



BYOD : Managing Mobility within the Oil & Gas Industry

Changing the way your workforce functions. We provide the perfect BYOD solution that allows your employees to use their personal mobile devices and notebook PC's - to access enterprise data and systems.

Overview

Enterprise mobility holds an important place within the oil and gas industry. With applications shifting from desktop to the cloud and becoming easily accessible on smart phones and other mobile devices, organizations are significantly improvising over their operational efficiency as well as real-time decision making capabilities.

The BYOD phenomenon has been on the rise across all industries including the oil and gas sector. According to a study by Oil and Gas IQ, over 71% of the workforces within this industry have switched to using personal mobile devices for work, which mostly includes senior management and those engaged in field operations and technical roles.

However we understand that managing costs, support & security of these devices in a BYOD deployment environment is becoming more and more challenging.



Challenges



Companies in the oil and gas industry are faced with rising pressures due to cut-throat competition, rapid change, aggressive regulation procedures and an increasingly dispersed workforce to use cloud-based mobility to improve real-time staff connectivity, quality control and data accuracy.

Due to the nature of the oil and gas industry- volatile and often operating in hazardous locations, BYOD deployments can lead to special technical challenges and unexpectedly hefty costs such as:

Keeping an account over **unauthorized international roaming** and other mobile device usage behaviors' that have expensive consequences.

Maintaining tabs for on-the-go users who have access to a variety of devices, computers, and connectivity sources can be tough as **security** is a major issue. If left unmanaged BYOD can lead to loss of control, affect network availability and cause data loss.

Corporate Liability: It all comes down to who is responsible for getting targets achieved through mobile assets as many CIO's are of the opinion that the BYO model removes corporate liability for the device and the service plan for the employee.

Governance & Compliance: BYOD could cause you to violate rules, regulations, trust, intellectual property and other critical business obligations. The right network access strategies and policies are needed to secure your environment.

Solution

We realize that security plays a vital role within the oil and gas industry as more and more employees are accessing corporate information from personal mobile devices which thus highlights the need for strategy, policy and technical security controls.

BYOD (Bring Your Own Device) delivers a robust, simple, scalable and secure method to allow your enterprise to allow users to access corporate information from their personal devices.

We can provide your company workforce with a secure, customized application via a private, dedicated cloud which means fast deployments, instant software updates and real-time accessibility. With the help of our mobile application enabling BYOD solution, we are capable of handling:



Setting Geofencing Boundaries:

Automatically activates and deactivates device features and access to apps and corporate data on the basis of GPS location of enrolled mobile devices.

Workforce is mobilized with automatic Wi-Fi and email server access configuration as devices move in and out of geofence boundaries.

Within geofenced work locations, restricted access to sensitive corporate apps and market apps are enabled. Also, camera and other device settings are disabled to protect sensitive corporate information.



Tracking Expenses:

This solution ensures that there are no more unaccounted expenditures as it provides enterprises with a detailed insight into how much they are paying for mobile communications on a monthly basis and the utility of those costs.

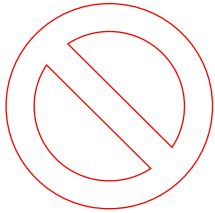
It also provides reports and audit bills regarding usage spikes so as to notify senior management, thus adjusting work patterns and cost optimization together.



Restricting App Access:

Oil and gas enterprises are given complete control as to how their workforce uses their mobile devices when they are both on and off work premises. For example: A company that doesn't want its employees to access social networking websites on their corporate-owned devices can block access to the sites across all their mobile devices.

Restrictions for certain features such as personal e-mail can also be enabled with this solution to prevent employees from using those features on their devices.



Creating Application Blacklists and Whitelists:

Accessing public mobile apps can be controlled with the help of custom whitelist and blacklist policies. Apps which are recognized as 'safe' for the workplace are categorized as white listed as they have been granted permission for usage across all mobile devices. Blacklisted apps on the other hand are restricted from usage.

Name	Class Name	Is locked	Apply Geofencing
About Device	android:restrictedAccountType="com.example.account.type"	Yes	Yes
Device	restrictions.getBoolean(UserManager.DISALLOW_MODIFY_ACCOUNTS)	Yes	Yes
Accessibility	restrictions.getBoolean	Yes	No
Accessibility(HTC)	restrictions.getBoolean	Yes	No

App Name	App Category	Required on Device	Secure Kiosk App
IR Show	Sales, Enterprise, SME, Enterprise Level Sales, Market Analysis	Optional	Invisible
Actavis IR	Sales, Enterprise, SME, Enterprise Level Sales, Market Analysis	Optional	Visible
Biblical Citizenship Houston	Sales, Enterprise, SME, Enterprise Level Sales, Market Analysis	Optional	Invisible

Features

BYOD revolutionizes your organization as employees use their own devices thus guaranteeing complete access to both business as well as personal applications at all times with the help of:

How?

Unique Policy Management:

We deliver a unified security policy across the entire organization and an optimized and managed experience for varied users with diverse business, security and device requirements. This policy helps you detect the device and the associated user, run a security check for clearance of viruses and bugs and determine what systems and applications they have access too.

