**Step 1: Measure and Set Goals**

1. There are many risks involved in BYOD (Bring your own device) and all can pose their own repercussions and potential side effects, there can be Data theft, poor phone or device management, staff may not understand the requirements for them to secure their own device as well as Malware.  
   Three potential attacks include; Having Malicious apps Installed on the Phone, A physical attack I.E someone stealing the device, Man in the middle attacks caused by insecure networks while accessing company systems or email.  
   (Hollander, 2021), (Poggi, 2021)
2. Based on the scenario above the correct behaviour for staff are beyond not using personal devices at all are;  
   -Have staff Trained and up to date on the risks of Possible malware infected apps, have a known list of harmful apps available so staff can see what to install, have staff install mobile application management software so the IT team can identify potentially malicious software on an automated system.  
   -Have staff install a piece of software to track the devices whereabouts and allow them to completely wipe all data from their phone remotely if need be.  
   -Have all employees follow the inplace BYOD policies, have a private vpn tool for the employee to use in order to access company information or some other form of two factor authentication, ideally both.  
   (Hollander, 2021), (Poggi, 2021)
3. In order to track these behaviours for assessment i would implement the following tactics;  
   - Conduct a survey to determine what apps are installed on employee’s phones.  
   - Have online training that includes a test component to see how many employees require further/retraining.  
   -Have the IT Security Team Track IP addresses coming into the system from insecure Networks or unauthorized networks.
4. The Appropriate goals for these specific tests would be;  
   -0% access from unauthorized/insecure IPs  
   -<5% Malicious software installed on devices  
   -100% of employees have the correct software installed on their phones for IT teams to maintain security.

**Step 2: Involve the Right People**

In order for this Plan to work as intended and achieve its goals Everybody in the company needs to be involved to some degree but the 5 most important people are as follows;

-CEO, Without approval from the CEO we will not achieve funds or resources to make this plan successful, the CEOs responsibility will be to monitor the functionality of each Policy or tech solution and receive feedback from the others involved on how targets are being reached.

-HR, the HR team needs to be involved to monitor the process to ensure the Privacy and safety of employees is maintained and to organize training for all the staff members, the surveys will also be conducted by the HR team.

-CISO, The CISO needs to be involved in order to strategize the development of the tech solutions and relay this to Their team in order for security functions to operate smoothly.  
-IT security team, The IT team needs to be involved in order to gather data on web traffic coming in from insecure platforms and also to develop, push out and maintain any security software on employees devices.  
-CFO, The CFO needs to be involved in order to have an accurate estimate of cost and determine the scope of the solution from a monetary point of view, They will be able to track the impact of the Financial impact on our current status and once goals are achieved.

**Step 3: Training Plan**

BYOD training is the most Crucial element in order for any other tactics to work, with out employees having the knowledge and tools for success then all other solutions will surely fail.  
  
Training will be Held Quarterly and only a selection of employees will attend with an aim to see all employees every Year. The format for this training will be in person training followed by an online form of training within 6 months after the initial in person training in order to solidify information.  
The training will cover the following topics;  
-What BYOD will mean for this company, without explaining the importance of BYOD policies to employees they will not understand the importance and most people aim to do the correct thing.  
-Explanation of software to be installed on personal devices, this is so employees understand what and why the appropriate applications are to be installed on their devices.

-Define BYOD security, Cover topics like password policies, corporate network security, public wifi dangers and device loss/theft policies.

-Data ownership policies, Corporate vs private emails, business vs personal contacts and corporate data on the device.  
- Define Mobile Device Management (MDM), introduce employees to the correct process to manage their device and what good MDM looks like, describe any relevant features  
-Teach employees to use Mobile office suites, this includes Document security and how to prevent others from having read/write access to private documents, recommend mobile office apps for use.  
-Supply BYOD guide book and Explain responsibility, this way all employees have the knowledge to maintain their own MDM and understand they are responsible for it.  
-Teach on how to access corporate resources, include things like VPN access, Corporate email, sales tool ect.  
-Explain technical support, how to access help and the escalation plan so fix any issues that arise.  
  
The effectiveness will be Measured Primarily by the follow up Online training, it will contain a refresher on the information provided in the main session which is then followed by a test to determine if the employee has understood the process and information that is required of them. If the employee does not achieve 100% on this test then they are to restart the module a second time and attempt the test again, upon a second failure it is escalated to required management so the employee in question can receive retraining.

(Kelly, 2021)

**Bonus: Other Solutions**

Two other potential solutions are as follows;  
  
- Don’t allow BYOD access for your business, if there aren't any unsecured devices connecting to the company network then security risks are mitigated.  
This is a Physical Control since employees will either need to have a company supplied device OR be on location in order to access the network. This control is also Preventative as it is stopping potential risks from coming through before the risk has a chance to impact the company.  
**Advantage** - It seriously impacts the security by closing security risks coming from insecure devices that haven’t been approved by the company.  
**Disadvantage** - Limits employees to only being able to work on site, will prevent remote working or if the company supplies approved devices then this could be an expensive solution for the company.

-Install monitoring software on the personal device allowing IT to track apps and usage.  
This is a technical solution as it requires tailored software to be installed on a device.  
It is also a Detective control as it doesn’t stop a breach but simply allows the IT team to find the issue faster.  
**Advantage** - can be used to quickly eliminate unwanted malware or track any attempted/successful breaches into the personal device. It also keeps the company in control.  
**Disadvantage** - It can be a privacy concern and would need to be heavily monitored by HR team to ensure no misuse is occurring, it also doesn’t stop any breach from happening in the first place which could be very detrimental to the company.

**Bibliography**

Hollander, G., 2021. *The Top 7 Risks Involved With Bring Your Own Device (BYOD)*. [online] M-Files. Available at: <<https://resources.m-files.com/blog/the-top-7-risks-involved-with-bring-your-own-device-byod-3>>

Poggi, N., 2021. *The BYOD Policy Guide: Biggest Risks and Best Solutions for Security - The Missing Report*. [online] The Missing Report. Available at: <<https://preyproject.com/blog/en/10-tips-for-creating-a-secure-byod-policy-for-your-company/>>

Kelly, W., 2021. *10 essential elements of BYOD training*. [online] TechRepublic. Available at: <<https://www.techrepublic.com/blog/10-things/10-essential-elements-of-byod-training/>>