WHITE PAPER

FieldAware™
Field Services...Managed!

IS BYOD (BRING YOUR OWN DEVICE) PART OF YOUR COMPANY'S FIELD SERVICE AUTOMATION PLAN?

INTRODUCTION

A recent study by Ericsson projects that there will be 5.6 billion smartphones (or 60 percent of the total number of mobile phone subscriptions) in use by 2019. They also project that smartphone traffic will reach 10 exabytes and that mobile data traffic will grow 45 percent between now and 2019.

Clearly, consumers of all ages, incomes and abilities are purchasing and using smartphones – as well as tablets – to do much more than perform voice communications. In fact, Ericsson notes that video will be 50 percent of all mobile traffic by 2019, audio traffic will grow 40 percent annually and that social networking and web services will expand by 10 percent. Finally the study notes that 76 percent of all U.S. Android and iPhone users play games on their devices.

Users' fascination with their smartphones doesn't end at home or during their time away from work. They often want to use their personal devices at work – and for work – as well. For field service organizations this presents possible benefits (reduced capital expense, limited use of corporate mobile voice and data plans) and dangers (mixing of personal and corporate data) as well. Therefore it's important for every company to understand the challenges that BYOD creates and the policies and systems that should be in place before field technician owned devices are incorporated into a field service automation framework.

The four challenges of BYOD:

- *Security*
- *Regulatory Compliance*
- *Device Support*
- *End User Support*

THE CHALLENGES

Companies that intend to allow field technicians to bring to and use their own devices at work face four significant business challenges:

1. *Security:* In a BYOD environment, personal and company access, applications and data are comingled onto a single device. The threat in this case is twofold. Many smartphone owners do not update their device's operating systems and applications on a regular basis. This exposes not only the device but company applications to a variety of security vulnerabilities. Additionally, applications that field technicians download for their personal use may also include security vulnerabilities or may inadvertently access company data. For example: a productivity application might access a calendar that is used for both personal and company tasks and appointments.

2. *Regulatory Compliance:* There are any number of existing state, federal and industry regulations designed to protect information security. Complying with these regulations (i.e. CIS, DISA, FDCC, GCSx, GLBA, HIPAA, ISO 27001, MA 201, NERC, NIST 800, PCI, SOX) can be difficult in a mobile environment, and more so in one that accommodates BYOD.

3. *Device Support:* Although the number of mobile operating systems might have decreased, the versions of those operating systems is still increasing. iOS, Android, Windows and Blackberry smartphones and tablets come not only in various shapes and sizes, but with software versions that are, in some cases, not upgradeable to more current versions. As a result, field service organizations may be forced to support numerous OS types and versions on devices from any number of manufacturers.

4. *End User Support:* With all of the different operating systems and devices, end user support costs can skyrocket. The time required to troubleshoot a problem may double or even triple, and more importantly, the productivity of the field technician experiencing the technical problem can be severely impacted. Consequently, costs could go up while revenue might go down.

BYOD means providing support for a variety of mobile operating systems, software versions, devices and manufacturers.

With all of the challenges that BYOD creates, it might appear that the easiest solution is ban the use of personal devices. However, many companies have successfully implemented BYOD solutions that were secure, compliant with existing regulations, limited device support and did not result in increased end user support costs or lost revenue. How did they do it?

POLICY

One of the most effective ways to meet the challenges of BYOD in a field service organization is to create a BYOD policy. Developing a policy not only protects the organization's network and data, it forces companies to think through how they will implement and support corporate applications and data on personal devices. Some important areas that BYOD policies should address include:

- Acceptable use: The activities that the field technician will be able to perform on his/her device during working hours. The policy might include:
    - Access to some personal use applications like email, reading or game playing
    - Blocking certain web sites during business hours
    - Information that may not be stored or transmitted
    - Allowed and disallowed applications
    - Rules against texting or emailing while driving
- Supported Devices: The smartphones and tablets that will be supported including models, operating systems and versions of those operating systems. Also include:
    - Who the field technicians should contact for device and operating system problems (not corporate technical support!)
    - Who will be responsible for provisioning and configuration of network access and company applications
- Security: Access requirements including passwords and password policies. Include:
    - Device PINs and locking policies
    - Number of failed login attempts before the device locks
    - Policy regarding jail broken (iOS) or rooted (Android) devices
    - Restrictions on applications that are not on the company's approved application list
    - Device wiping policy (if lost, worker is terminated, a virus is detected, or there is a policy breach by the worker)

A strong BYOD policy is a good first step that will enable companies to protect their own, and their customers' data.