Also, BYOD is a network-centric, integrated approach to security that enables:

Persistent security across all devices (traditional PCs and mobile devices)
Cloud-based web security for Internet, intranet, and cloud-based services
Separation of personal and enterprise apps and content while preserving the native mobile user experience
Use of all access methods (wired, wireless and VPN)
Privacy policy and selective wipe to secure corporate data while protecting personal data
Secured e-mail which minimizes the risk of data loss
Device Registration Portal for employee self-service

Benefits of BYOD

- ✓ Simplifies the mobile management process for enterprise organizations
 - ✓ Combines mobile device management, mobile expense management, and mobile apps
 - ✓ Reduces corporate and personal liability and risks
 - ✓ Built for mid-size enterprises with field service operations
 - ✓ Increases efficiency for employees by securing mobile devices and data access
-



Why Mobisoft Infotech for BYOD?

Because a closely integrated system is always the strongest. To enhance the productivity we offer BYOD as well as CYOD solutions to help control devices as they connect to your networks, data and apps. We can help ensure a smooth workflow and secure operations across a wide range of devices.

Apart from BYOD, we also recommend an alternative mobility strategy which can be pursued, **CYOD (Choose Your Own Device)**.

CYOD (Choose Your Own Device)

Pre Approved Device, owned by company, can be used anywhere

While many organizations are implementing BYOD programs, issues regarding security, management, support and compliance are major concerns. But when it comes to employees using personal devices in the workplace, companies need a balanced requirement between 'productivity' and 'security' which has given rise to CYOD.

What is CYOD?

Unlike BYOD, which encourages employees to work on a personally owned device, choose-your-own-device (CYOD) offers employees the freedom to use approved company-issued devices. In short, CYOD strategies indicate more control for IT, while still providing employees the flexibility to use the device of their preferred choice.



Challenges

The leading challenge faced by CYOD models for the company is to cover the exorbitant capital expenditure of the device. Most of the issues faced by CYOD models are similar to BYOD; they just take a simpler form and over time they generate fewer complexities and lower costs.

Compliance & Governance:

The main challenge that exists for both BYOD & CYOD is the lack of a systematic strategy for managing data across a variety of devices. Compliance is still a consideration; the same company mandates and government regulations apply. However, for CYOD it is simple to attain as the company has pre selected the choice of devices, which means hardware and software versions are under company control.

Security & Network Access Control:

As employees have access to corporate devices, how they access the network and company sensitive data is a constant challenge. But security is more straightforward with CYOD models as the company owns and controls the devices. Thus, this ensures that all software configurations are optimized according to the company security policies.

IT Support:

Even though this is a pressing challenge for CYOD, it is simplified as the IT Department is accountable only for a handful of pre-approved devices instead of having to handle an endless range of hardware and software combinations.

However, as these mobile devices would be used by employees outside the company, across networks that aren't owned and controlled by the organization, security and support challenges still exist for the IT Department.

CYOD Benefits:

CYOD models offer a similarly diverse range of clear strengths such as:

Employees choose their mobile device or laptop from a list of pre-approved devices that best fits their requirements and job descriptions without having to bear the initial cost. Since it is a work-related device, segregating personal and corporate data is a simpler process for the employee.

The work/ business divide is beneficial for the organization too as they can access the CYOD model at any given point of time without having to worry about the data being personal or not.

IT has its share of benefits too as it extends support only to a list of selected pre-approved devices which results in simplified troubleshooting, quick problem resolution, timely software updates and in compliance with regulations and internal mandates.

BYOD v/s CYOD: Achieving the best of both models

The indicator of a good CYOD policy provides your employees with freedom and mobility, without your IT Department losing control of company data. The key to success is to guarantee a secure workspace for easy IT management, security policy enforcement and offline capability.

Mobility is the core requirement for companies to perform tasks accurately and **BYOD** as well as **CYOD** operate on the same.

Issues regarding user privacy & corporate data security are a constant concern within the **BYOD** industry and lesser within **CYOD** as the devices are company-owned.

BYOD complicates IT security and manageability efforts. **CYOD** calls for high hardware acquisition costs, but can enforce clear-cut manageability and security policies.

Choosing between these models has their set of pros and cons, while providing varied benefit levels for IT. Thus, before choosing, your IT team should take the apt decision for their specific security posture & compliance requirements, while ensuring employee satisfaction too.

Contact

Powering the Future of business with comprehensive Mobility Solutions

Mobisoft works with businesses to enable them to gain flexibility, increase productivity, and reduce costs with end-to-end mobility services. Our enterprise mobility services cover all your mobility needs from strategic planning to device management to end-user application.



Houston business journal fast
100 company



NASA
Space Health Challenge



CES
Best Energy Monitoring App

Mobisoftinfotech.com

HOUSTON, USA

5433, Westheimer Rd, Suite 750,
Houston, TX - 77056.
855-572-2777 / 855-572-APPS
+1 832-420-1153
San Francisco: +1 925-257-4245

VANCOUVER, USA

15640 NE Fourth Plain Blvd,
Suite 222,
Vancouver, WA 98682
Phone: 360 909 0534

PUNE, INDIA

Plot No. 46, Rajiv Gandhi Info-
Tech Park,
Phase I, MIDC, Hinjewadi,
Pune, India - 411 057,
Phone: +91-20-65293691,
+91-20-65293692