**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.

**Answer: -** Employees are the most important and valuable asset to any company, however employees create risk to the company as well. Reputable Cybersecurity organization found that approximately 88 percent of all data breaches are caused by an employee mistake and majority of cyber-attacks due to human error and it’s not easy to find a solution for this error. Below mentioned are three potential attacks.

**Attack 1**: - Phishing Attacks

The biggest and most damaging and easy widespread attack is the Phishing attack for any company. In Fact, a study conducted by PhishMe tracked that 91% of cyber-attacks started with a phishing email.

So, let’s look over how an employee can get phishing attack, one of the employees of SilverCorp is using company email account and personal email account on personal device, the employee gets phishing email on personal email account and by clicking on a link in the phishing email, employee may end up giving the attacker access to sensitive data of SilverCorp email account.

**Attack 2**: - Man In The Middle Attacks (MITM)

If an employee is doing company work on personal Laptop or Mobile device and once employee log in to unsecured Public Wireless Connections, it could allow hackers access to confidential company information as well as access to passwords, by way of MITM attacks. And next time the employee logs in to SilverCorp network with a personal device the virus and malware could spread and infect SilverCorp whole network. Public Wireless Connections are not secure for personal or Company use.

**Attack 3**: - Drive-by attack

Drive-by attacks are common method of spreading malware via HTTP websites, SilverCorp company employee easily can visit unsecure HTTP website and hacker will plant a malicious script into HTTP or PHP code on one of website page and the script will install malware directly into the employee computer or it will redirect to a hacker site.

And drive-by attack doesn’t rely on a person to do anything to actively enable the attack, person no need to click a download button or open another page to become infected, as soon as person open HTTP website, drive-by attack can take advantage from website to operating system or web browser that contains security flaws due to unsuccessful updates or lack of updates.



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

- For example, if employees were downloading suspicious email attachments, the preferred behaviour would be that employees only download attachments from trusted sources.

**Answer: -** For the potential three risks listed above, the preferred Behaviour is as follows: -

1. Increasing awareness of phishing email and provide employee below technique: -
2. Analyse Email Inbox - Do not open email from an unsecured email address, analyse the email address domain and subject for a minute before opening.
3. Hover over the email or link - Move mouse over the email or link, and do not click on it, just let the mouse cursor hover on the link and see what is the link and do critical thinking to decipher the URL.
4. Sandboxing – Employees can test email content in a sandbox environment.
5. Make SilverCorp work environment to such an extent that the employee does not have to work from home. Although this may not be achievable in other situations and some employees have to work from home and in these situations, employees should be able to do work from home while using a VPN and the company should provide and have a policy to issue encrypted secure laptops or computers to the employees for company work. And also provide information to employees about wifi connectivity through a secure and encrypted WPA2 connection.
6. Increased protection from virus:

Installing an antivirus on employee personal devices, SilverCorp can offer employees to install the latest anti-virus software on their personal devices as part of using personal devices in the office.

1. HTTP & HTTPS awareness:

SilverCorp should provide information about HTTP and HTTPS to employees and also block all HTTP websites from the company network.



3. What methods would you use to measure how often employees are currently \_not\_ behaving according to the preferred behaviour?

- For example, conduct a survey to see how often people download email attachments from unknown senders.

**Answer: -** Below aremethods SilverCorp should measure for employees:

1. SilverCorp should conduct a live practice cyber-attacks to see how employees react towards unsecured HTTP websites, phishing email and unsecured networks. It will be just like a fire drill, and running practice attacks will help SilverCorp employees to learn from their mistakes and SilverCorp will also get data on how many employees in the company need help for improvement and it will generate future plans for how to train employees.
2. Make few company policies and provide training to employees and after the training do knowledge base tests or survey with employees to see how good they are after training, here are few example policies: -
3. Bring Your Own Device policy.
4. Unwanted data policy.
5. How to report suspicious emails or ransomware policy.
6. Strong and complex passwords policy for all company employees to access any company system or network.
7. SilverCorp should implement email authentication technology that blocks suspicious emails and train employees about phasing email.
8. SilverCorp should also implement a multi-factor authentication policy to access sensitive network areas, such as providing a temporary code that is sent to your mobile phone to log in.
9. SilverCorp should look over their network firewall system and create a list of how many employees have visited HTTP and unsecured websites.



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

- For example, to have less than 5% of employees downloading suspicious email attachments.

**Answer: -** The goal will be definitely to secure 100% employees but it will be depending on the result of the live practice cyber-attacks, for example, after first training SilverCorp security team collected the data showing 75% employees click on suspicious email and then SilverCorp should do one more time live practice cyber-attack and then see what percentage of employees are clicking on suspicious email, and if 25% employees are still clicking suspicious email attachments or clicking on link provide in the email, then all those employees go through training every month.

And the compliance goal for SilverCorp will be to achieve 99%, and in future SilverCorp will be in good positioning for 0% systems breach by way of employee’s use of personal mobile phones.



**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.

**Answer: -** Below are the five SilverCorp employees.

1. **Designation**: Chief Executive Officer (CEO)

**Role**: CEO role will be taking an initiative to create vision for the SilverCorp and start a mission for security defences.