- Reimbursement: Detail whether or not the company will reimburse the worker for all, some or none of the device purchase as well as coverage of the worker's voice/data plan.
- Disclaimers: Specify risks/liabilities and responsibilities of the field technician for company and personal data and the device itself. Include: Some important areas that BYOD policies should address include:
    - Back-up of company and personal data
    - Company's right to disconnect or disable services
    - Lost or stolen device reporting
    - Adherence to the acceptable use policy outlined above
    - Worker's assumption of liabilities for areas including:
        - Loss of company or personal data due to operating system crashes, errors, bugs, viruses, malware
        - Loss of company or personal data due to hardware or application failures
    - Disciplinary actions available should field technicians not comply with company policy

A strong, yet straight forward policy is a good first step to ensuring the success of integrating BYOD into a field service automation solution. However, it is often also important to integrate one final area to ensure that company and customer data is secure and that the system complies with industry recommendations and governmental regulations regarding information security.

MOBILE DEVICE MANAGEMENT

Mobile device management software systems enable companies to remotely configure mobile devices –singly or in in larger groups. Managers can send software and operating system updates, remotely lock or wipe a device and perform remote troubleshooting of devices. These capabilities enable companies to protect company and customer data should a device become lost or stolen or halt inappropriate use by the field technician.

There are a number of mobile device management software systems currently available. The table below outlines solutions from some of the top vendors.

Mobile device management software can send software and operating system updates, remotely lock or wipe a device and enable remote troubleshooting of devices.

Company	Product	Web Site
3CX	3CX Mobile Device Manager	http://www.mobiledevicemanager.com
4app	4app	http://www.4app-mdm.com/home/
Absolute Manage	Absolute Manage	http://www.absolute.com/en
airwatch	AirWatch	http://www.air-watch.com/
AmTel	Amtel MDM	http://www.amtelnet.com/mobile-device-management/
AppBlade	AppBlade	https://appblade.com
AppTec360	AppTec-Free Enterprise Mobile Manager	http://www.apptec360.com/en_home.html
auralis	Auralis	http://www.auralis.de/en/
BoxTone	BoxTone	http://www.boxtone.com
Capricode	SyncShield	http://www.capricode.com/
Centrify	Centrify User Suite	http://www.centrify.com/products/centrify-user-suite.asp
Cisco	Meraki System Manager	https://meraki.cisco.com/products/systems-manager
Citrix	Citrix XenMobile	http://www.citrix.com/products/xenmobile/overview.html
Codeproof	Codeproof MDM	https://codeproof.com/
Cortado	Cortado Corporate Server	http://corporateserver.cortado.com/
Crea Lab	Crea MDM	http://www.crearelab.com/sites/ENG/CREA-MDM/
Dell	Dell Mobile Management	http://www.dell.com/learn/us/en/555/operating-systems/sol-mobiledevicemanagement-home
DeviceLink	DeviceLink	http://www.unwireddevicelink.com/
Endpoint Protector	Endpoint Protector MDM	http://www.endpointprotector.com
Excitor	Excitor DME	http://www.excitor.com

Company	Product	Web Site
FancyFon	FancyFon Mobility Center (FAMOC)	http://www.fancyfon.com
FileWave	FileWave	http://www.filewave.com/index.php/features/management-suite/mdm-mobile-device-management
Globo Group	Notify MDM	http://www.notifycorp.com/products/notifymdm/overview
Good	Good for Enterprise	http://www1.good.com/secure-mobility-solution/mobile-device-management.html
IBM	Fiberlink MaaS360, IBM Endpoint Manager for Mobile Devices	http://www.maas360.com, http://www-03.ibm.com/software/products/en/ibmendpmanaformobidevi/
iboss Security	MobileEther MDM	http://iboss.com/ibwf_wf_byod.html
JanFSoftware	Casper Suite	http://www.jamfsoftware.com/software
LANDesk	LANDesk Mobility Manager	http://www.landesk.com/products/mobility-manager/
Lightspeed Systems	Lightspeed Systems Mobile Manager	http://www.lightspeedsystems.com/products/mobile-manager/
Lyceum Solutions	AppTrack	http://www.lyceumsolutions.com/
McAfee	McAfee EMM	http://www.mdafee.com/us/products/enterprise-mobility-management.aspx
ManageEngine	ManageEngine Desktop central	http://www.manageengine.com/mobile-device-management.html
Mformation	Mformation Enterprise Mobility Manager	http://www.mformation.com/solutions/enterprise-mobility-manager/#.Up4TGsPnapo
midpoints	midpoints mobile. profiler	http://midpoints.de/en-home
MobileIron	MobileIron	http://www.mobileiron.com/
nuVizz	nuVizz enterprise MDM	http://nuvizz.com/solutions/mobile-device-management/index.html
Optimal Biz	Optimal Biz for Mobile	http://en.optim.co.jp/products-detail/top/138

