1mobility

April 2014

BYOD Guidelines

A practical guide for implementing a successful BYOD Management program in an organization of any size.

Bring your own device (BYOD) refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications.

Benefits of BYOD

- Cost savings
- Shift responsibilities like procurement, ownership, carrier contracts and support for devices to individuals.
- Employees don't need to carry multiple devices.
- Ease of use as employees work with device and platform of their preference
- Improved productivity and above all ***greater job satisfaction!***

Challenges with BYOD

Though BYOD brings many benefits, it creates challenges for organizations to manage and secure the corporate data on these personal devices.

Organizations need to implement a solution that ***protects the privacy of employees without compromising security of corporate data and assets.***

BYOD Practice Transition

What Does BYOD Management Involve?

- Managing devices that connect to corporate network and resources using a software
- Written policies and acceptance by users
- Securely enabling data and corporate assets on the employee owned devices

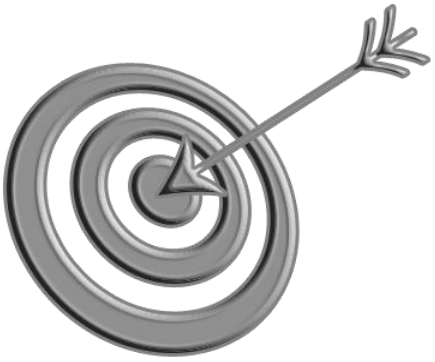
Are you in denial?

Do you think you have no digital data at risk? Do you think you have no sensitive data in the emails (financials, HR data, sales projections, salary data, IP, business plans and secrets)?

Do you think you can live without mobile devices (tablets, smartphones and laptops)? You will never allow BYOD? Do you think nobody in your organization intentionally or unintentionally leak the data?

If you are thinking yes to any of these questions, you have to accept that YOU ARE IN DENIAL. Your competition may have embraced mobility and made progress; accept the reality and prepare yourself for enterprise mobility.

Identifying Business Goals



BYOD is not mandatory to any organization but it is obvious. It has become a fact of business life.

It is very important to define which business benefits you are looking for by allowing BYOD.

- Better integration of Personal and Work lives
- Cost Savings
- Flexibility
- Mobility
- Increased productivity
- Improved customer relationship

Is BYOD IT Project? That's a myth!

BYOD is for empowering business. It also involves cost savings, policies, budgeting for security and many more things. All or some of these departments are stakeholders in the BYOD Management Project –

- Finance
- Legal
- IT
- HR
- Vendors
- Partners

BYOD Management Do's

- Define what does BYOD mean to your organization? **Focus on business goals throughout the entire process.**
- Identify stakeholders and get them involved
- Identify your valuables and vulnerabilities before planning strategy, tools and solutions.
- Define Plan for Eligibility, Policies and Roll out process
- Think device independent technologies and solutions, devices will change continuously.

BYOD Management Dont's

- 'One size fits all' approach doesn't work with BYOD. You have define your own needs, risks and plans
- There is no silver bullet. Don't assume all your problems will be used by one solution.
- BYOD is not a tactical plan and a one off project, it is strategic! Make it iterative. Take baby steps.
- Don't get overwhelmed by feature lists provided by various vendors. You need solutions and not features!

Step-by-Step Guide

Step1: Define Eligibility

Identify who among employees, contractors, vendors and partners should be allowed BYOD?

Remember, you don't have to allow BYOD to everybody.

For management of devices whether corporate or BYOD, you need access to the devices. You should identify vulnerable (lower versions of Androids don't support encryption) or non-manageable devices and choose not to allow these devices on the corporate network.

If your infrastructure at this stage is not compatible with all types of mobile devices, don't be forced to apply "all or none" approach.

Allow devices that you are confident you can manage and allow you to be in control of corporate data and management of risk.

Step 2: Cost Planning

For implementing BYOD, there are few things you need to budget for. Think through reimbursement, if any, for the hardware, data/voice plans, apps and how much.

It is MUST that you are able to identify the devices that connect to your network and access corporate data, you will need to budget for Mobile Device Management (MDM) solution.

Usually, MDM solutions are easy to manage, but ensure that you have a trained employee or consultant to define security policies and management of mobile devices.

As you mature in your enterprise mobility, you need to budget for the advanced implementations like secure enterprise apps, information rights management (IRM), services and support for continuously evolving mobile environment.

Like any other project, BYOD management requires various departments involved, you will need to budget the human resources and their time.

Step 3: Implementation Planning - Keep it Simple!

Choose the solution that solves your problems and don't fall for a long list of features which you may never need.

At a minimum, you need MDM as a base solution that can manage approved list of heterogeneous devices.

Review your needs for device lockdown, encryption requirements, whitelist/blacklist of content and apps, enterprise level configurations for Wi-fi, VPN etc. as well as compliance enforcement.

