Step 1: Measure and Set Goals

1. Malicious Mobile Applications, Phishing, Device Loss or Theft.
2. Malicious Mobile Applications - For mobile devices, companies should consider providing endpoint [security solutions](https://www.trendmicro.com/en_us/forHome/products/mobile-security.html#compare-versions) that feature app reputation technology that can detect whether certain apps are safe to use. In addition, the organization’s [enterprise solutions](https://www.trendmicro.com/en_us/business/products/user-protection/sps.html) should include device management and application management features that allow IT professionals to manage the installation of applications from a single, centralized console.

Phishing - Organizations should make user education a high priority. Employees should be taught to detect phishing attacks and briefed on what to do in case they receive suspicious messages or emails. As an extra security measure, companies should also look into installing solutions that can prevent or at least minimize the impact of phishing attacks on the devices of their employees. For mobile devices, this includes [solutions that integrate tools such as integrated data loss prevention, application control, and web filtering.](http://apac.trendmicro.com/apac/enterprise/product-security/mobile-security/)

Device Loss or Theft - Employees who use their own devices should be required to use security solutions that can encrypt the data contained in their devices. Full disk encryption ensures that even if a device falls into the wrong hands, the data contained within is essentially unreadable to everyone except those who have access to the decryption tools. Secure authentication is another important aspect of personal device security. Many people place minimal authentication into their devices, thinking that they can never be lost or stolen. This means that important information stored on these devices can invariably be accessed with just a little tinkering. Organizations should also require any user who stores company information on their devices to enable [multi-factor authentication](http://blog.trendmicro.com/whats-the-deal-with-two-factor-authentication/) to ensure that any data stored in an employee’s device is not accessed easily. The true cost of a lost mobile device goes far beyond the price of replacement, thanks to lost productivity, loss of intellectual property, data breaches and legal fees.

1. Device Loss or Theft - Take a poll/survey to see who has [multi-factor authentication](http://blog.trendmicro.com/whats-the-deal-with-two-factor-authentication/) on their devices, if anyone else uses or has access to those devices, and if any employees have lost or have had their personal devices ever

stolen.

1. Ideally all employees must have [multi-factor authentication](http://blog.trendmicro.com/whats-the-deal-with-two-factor-authentication/) (MFA) on devices with company data. A current goal of under 10% of employees without MFA on devices.

Step 2: Involve the Right People

* Chief Operating Officer (COO) - Oversees people management for the Implementation of the plan. In charge of hiring people to help progress the plan at all stages. In charge of firing employees who disregard or who fail to follow the plan.
* Chief Financial Officer (CFO) - Allocates funds for the project as a whole. In charge of the budget for each section of the project, depending on importance.
* Chief Information Officer (CIO) - Setting up employee devices for MFA. Setting up secure data storage on all employee devices and VPN for company servers.
* Chief Information Security Officer (CISO) - In charge of managing risk to an organization's data throughout the program. They are responsible for ensuring that the company's data is safe from the time it's collected to the time it's stored and retrieved. They develop and disseminate training to personnel, working with the CIO to coordinate implementation of the security policy by IT teams.
* Human Resources - Responsible for internal communication of plan and scheduling training of employees.

Step 3: Training Plan

When implementing a new program into an organization, it’s crucial to offer the necessary training to make your program, policies, and frontline associates successful. As management is interacting with your frontline staff on a weekly basis, get them up to speed first, on your BYOD policy and mobile program. Host onboarding sessions specifically for management to make sure everyone is on board and that they have the right information to answer staff questions. Once management is aligned, host multiple onboarding sessions for staff to listen, learn, and ask questions regarding MFA.

Training should be done in groups/sectors of the company and will be done in person with members of IT and human resources. Twice a week, a meeting will be convened in which employees will have IT help them with the implementation of MFA onto their personal devices that are used for company purposes. The MFA training will include SMS token authentication, employee ID, and employee password. SMS token authentication is when the organization sends a PIN number to a user via a text message. An employee’s password will also be changed every 6 months to prevent keylogging. IT will also teach employees how to maintain the security of their personal devices, Human resources will schedule the meetings and assign which employees will attend what times.

To increase adoption and engagement of the MFA program, human resources can create a competition with rewards and prizes. This will help engage staff, increase adoption, and start MFA on personal devices off on a positive note. First experiences by the employees will either make or break the policy. IT and human resources will work together to create an onboarding process that is easy and quick for staff to opt-in to the program and sign-up to company platforms and tools. Encourage feedback from employees by encouraging feedback and ideas to help the policy and training improve and succeed.

Bonus:

1. Application that will give you the capability to remotely wipe any device to protect your company’s data. It is a technical, preventative measure that protects company data before a lost device is compromised. The downside is that all the data is lost unless it is backed up. If the device is then found, it would take time to be reformatted and reset.
2. Leaving company data on a personal device when that person retires, finds work elsewhere, or is terminated can be a big problem. An administrative solution is having a specific set of procedures when this occurs. Upon any termination, an organization is obliged to ensure all data is removed from the device and permissions removed from company applications. This is a good preventative measure to ensure that no company data is compromised.