Company	Product	Web Site
Pradeo	CheckMyApps	http://www.pradeo.net/en/solutions/check-my-apps
ProMDM	ProMDM	http://promdm.com/
PushManager	PushManager	http://www.pushmanager.com/mobiledevice-management/en
Relution	Relution Enterprise MDM	http://www.relution.io/en/products/mdm/
Robot Cloud	Robot Cloud	http://robotcloud.net/
SAP	Afaria	http://www.sap.com/pc/tech/mobile/software/solutions/device-management/overview.html
Sophos	Mobile Control	http://www.sophos.com/en-us/products/mobile-control.aspx
SOTI	SOTI MobiControl	http://www.soti.net
Symantec	Symantec Mobile Management	http://www.symantec.com/mobile-management
Tangoe	Tangoe MDM	http://www.tangoe.com/solutions/MDM-overview.aspx
Tower-One	Tarmac	http://tower-one.net/en/products.html

The second table offers another option for BYOD management. It provides a listing of companies that provide mobile device management as a service. No software purchase is required and the service provider takes on all tasks related to management of smartphones and tablets. A monthly fee is charged based on the number of devices managed.

Company	Service	Web Site
AT&T	Mobile Management Services	http://www.business.att.com/enterprise/Family/mobility-services/mobile-management/
CompuCom	CompuCom MDM	http://www.compucom.com/consulting/end-user-computing/mobile-device-management
Earthlink	Earthlink MDM	http://www.earthlinkbusiness.com/itservices/mobile-devicemanagement
IBM	IBM Hosted Mobile Device Security Management	http://www-935.ibm.com/services/us/en/it-services/managed-security-services-cloud-computing-hosted-mobile-device-security-management.html
Neoscope Technology Solutions	Neoscope MDM	http://www.neoscopetechnology.com/services/mobile-device-management/
NetWorks Group	NetWorks Group MDM	http://www.networksgroup.com/managed-services/mobile-device-management
NexusIS	NexusIS MDM	http://www.nexusis.com/solutions/enterprise-networking/mobility/
RMS Omega Technologies	RMS Omega Technologies	http://www.rmsomega.com/Managed-Services-Mobile-Device-IT-Management.php
SilverSky	SilverSky MDM	https://www.silversky.com/knowledge-center/data-sheets/mobile-device-management
T-Mobile	T-Mobile MDM	https://business.t-mobile.com/corporate/solutions/mobile-device-management
TusHAUS	TusHAUS MDM	http://www.tushaus.com/Solutions/Managed-Solutions/Mobile-Device-Management

Company	Service	Web Site
Verizon	Verizon MDM	http://www.verizonenterprise.com/resources/factsheet/fs-cm-mwf-employee-devices_en_xg.pdf
Vertela	Virtela MDM	http://virtela.com/services/mobiltiy/mobile-device-management-mdm/

CONCLUSION

BYOD has obvious benefits for field service organizations. It reduces capital expenditure and can decrease or eliminate the need for extensive corporate mobile voice and data plans. However, organizations that choose BYOD for the field service automation implementations should also develop strong BYOD policies, and implement a mobile device management system or service to ensure the integrity and security of their data.

ABOUT FIELDAWARE

We are re-shaping the field service industry! Our made-for-mobile, cloud-based software was designed from the ground up to provide ease of use with incredible flexibility – a combination that enables field service organizations to amaze their customers, astonish the staff and surprise the competition. Our software was architected as a mobile platform, with no incumbent legacy technologies to modify or migrate from.

Based on our founders' intimate knowledge of the unique needs of engineers and technicians in the field – and the operational personnel and management that support them – FieldAware is focused on providing field service organizations, both large and small, with:

- Intelligence about your Customers: So you can increase revenue, expand into new markets, differentiate your services and create customer advocates.
- Intelligence about your Business: That enables you to increase the productivity of your staff (and keep them happy!), use company resources more efficiently, simplify your business processes and "right size" your parts and repair inventory.

We combine our software with the industry's best implementation, on-boarding and support services enabling companies to take full and rapid advantage of today's mobile environment.

To learn more about our solutions or to schedule a demo, contact your local FieldAware representative at fieldaware-sales@fieldaware.com or by calling 800-935-0736.