Keep it Simple: examples, If you don't have any enterprise Apps or don't plan to have any in near future, don't opt for advanced App wrapping solutions. If you allow only emails and email attachments on the mobile devices, focus on a strong enterprise level Mobile email app that helps you configure and tightly manage the emails. If the mobility management solution demands too many changes to your existing infrastructure, then it is a big no-no!

Automation of compliance checks is critical as you don't want to depend on manual compliance enforcement. Your mobility management solution should provide decent automation and appropriate reporting.

IT administrators should not become bottleneck. Over-the-Air management and self-management capabilities for employees are important. Remember, BYOD is supposed to bring cost savings and not additional significant IT cost.

Step 4: Define Policies

Putting together policies around BYOD is a good exercise. You will be surprised, how many things have not been given a thought in various areas of general management and may help you fix some other processes.

Acceptable Use Policies and consequences of violations are absolutely important to be defined.

For reimbursement policies, who, how much, when, approval process and expense limits, personal VS corporate usage are some of the things that need to be considered.

HR may define new employee and exit formalities considering devices used for business purposes. HR should define policy around cleaning up personal devices and removing all corporate data access from BYOD.

You may have different policies for BYOD devices compared to corporate devices. Security policies will usually be based on the employee's role, group and location employee/contractor belongs to.

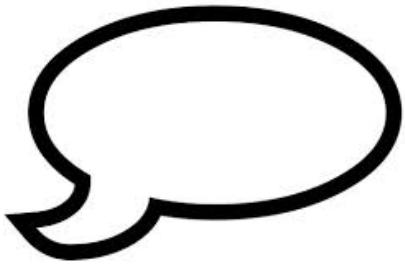
Security policies should consider situations like employee doesn't accept the use policy or device is lost or stolen, and guideline around how quickly employees should inform of the lost device, how frequently compliances should be checked and severity levels of violations.

Protecting privacy of employee's personal data, media and apps needs to be considered. What's the level of privacy protection your organization would consider while keeping the corporate data secure. Example – a government department may need full access to devices and the data on the devices; employee may not have any privacy leverage here.

Remotely wiping of the data is the basic data loss prevention strategy used, so it is important to define what data administrators are able to wipe; corporate only or personal too.

Step 5: Communication and Awareness

End users need to know what's valuable on their devices as well as what are the vulnerabilities. Training and awareness are very important.



Though employees may be using latest devices, don't assume all users are tech savvy and know threats through insecure networks, unintentional leaking of data, unencrypted data storage, threats through social media, malware and many other risks.

Explain policies and consequences of violations of policies and have the **end user license** (EULA) signed by each employee before they can get enrolled into the system to start using corporate network and corporate assets.

Step 6: Securely enable corporate network and data on the devices

Define security policies and DLP strategies like these but not limited to

- Heartbeat monitoring
- Containerization of Apps
- Virtualization
- Policy based access control
- Remotely lock device
- Wipe corporate data

- User identification and device authorization
- Passcode policy
- Remotely locate device
- Disable device features like screen shots, Bluetooth connectivity etc.
- SD card encryption & usage policy
- Blacklist/Whitelist Content
- Detection of compromised devices- rooted or jailbroken
- Enforce encrypted backups
- Separating personal and work data on the device

Step 7: Roll out Advanced Security Features

Based on the maturity level of your enterprise mobility, you may now move to implementing

Apps Management

- Over-the-air distribution of the public or enterprise apps
- Implement apps compliances – recommended and blacklisted apps
- Secure implementation of enterprise apps through app wrapping or SDK integration that allows developers to include security features like – encryption, authentication/single sign-on, VPN tunneling, analytical data collection, secure exchange of data between the apps

Geo-fencing

- Applying and releasing compliances based on the location of the device. This can be achieved by detecting if device has connected to your corporate Wi-Fi network or physically present in the restricted geo-location.

- This enables advanced management of BYOD devices. Individuals can enjoy their device features fully when not connected to the corporate network

Containerization

Keeping corporate data completely secluded from personal data is important and brings additional level of security to corporate data. Based on your organization's needs, you may have an advanced containerization or may use specific apps like email container or content viewer apps.

Step 8: Make it iterative

As you sail through your initial challenges with BYOD and overall mobility management challenges, revisit the policies and compliance enforcement strategies continuously.

It is important that you revisit your business goals at every steps of the way, don't lose your business vision.

A ship is always safe at the shore. But it was not built for that. So take risk and achieve more.

BYOD is a Fact of Business Life. Empower your organization with mobile technology and BYOD policy!

About 1Mobility

1Mobility is a global company with a cloud based, internationalized and scalable enterprise mobility management solution that secures, monitors, manages and supports mobile devices across platforms, service providers and manufacturers.

1Mobility provides an affordable, versatile and modular solution that enables over-the-air distribution of mobile applications, configuration settings and security policies to corporate owned or employee owned (BYOD) devices through a central web console.

www.1Mobility.com info@1Mobility.com