## Measure and Set Goals

**1.**

Providing access to company information on personal devices (specifically phones in this scenario) brings about two major concerns - access control and storage management.

Being able to save credentials on devices for apps, makes it hard to verify that the employee is the actual agent accessing the data, rather than a malicious entity.  
  
Similarly, if employees are able to download documents and information, which may be confidential to the business, there is no way of then controlling future access to the file now stored on the device.

A malicious entity could attempt to exfiltrate this information with a range of methods including:

**Email/SMS phishing** - whereby the user is directed to a URL containing malicious code.  
**URL padding** - whereby the user is directed to a URL that appears to be valid, but in fact is malicious.  
**Man in the middle** - whereby a rogue AP may be set up in a non-trusted location, allowing interception of traffic.  
**Device theft** - thereby giving access to information sources and downloaded content.

**2.**

Preferred employee behaviour for the access of company information via personal phone devices would be to:

* Generally avoid visiting links from unknown or external contacts.
* Ensure their device remains on them at all times to reduce the risk of theft.

**3.**

Performing a regular test email such as a Phriendly Phishing campaign will result in some metrics relating to the access of links from unknown or external sources - however this would reflect both personal and company owned devices.

Unfortunately the loss of personal devices is not common knowledge to SilverCorp, so we would have to rely on surveys to account for device theft/misplacement.

**4.**

The goals I would like to set for Silvercorp are:

* Less than 10% of employees are accessing suspicious links from emails or SMSs
* 100% of stolen or lost personal devices used for work are reported so that appropriate measures can be taken.

## Involve the Right People

In order to achieve these goals, the following people/departments will need to be involved:

**Security Culture Leaders**

Essentially the team of security experts within the organisation who have assessed the current landscape and come up with some viable goals. In this scenario ‘Us’

**CISO**

The CISO must be informed of the assessed risks and the potential outcomes of achieving the goals set. This will most importantly include an idea on cost, which will determine our ability to complete the objective.

**Human Resources**

The HR team knows how many people and what roles they are in. Their input is mandatory to ensuring we are able to improve security culture across all employees.

**Communications**

Unfortunately our letterheads aren’t up to scratch - fortunately the communications team that handles company wide memos and announcements have just the right way to catch the eye of our employees, ensuring that they are all informed of the plans to improve culture.

**Employees**

Every single one. We cannot achieve a change in mindset or culture without the involvement of the employees.

## 

## Training Plan

Our training plan will aim to educate all employees on two very important items.

1. How to assess and treat suspicious communications
2. The importance of reporting the loss or theft of a personal device used for work

The topics covered within these two items are as follows:

**What Is Phishing**

Explanation of who, what and why phishing is such a common attack

**Phishing Basics**

How phishing works, examine the core elements of every phishing attack. The message, the call to action and the collection of information.

**What Is Spear Fishing**

How it differs from normal phishing.

**Digging Deeper**

How can we identify a phishing message, what are some key indicators? Cover off examples such as from address, odd formatting, poor literacy, strong language.

**Slow Down Be Cautious**

At the end of the day take a breather and think before taking action. If something is real and truly urgent, surely you should receive a phone call. You may even decide to call the organisation via an accurately sourced phone number.

**How Much Is Your Phone Worth?**

Go over the personal value of a phone and compare it with the value of personal data. Extrapolate this to highlight the importance and value of company data.

**What To Do If You Lose Your Phone**

Explain what measures the organisation can take to revoke access if your phone is misplaced or stolen, and why it matters not just to the company, but to the employee.  
  
The training plan will be rolled out in a three phase program:

**Phase 1 - 0% Educated**

Period: Daily  
Length: 45 minutes - In person  
Incentive: During lunch time, lunch is provided.  
Attendance: Voluntary  
Group Limit: 40  
Followup: 3 days post attendance, staff are required to complete an online test.

**Phase 2 - 50% Educated**

Period: Weekly  
Length: 45 minutes - In person  
Incentive: none  
Attendance: Mandatory, selected at random. Absentees will be followed up.  
Group Limit: 40  
Followup: 3 days post attendance, staff are required to complete an online test.

**Phase 3 - 80% Educated**

Period: Monthly  
Length: 60 minutes - In person with test  
Incentive: Restoration of access rights  
Attendance: Mandatory, selected at random  
Group Limit: 40  
  
**Reinforcement Program**

Users that fail the subsequent online test will be subscribed to this program, whereby access to email from their personal device is revoked. They are then required to watch a recorded session and complete the test immediately afterwards.

Access is restored upon passing the test.  
  
**Post-Training**  
Phishing campaigns will be sent out monthly, to all educated users. If a user clicks the subsequent link, they are sent a concise email advising them of their failure. Repeated failures result in the user being subscribed to the Reinforcement Program.  
These metrics will be monitored so that we can ascertain a success rate.

## Other Solutions

1. **Mobile Device Management** - a technical control which can be considered quite invasive. This solution allows the remote management of personal devices, to the extent they can have restrictions on apps, geolocation and even erased. It is primarily a corrective solution as typically it would be engaged post-incident to remove access or information. The advantage of this solution is the very high level of control provided, however it can be very costly to deploy in large organisations.
2. **Prevent Sign In From Mobile Devices** - A technical control which prevents users from being able to logon from their device. Instead, they can only logon from work desktops/laptops. This can be considered a preventative control in that it prevents information being accessed on mobile devices, thereby reducing their risk factor considerably. The obvious advantage of this is that no training is required and it can be deployed instantly. The downside is that it would likely hamper productivity and morale.

**External sources of note which used in this assignment:**Phishing Training - https://securitytraining.opennews.org/en/latest/Chapter02-08-Phishing.html