#### **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.**
   * Data theft
   * Malware infiltration
   * Device Loss or Theft
2. **Based on the above scenario, what is the preferred employee behavior?**
   * Users would only send information from their device while connected to a private network and/or VPN
   * Users would only download files or information through trusted company sources
   * Users would follow very strict security protocols to ensure that their device is always secure and hidden away from potential thievery
3. **What methods would you use to measure how often employees are currently *not* behaving according to the preferred behavior?**
   * Run yearly training modules along with surveys to ensure that the employees are conducting business with their devices properly
   * Send out fake company-wide phishing emails to see how many employees would click on the “malicious link”
   * Have a logon tracker within the users VPN to ensure that they are logging into it before conducting business
4. **What is the goal that you would like the organization to reach regarding this behavior?**
   * Have 100% on-time completion of the annual training module
   * Have at least 25% of employees complete a survey
   * Have less than 10% of employees click on the fake phishing email links

#### 

#### 

#### 

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

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

1. Legal/HR
   * Legal and/or HR will need to be involved to ensure that the training modules are conducted in a manner that is appropriate for employees. They will also need to make sure that what we are teaching is correct in terms of legality.
2. Tech Infrastructure (IT)
   * IT’s job will be to deploy devices with proper security features and protocols as well as making sure that these devices work properly. IT will also focus on repairing these devices if they malfunction or to reinstall faulty security software.
3. Finance
   * The Finance department creates the budget for the plan as well as approves the cost of training expenses and devices for each employee.
4. Engineering
   * The Engineering team will be in charge of designing and developing training plans and security software. They will need to work closely with HR and Legal when developing the training software to make sure it’s compliant with workplace fairness.
5. Employees
   * The employees will help with testing and completing their annual training modules to make sure that they are clear and coherent. They will also be urged to complete surveys in order to give feedback on how the training and their workplace environment is conducted.

#### **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? (i.e. in-person, online, a combination of both)
* What topics will you cover in your training and why? (This should be the bulk of the deliverable.)
* After you’ve run your training, how will you measure its effectiveness?

This portion will require additional outside research on the topic so that you can layout a clear and thorough training agenda.

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

Compliance and security training will be given to employees every year starting January 1st or whenever the employee is on-boarded. This training will be in the form of various different online training modules, such as data security, phishing protection tactics, on-site what to-dos, and what not-dos, etc. Targeting training modules will also be provided if an employee is seemingly doing something that they are not meant to be doing. For example, if an employee receives a fake phishing email that we send out and they click on it, they will automatically be assigned the phishing protection tactics training module and will be urged to complete the training by the end of the week.

Arguably the most important training plan that we will be pushing to all of our employees will be Data Security. After an employee takes this Data Security training module, they should be able to easily identify several, if not all data types in practice, such as PII (personally identifiable information), financial information, restricted/sensitive information, confidential information, etc. The purpose of pushing this training module specifically is to ensure that our employees can properly protect our company’s sensitive data and arguably more important, our customers data. Of course, however, we will also be pushing several other training modules in order to protect our employees from possibly corrupting our company’s system with malware, which could potentially damage company property or leak customer’s confidential data to the public. These training modules will also contain guides and templates to employees on how to properly conduct themselves in the workplace in hopes to be proactive in the riddance/reduction of workplace sexual harassment cases, possible tailgating into the building, and disaster plans for the building. The disaster plans would be instructions on what to do in case of various different kinds of scenarios, such as a building fire, an active shooter in the area or in the building, and natural disasters.

#### After running the training modules we will set up systems to track how well the training modules taught our employees. We can track how well the phishing protection tactics training worked by setting up a system in which we can push false phishing emails to our employees and tracking the number of times that the link inside that email is clicked. We would be able to track how well the tailgating training worked by installing a camera near the doors in the building and have a SOC analyst record the number of times someone is let through a door without badging. Tracking data security would be as easy as setting up a survey after someone accesses confidential/sensitive data and ask why they were accessing that specific set of data. Once reviewed, if the reviewer deems that their reasoning was not good enough to be accessing that data, they will be given the Data Security training again and be forced to complete it by the end of the week in order to get their permissions reinstated. If said employee fails to complete their training they will be temporarily suspended until the training is complete.

#### **Step 4: Other Solutions**

Training alone often isn't the entire solution to a security concern.

* Indicate at least two other potential solutions. For each one, indicate the following:

1. **Requiring any access to customer/confidential/sensitive data to have specific approval from either the data owner or from someone of equal clearance level**
2. **Requiring one-by-one badging into the main entrance of the building which is monitored by on-site security**
   * What type of control is it? Administrative, technical, or physical?
3. **Administrative control**
4. **Physical control**
   * What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?
5. **Preventative**
6. **Preventative**
   * What is one advantage of each solution?
7. **The main advantage of this is that it would make the data that needs the approval to access extremely secure since in order for anybody to see it they need to go through an entire approval process.**
8. **This solution could be advantageous because it would make the likelihood of tailgating into the building almost non-existent since everything would be closely inspected by a physical security guard**
   * What is one disadvantage of each solution?
9. **The primary disadvantage to this is that the access of this data would take a significant amount of time which would slow down production by a huge margin**
10. **A huge disadvantage of this solution is that not only would it take getting into the building take a lot of time, but it would also be financially inadequate to hire 24/7 security guards just to watch people come in and out of the building and inspect their badging activity**