**Responsibilities**: CEO responsibilities will be starting processes, plotting the overall direction and bringing all heads of department into operation and evaluating the work to other executive leaders, and provide support for the security culture goals by giving approval to security defences budget as well as communicating to the company board of directors.

1. **Designation**: Chief Information Officer (CIO)

**Role**: Develops IT systems that support the business and implement the technological aspects of the cybersecurity proposed plan, for example installing malwares, upgrading company network system & firewall.

**Responsibilities**: Conduct surveys for the assessment of SilverCorp security culture, quality control studies for repeat assessment of whether the company is achieving the set milestones and goals for the implementation of the security policy, and ensure all employees have taken the training, work with managers and administrators to confirm and ensure compliance.

1. **Designation**: Chief Information Security Officer (CISO)

**Role**: Real-time analysis of an organization’s data and system and build a full information security program with well known three information security in mind and they are confidentiality, integrity, and availability.

**Responsibilities**: CISO will be responsible for creating a plan on how employees will get access to online training resources and create a method about live practice cyber-attacks, and as well as providing data after training & live practice cyber-attacks to CEO.

1. **Designation**: Director of Human Resources

**Role:** HR role is to manage human resources operations in recruiting and selecting employees for implementing the new security culture and also planning, monitoring, and reviewing staff contributions within the survey.

**Responsibilities**: Ensure all employees have taken the training and work with managers and administrators to confirm and ensure compliance.

1. **Designation**: Internal Training & Communications Manager

**Role**: Internal Communications Manager works across the company to increase awareness, understanding, and connection to the company leadership among members, fostering an internal culture of transparency and shared understanding.

**Responsibilities**: Communicating the policy changes to the employees and provide training to the SilverCorp employees against the security threats by creating awareness of cyber-attacks.



**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:

1. How frequently will you run training? What format will it take? (i.e., in-person, online, a combination of both)

**Answer:** Initially the live practice attack & survey will be conducted to assess the knowledge base of the existing employees. The results of the live practice attack will be analysed for reliability and validity, and then SliverCorp should be able to make decisions and run training programs every month for those employees who download insecure attachment from the network and three months for each employee with surveys. And the format of the training will be composed of both in person interactive sessions and online learning. Company’s CEO, CIO, CISO, HR and other senior managers will be directly involved in all these training.

1. What topics will you cover in your training and why? (This should be the bulk of the deliverable.)

**Answer:** Some training courses will be broad based creating general awareness (i.e., how to avoid insecure behaviour), and others will be targeted by specific areas of vulnerability, and general courses will be repeated every year but specific topics will be covered every 3 to 6 months with updated data. All these training will help the employees understand the potential quantitative impact of non-compliance with the security culture policy

Below are the training details information: -

**Phishing Attacks: -** Phishing attacks topic is really important and all employees need to recognise potentially harmful emails and reporting suspicious ones, by offering this training attacks can be dramatically reduced.

**Passwords and Authentication: -** Train employees how to implement randomised passwords and other steps, such as two-factor authentication.

**Physical Security: -** Provideawareness of the risks of leaving documents, unattended computers and passwords around the office space. And if SliverCorp implements a clean-desk policy, the threat of unattended documents being stolen or copied can be significantly reduced, and also give training regarding Physical Access Control Policy (i.e., how to enter in office with key access card).

**Removable Media: -** Removablemedia awareness topic should be included in all training and cover examples of removable media, how employees can prevent the risks such as lost or stolen removable devices, or USB sticks attack and get malware infections and copyright infringement.

**Public Wi-Fi: -** Educating employees on the safe use of public Wi-Fi and providing information about fake public Wi-Fi networks, often posing in coffee shops as free Wi-Fi, can leave end users vulnerable to entering information into non-secure public servers.

**Social Media Use: -** Educating employees on protecting the privacy settings of their social media accounts, and preventing the spread of public information of SliverCorp company will reduce the risk of the potential leverage that hackers can gain from this access to employees’ personal network.



1. After you’ve run your training, how will you measure its effectiveness?

**Answer: -** To measure the effectiveness of SliverCorp training and security culture policy security team should do direct device compliance audits, and test employee's knowledge by conducting surveys and comparing results for before and after training using the same survey, also get all employee’s feedback.

Another way of measuring the effectiveness is simulating phishing attacks and measuring how many employees fell into the trap.



**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:

* 1. What type of control is it? Administrative, technical, or physical?
  2. What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?
  3. What is one advantage of each solution?
  4. What is one disadvantage of each solution?

**Answer: -**

* + 1. MAC Filtering, Access Control List or VPA

**Type of control:** Technical

**Goal**: Preventative (This will allow employees to access company resources with appropriate credentials network)

**Advantage**: Employees are able to do their work from home or out of the office and this will secure the company system and data.

**Disadvantage**: Due to the large number of employees, there will be chances of high cost of installing software and maintaining data of employee’s accessibility may be time consuming.

* + 1. Acceptable Use Policy – Employees can’t use their personal devices to access company resources.

**Type of control**: Technical and Administrative

**Goal**: Corrective & Deterrent (Protection of sensitive data in the event of a breach & if employee try to access then it will be losing their employment)

**Advantage**: Employees won’t be able to disclose company data to their insecure environment or personal bad habits.

**Disadvantage**: Employees won’t be able to do their work outside of company hours, possibly it will impact the competitive potential of the company.