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

**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.**

The potential security risks that SilverCorp may encounter are that employees are opening phishing emails. Employees could possibly have their devices stolen or may lose their devices. Another risk is the download of malicious applications. If an employee clicks on a phishing email then login information can easily be stolen by a hacker. Downloading malicious applications through personal devices means that malware can easily be deployed by a hacker. If the employee is working on their personal device and they leave their computer open or leave their device then malicious software can be downloaded onto their server through a USB.

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

Employees should only use their own devices on private networks when accessing work email or when doing work related activities. Employees should use their work email for work related communication and should not download or click on links from untrusted senders.

**3. What methods would you use to measure how often employees are currently not behaving according to the preferred behavior?**

Employees can complete a self survey that asks them if they feel that they are behaving according to the preferred behavior. This will keep track of how many employees feel they are being safe. Another survey that keeps track of completed training. Another method would be to keep track of the number employees and their names who fail threat simulations. There should also be a survey asking employees if they have their own devices, whether it is a mobile device or personal computer so that the company knows the number of employees posing potential risks.

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

The ultimate goal would be that 0% of employees are not downloading/ clicking onto untrusted sites/links. However humans are not perfect so the end goal should be less than 5% of employees are outside of preferred behavior.

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

* The chief financial officer would be involved to assess how much money is available in order to implement training, it could be that SilverCorp only has funds for online training instead of in person training. The team will make sure that SilverCorp is using their finances to reach set goals.
* The management team and human resource team will work together to ensure that every employee in each department of SilverCorp is receiving training. They will also implement training requirements and be able to discipline employees who fail to meet basic training requirements.
* The chief information officer will develop systems to support SilverCorp. Their main goal is to get IT systems/equipment that best benefits SilverCorp from the needs of the business, user needs and information/communication needs.
* The chief information security officer will also be involved as their primary goal is to manage the risks that SilverCorp may encounter and weigh in on what would be their most vulnerable asset.
* The chief executive officer will be responsible for ultimately making sure that the goals are being reached based on reports of trajectory for the other departments.

**#### Step 3: Training Plan**

Security educational training will be required during the first week of a new hire, and should be conducted once every year for all employees at SilverCrop, the company would benefit from doing mass training during a 30-60 day period every year, telling the employees they have till March 31 to complete training. The training for security training will be conducted online through video training and interactive tests.

The main topics covered during the training videos will be how to determine if an email is a phishing attack. The main training points would be that the emails will try to mimic a trusted sender and ask the employee to download or click on a link. The employee will be trained to confirm that the sender has a valid email address, to pay attention to misspelling of words, and how to spot fraudulent URLs. This training will also inform the employee on what to do if a phishing email is found. After providing the employee with the education then they will be tested, the test will consist of a simulation email, it could be totally trusted or not, the employee will show understanding by interacting with spotting an attack. Once successfully completing the training then the employee will have (or continue to have) access to their work provided email. Another training video will show the importance of using a verified private network when accessing their work email or when doing their work through their personal devices, this part will show the dangers of unsecured networks and provide statistics to inform the employee about cybercrime attacks, informing employees about the dangers of downloading untrusted applications and informing the employee about the dangers of clicking on advertisements that could potentially have malware. Again they would be tested and only be able to access company information once completion of training is done. Since this needs to occur yearly then HR will be responsible for reminding employees and management will enforce completion.

In order to measure how effective training was the employee will pass their interactive test after watching training videos, employees will pass if they score an 80% or higher, if they fail to meet criteria they will rewatch the section and be tested again. The test will allow the employee multiple attempts until their deadline. Throughout the year the employees will have phishing simulations. Every employee will have a couple emails sent quarterly and those who click on the untrusted links of this email will be reported, they will receive an email stating they failed to identify that the email was a phishing attack. Multiple offenders will be required to retrain. Once there is an overall satisfaction then the emails will be sent out less frequently. For those employees who report the phishing emails can be rewarded with an email that provides positive reinforcement. At the end of the year those employees who constantly reported these simulation phishing attacks then can be compensated therefore encouraging a positive security culture at SilverCorp.

**#### Bonus: Other Solutions**

Two other potential solutions are requiring employees to use 2 factor authentication when logging into their work email or when logging through their personal devices. This is considered a technical control which will prevent another user from accessing company information. This is an advantage because a two factor authentication can be through a mobile application making it easier for the employee to authenticate. A disadvantage could be, if this is an app that requires internet connection or the employee has limited storage space then the employee will not be able to access their email or do work activities on their own devices.

Another solution is to require employees to log on through a remote desktop to access information from SilverCorp including logging into your email. This is another technical solution, this remote desktop will allow the employee to work remotely and access company information through encrypted channels on servers. A RDP would be a preventive and deterrent control, because only employees that require access outside of work could be allowed to have remote access. An advantage is that the number of employees with remote access can be smaller, a disadvantage would be that the remote desktop software requires too much storage space from the employees personal device. Both solutions are detective controls as it can help identify and alert attempts to access resources from the company.