TM Forum
CyberOps Metrics
GB966 Quick Start Guide: Mobile Device Management
September 2012
Version 1.2

www.tmforum.org

North America
240 Headquarters Plaza
East Tower, 10th Floor
Morristown, NJ 07960
United States

Tel: +1 973-944-5100
Fax: +1 973-944-5110

Europe
47 Lower Brook Street
Ipswich
Suffolk IP4 1AQ
United Kingdom

Tel/Fax: +44 (0)207-748-6615

Notice

Direct inquiries to the TM Forum office:

240 Headquarters Plaza,
East Tower – 10th Floor,
Morristown, NJ 07960 USA
Tel No. +1 973 944 5100
Fax No. +1 973 944 5110
TM Forum Web Page: www.TM Forum.org

Contents

Glossary of Terms

BES	Blackberry Enterprise server
BYOD	Bring Your Own Device (in this case we mean Mobile Devices – See below)
DIVM	Device Integrity Validation Management (jail breaking /rooting protection)
DLP	Data Loss Prevention
ENEPID	Everything Not Expressly Permitted Is Denied
KPI	Key Performance Indicator
LD	Long Distance
MAM	Mobile Application Management (Approved Applications)
MAS	Mobile Application Store (Approved Updates)
MDM	Mobile Device Management, specifically security policy as it applies to the mobile device
RIM	Research In Motion
Mobile Device	For the purpose of this document; typically a smartphone or tablet
Mobile Malware	Unwanted and possibly malicious software on a mobile device
SAAS	Software-as-a-Service
SMS	Short Message Service

Introduction

“Stop me, if you think you’ve heard this one before.” Experienced security and device operations practitioners will quickly recognize that, for mobile device security, plus can change, plus c’est la meme chose. Laptops and other earlier mobile devices have laid a security foundation on which it’s logical to both extend and to build for security of the latest and future generations of mobile devices.

That is not to say that this new mobile device world is not without freshly complex nuances; this quick start guide addresses the most important new differences, and sketches extensions to emerging security vectors including in-vehicle systems, network integrated medical devices, and facility controls. Is a network-enabled air conditioner with an unprotected wireless remote control secure? Unknown risks can’t be quantified. While it used to be true that nobody got caught by an exploit they already knew, at present, organizational ability to respond lags days to months behind exploiters ability to innovate. Mobile devices offer an incomplete, dynamic and complex environment that is a potential habitat for hackers, and increasingly, those devices may hold data and access of high target value.

Mobile Device Management (MDM) is a system that enables enterprises to manage, update, and control the mobile devices on their network. MDM has become increasingly popular, driven by recent trends like BYOD (Bring Your Own Device), but mobile malware, device data security and other security concerns must be addressed by the IT security world for BYOD not to introduce terrible new threat and risk vectors in a very short period of time.

The bottom line remains: for best security, BYOD is inarguably still a second-best strategy. If you don’t own it, you can’t control it without an MDM solution[1]. If you can’t control it, you can’t secure it. The ability to control mobile devices will become increasingly popular as malware rates increase and BYOD begins to take hold. There are two issues that need to be dealt with at the MDM level. One: the corporate device. Two: the personal device for use on the corporate network. In both cases, data protection and unauthorized systems access are the central security issues.

Proliferation of threats on ‘consumer-grade’ devices being used for enterprise purposes may be assumed to be similar to those for the ‘consumerization of the personal computer’, and in vastly greater scale. Compared to lifecycles for the adoption of laptop computing, there is far less time for an organization to react in a holistic way. Lastly, compared with laptops, there is a greater possible negative impact on productivity and communications required when quick and effective security intervention is needed to prevent rapidly emerging threats.

Being able to manage and control mobile devices is a critical piece of the mobile security puzzle, and most important of all that control is the ability to secure or delete corporate data. The mobile device is a new threat vector in which cyber criminals can get information about users such as contact lists, photos, banking information and SMS messages. Additional, a compromised device can allow a hacker to use of the onboard camera to capture pictures near the user, or the onboard microphone to collect unauthorized audio.

[1] The Trusted Computing Group is one example of where such solutions may be found if not OEM-provided.

This is usually done through malicious applications that are downloaded from insecure app stores (or, in some cases 'less secure' approved application stores). Protection mechanisms in place are often ineffective and relatively easily bypassed at present by exploits that have already been released into the wild in root kit or equivalent form[2]. The infected devices can perform malicious activities like premium SMS or long-distance toll fraud.

