to SilverCorp data and now has the option to sell and/or download malware.If the employee has work info on their phone and they download apps onto that phone for personal use the apps may ask for the user to share all data associated on the phone and that is a major intrusion on SilverCorp especially if the company is a competitor. Another possible threat to silverCorp is if the employee is on public wifi accessing work info and a potential hacker now has easier access gaining entry onto the employees device which is now a threat to SilverCorp data.

2.SilverCorps preferred behavior of the employees is to not access work data on their personal phones.

3.SilverCorps Incident response team will work along with the IT department and will monitor the employees success of following the new policy with Bi-weekly monitoring of the IP addresses that access any company data.

4.SilverCorps goal is to have 0% of employees using their personal phones on any of SilverCorps data.

**Step 2:Involve the Right People**

Silvercorp has gathered various management and departments to collaborate on the plan for the policy to meet expectations. Since there is risk involved to the data the CISO will be present because their responsibilities contain managing risk to an organization's data throughout its lifecycle. The CISO will be overwatching the (IR) team and IT as they monitor.

The IT department will also be involved due to their responsibility of training and the security of servers/data.They will be working alongside the IR team in monitoring the employees activity on company data and notifying HR of any mobile phone breaches.

The Incident Response team will be a big part of enabling the policy for their responsibilities containing Identifying and responding to security breaches. The IR team will be working alongside the IT department to alert the IT team of any mobile IP addresses accessing company data.

HR will also be a huge partner in collaboration with their responsibilities being responsible for internal communications, scheduling training, and tracking attendance. HR will be alerting the employees of the new behavior expected of the employees,and will be keeping on top of the employees to make sure they are doing so.

The COO will also be involved with CISO in overwatch of the IR and IT team but will also be checking in with the HR team to ensure that everyone has been notified of the policy and ensuring the CEO the policy is in effect. The COO’s responsibilities are ensuring business functions operate effectively day-to-day, monitor day-to-day operations, keeping the CEO aware of significant achievements and setbacks, and oversee people management.

**Step 3: Training Plan**

SilverCorp has decided that training will happen twice a year both in office and online through zoom meetings to accommodate the employees. SilverCorp employees will be informed of the security threats of employees using personal cell phones to access company data of any sort. The main security threat points that will be addressed in training go as follows, devices being stolen and an outsider has access to SilverCorp data and now has the option to sell and/or download malware.If the employee has work info on their phone and they download apps onto that phone for personal use the apps may ask for the user to share all data associated on the phone and that is a major intrusion on SilverCorp especially if the company is a competitor. Another possible threat to silverCorp is if the employee is on public wifi accessing work info and a potential hacker now has easier access gaining entry onto the employees device which is now a threat to SilverCorp data. The employees will be informed of these threats to ensure security knowledge is being implemented with the employees and also explaining why the new policy is being placed into effect.

The employees will also be informed of the new policy of no longer allowing employees to use personal cell phones to access SilverCorp data. The employees will also be informed of repercussions of using personal cell phones to access company data to ensure that the policy will be followed. The repercussions are set as the three strike rule, 1st strike is written warning, 2nd strike is 3 day unpaid suspension, and the 3rd strike will involve termination. The repercussions are set so high to ensure that Silvercorp can guarantee that no employees are accessing company data on personal cell phones.

Silvercorp will measure the effectiveness of this new policy by checking in with the IR and IT teams and getting the percentage results bi-weekly of employees using personal cell phones for work purposes and having a third party consultant to do a threat/risk analysis on the company yearly.

SilverCorp Management.