#### **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.
   * The ultimate issue from a cyber attack would be
     1. information theft
     2. Business disruption
     3. Financial loss
     4. Impact on business reputation
   * This could happen in many ways, but here is a brief list:
     1. Theft of the device leading to confidential information breach, access to company network and infect other machines connected to the network and use them for botnet. Could use the company and personal resources like compute power for crypto mining etc.
     2. Unmanaged devices, especially personal devices with no active monitoring could potentially be a backdoor for the hackers as not all users would be able to keep the device secured and updated.
     3. Malware attack to the corporate network leading to either the loss to the information theft or business disruption or both.
     4. Malicious applications exploiting the device and gathering the business information.
     5. Insecure communication to the corporate network could be an invitation to all sorts of threats mentioned above along with being an easy target for the bad actors.
2. Based on the above scenario, what is the preferred employee behavior?  
   * For example, if employees were downloading suspicious email attachments, the preferred behavior would be that employees only download attachments from trusted sources.
   * Employees need to make sure that the device don’t have any non-genuine software installed
   * Employees also need to make sure that they don’t connect to the unsecure networks even for personal use as this could lead into being hacked and hence could be a source for the company security vulnerability.
   * Employees need to make sure the threat protection software is uptodate and Scan any files or attachments downloaded before opening them.
   * Employees should know, understand and follow the company BYOD policy.
3. What methods would you use to measure how often employees are currently *not* behaving according to the preferred behavior?  
   * For example, conduct a survey to see how often people download email attachments from unknown senders.
   * Conduct a survey once in a quarter or a month on:
     1. If they are checking the system & AV updates.
     2. If they are scanning an external HDD before opening the files on it.
     3. If they are scanning files downloaded from the internet before opening them.
     4. If they are following the file storage policies to secure the critical information.
   * Other matrix could be keeping and eye on the number of incidents on the network
   * Also engaging employees in open discussions about cyber security could give a measure on how well versed they are with the policies and could improve the overall company security stance.
   * A quick poll during team meetings could also help.
   * A simulated threat could also provide a great insight into the security posture of the company/organisation.
4. What is the goal that you would like the organization to reach regarding this behavior?  
   * For example, to have less than 5% of employees downloading suspicious email attachments.
   * I think the goal should be 0% with interim targets leading to it. This is only possible with regular professional development sessions to reiterate the policies and keeping them updated with the changing trends.
   * In addition to this, organisations should first and foremost have a dedicated cyber security team with the outlook to lead the company into the future safely and securely.

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

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

* Indicate at least five employees or departments that need to be involved. For each person or department, indicate in 2-3 sentences what their role and responsibilities will be.
* Here is the typical cyber security teams structure
  + **Security manager** - A line manager managing a team of security professionals. The objective of this role is to formulate, deploy and handle the controls that are finalised in conjunction with CISO & CSO. This role will assign jobs and mentor his team in implementing the security controls along with resolving any conflicts while doing so.
  + **Compliance Officer** - A professional to lead the organization with a compliance perspective. The main objective is to comply with the laws and regulations around the information handling and process execution. This role provides the company all the necessary handles to deploy controls related to the laws and regulations that are applicable to the organization/site.
  + **Privacy Officer** - A PO or CPO helps in handling the sensitive information, personal or corporate ensuring protection from disclosure and proper handling of the information. PO & CPO would be responsible to deploy controls to handle sensitive information including but not limited to, the employee & customer sensitive information, medical information, financial information. Their primary objective is to make sure the information is handled properly but the protection itself doesn’t fall into the scope of their role.
  + **Chief Information Security Officer** - CISO usually deals with Information security including physical protection. Of the many responsibilities, CISO would be responsible for the overall information security policy, risk management and treatment, security architecture and operations and security incident response.
  + **Chief Security Officer** - CSO usually deals with security related to both technology and non-technology. Of the many responsibilities, CSO would be responsible for the overall security policy, risk management and treatment, security architecture and operations and security incident response.

#### **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?

Training is a critical part of any organisation and as the online training is more cost & time effective than the in-person training, I think online training should be done more often than the in-person training.

In my opinion, Online training should be carried out once in a quarter excluding the quarter when the in-person training takes place, whereas in-person training should take place at least annually. I am sure it is not possible to tailor the in-person training to suit everyone’s role, but should be tailored to suit most of the cohort like common aspects that imply their job roles.

Topics that could be covered during training must include the most common issues like,

1. Password security and multi factor authentication,
2. Identifying phishing mails,
3. Identifying fake letter in the mail asking to scan a QR code,
4. Incase of unmanaged devices, updating OS and AV.
5. Physical security of the device
6. Threats of connecting to unsecured WiFi networks.
7. Scanning files downloaded from internet
8. Scanning their USB/external HDDs before opening.

Quick measure if the training is effective is to run a quick survey of their understanding in those topics. Other than the survey is to instrument a process to gather some matrix using simulated threats. This could provide a great insight into the company's security posture.

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

#### **Bonus: 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:  
  + What type of control is it? Administrative, technical, or physical?
  + What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?
  + What is one advantage of each solution?
  + What is one disadvantage of each solution?

1. Firewall/DMZ/VPN - This is a technical control. The goal is to prevent and streamline external access based on the user permission levels. The main advantage is this will stop most of the unauthorized external access, but can’t help with the internal attacks.
2. Key Cards/biometric scanners - This is a physical control. The goal is to prevent unauthorised physical access to the premises and depending on the implementation, it could streamline physical security to buildings/wings/rooms based on the requirements. The advantage is that it ensures only authorised personnel are in the premises and no physical access to the company resources to the unauthorised. Disadvantage is it can take time to implement.