The largest unmapped threat vector at present is connections with other devices and networks, the notion of mobile devices broadcasting, advertising, discovering and interoperating with data streams, applications and other devices in an increasingly layered and transparent way. This threat vector is made more insidious by the natural propensity of users to seek convenience, and it is almost always a trade-off between convenience and security where permitting interconnectivity or interoperability between mobile devices or network-enabled docks.

This Quick Start Guide (QSG) should be used for guidance on what can be done to protect your network and possibly give you the ability to determine your what your user base may be doing with their mobile devices, at least insofar as it affects your organization's valuable data and access security. This guide is the second in a series of five using DSD top 35[3], SANS top 20 and NIST/ISO general practises as guides. This QSG also acknowledges studies by Gartner, Forrester and other research groups, and the direct contributions of TM Forum participants and members including DISA, NATO, the UK MoD, and their contractors.

The SANS top 20[4] list provides:

1) Inventory of authorised and unauthorised devices
2) Wireless device control
3) Boundary defence
4) Malware defences

From the DSD 35:

1) User education (how to use devices securely)
2) Web content filtering
3) Non-persistent virtualized environment*

From the current joint efforts of NIST/ISO, the four levels of assurance[5] are a vital guideline[6]:

1) Simple password challenge-response protocols are allowed
2) Single factor remote network authentication
3) Multi-factor remote network authentication
4) Proof of possession of a key through a cryptographic protocol.

[2] This problem arises particularly in Android devices that download applications containing mobile malware
[3] http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
[4] http://www.sans.org/critical-security-controls/
[5] http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
[6] Future potential to reduce insurance premiums where compliance can be demonstrated

Conclusions

This projects 80:20 security purpose[7] is met with control over the following three areas:

- Configuration
- Encryption
- Vulnerability Management

All these areas are heavily affected by the concept of BYOD, Bring Your Own Device. A separate appendix of this document is devoted to those organizations that must permit BYOD for one reason or another.

In demonstrating control over the preceding areas, the following must be controlled:

Configuration:

- Hardware including all inputs and outputs, drivers, and firmware
- Operating System (OS) Patch and Update
- Application installation, Stores and Updates
- Data, including Wipe & Lock
- Connections
- Camera Use

Encryption[8]

Vulnerability Management:

- Device modification (jailbreak/root)

[7] The charter of this TM Forum Catalyst is to identify the Pareto rule (80:20) for security best practices that deliver the greatest proportion of security effect from out of all possibly available security activities

[8] Considering the four levels of ISO/NIST assurance as a scale from ‘none’ to ‘all’ for encryption across all data or access it is appropriate to encrypt on a device for the protection of the organization

Overview

This document will attempt to provide insights in to some best practices that will give you the ability to manage your mobile devices securely for your workforce. While MDM is a relatively new term, the concept is not, and it's important to begin with a clear distinction between past and present best practice in MDM. Research in Motion (RIM) has had a Blackberry Enterprise Server (BES) server for a long time that controls users' access to the web, applications and even pushes policies to BES attached Blackberry devices. In the less controlled world of iOS and Android, a different MDM solution is required.

It is up to each organization to enforce the policies that they want applied to the devices. As with any security solution, it is necessary to look at the risks to the actual operating business environment and not blind adherence to compliance standards when designing an operational and cost-effective solution. Once the risks are assessed[9], and appropriate solutions determined, you can then look at the KPI's that you may want to develop or use for management of the solution.

Cost is a significant factor in MDM, not just because of the technical complexity of the solutions, but because of the sheer volume of mobile devices that must be considered, all of which are more portable, inherently less secure and less secure-able, and of a shorter lifespan than other devices with organizational data or access. Processor capacity and storage are limited, which can affect the choice of security solutions significantly in terms of the impact on day-to-day productivity and convenience solely for the sake of security. Lastly, user behaviour is harder to control than ever before on this class of device, especially if the device is not owned by the organization, but by the user, and the primary contracting with the carrier is done by and controlled by the user.

[9] These would be the normal ongoing output of a vulnerability management program in a mature organization, and specifically such assessments would be available to executives and other decision makers in planned advance of the need for application of any new or enhanced solutions in a customer-use environment, as per proper ITIL release and change management practices

Key Security Attributes Detail

In this section we will discuss the attributes pertinent to mobile device security, as distinguished from general device security.

Hardware

A key assumption for security is that the organization can control the devices. Through this control, the organization can also guarantee itself the ability to secure access and data. As a reader of this document, if you don't have control over the hardware, you will need to use both Appendix A and Appendix B in this document to use as additional guides; you can assume less to be safe and secure than those organizations that control the hardware.

This is in large part because you have now lost the legal support of the carrier. In some cases and nations the carrier is legally restricted in what actions they can take on the organizations behalf without the explicit approval (and in some cases, direct and active involvement) of the device 'owner'. The 'owner' of the device is presumed in this case to be an employee or contractor of your organization using BYOD for a mobile device (of any form factor).

Without the carrier's ability or desire to be compelled, gaining the ability to immediately take any action to protect data or access on the device without the direct and active participation of the user becomes operationally impossible. Such coordination with employees and contractors can be done quickly and following proper processes under signed agreements between the involved parties, but not so quickly as central control can be exercised. Moreover, if there is disagreement between the employee or contractor and the organization, specifically if bench warrants or other instruments are required to compel a device owner to take action to protect organizational data or access, the attack will be long over before such compulsion can be effectively brought to bear.

Therefore, our conclusion about what is the most important aspect for hardware in mobile device security is 'Who Controls It?' If your organization cannot control the device being used to store your data or access your systems, then you will have to explore strategies of limiting exposure through containerization, restriction of access, and the installation of software to allow some degree of partial access while partially restricting the list of threat vectors described in Appendix A. The complexities of security for hardware under BYOD are magnified exponentially, and instead of a 'controlled or uncontrolled' measure of success, a scale of control as follows becomes relevant:

- Control of the Device
- Influence / Partial Control over Device Configuration and Settings
- Supervision / Approval Gate which is at least procedurally enforceable
- Auditability / Transparency of the configuration and settings on the device
- Detectability / Partial Transparency of the configuration and settings on the device
- Monitoring / Partial Detectability of the configuration and settings on the device

Fortunately, some TM Forum members already offer technological solutions of varying scope and effectiveness[10], and it is hoped that in the eventual Demonstration of the Catalyst Project supporting the creation of this QSG that such solutions will be included.

Security monitoring is closely related to hardware, and comes down to one question: how low can you go? Appendix A again provides a guideline for what must be monitored, but how all of these things will be monitored by an organization is outside the scope of this QSG.

Device Operating System

Device Operating Systems are ranked by the industry as to their innate degree of security; this is a standard consideration of Vulnerability Management for Security Design. If an organization uses an insecure OS, whether because it is more prone to malware than another, or because the OS is not under control of the organization, then understanding the amount of insecure OS devices in the enterprise gives one useful insight into the real risk level for the enterprise.

This knowledge is critical for scoping an audit of devices attached to the network, and in choosing applications to be used with these mobile devices. For example, if your population of mobile devices is largely centrally-controlled and updated, you want to create a webpage coded to provide certain business information only to your centrally controlled devices, and more limited information to other devices. Having this ability affects what work-flow options are securely available and what user-convenience features are securely permissible.

Malicious applications that are installed on mobile devices within insecure OS could be used to steal information from your organization's network, or from your users directly in a targeted attack. Users may be tricked into clicking on links in SMS messages to download applications and email messages that contain further malware, in a multi-stage exploit.

Operating System Patch and Update

As more devices become available from different vendors it is increasingly difficult to track what revision of OS they are running and from what source that version originates. Updates to the operating system on the smart phones are sometimes now in the users hands or the hands of the OEM device manufacturer. One specific example is the notion of a device 'image' that is certified by the organization. An equivalent concept is OS updates to a user's laptop that are started remotely by administrator tools and forced to be performed over organizational VPN. In general, methods and risks are less certain when attempting to mandate updates on a mobile computing device provided 'through' a telecommunications carrier. If the organization is going to exert an equivalent degree of control over mobile device version[11] and method of update[12], the methods required are more complex[13].

Knowing the revision level of Operating System that the smartphone is operating on is critical, and it's source. There have been known vulnerabilities in certain revisions of OS;

[10] Example: Cisco 'Borderless Networks' BYOD mobile device security solution

[11] Including source, especially necessary to record if the organization doesn't directly control the update and isn't able to exclude unapproved updates from being made to the device (by the user or by a malware exploit)

[12] Secure/approved application stores possibly including device OEM stores, but excluding other 3rd party stores

[13] And the tools for their administration in general not fully available from the OEM or other certifiable source

understanding the revision level the user population is currently using is critical in determining which devices you can allow to attach to the organizational network or to house organizational data. Key Performance Indicators (KPIs) for OS are Age and Source.

Application Installation, Stores and Updates

For Security, an enforced installation of certified updates from an authorized source is best, and to prevent installation for all unauthorized sources. In practice, this can pose such an onerous restriction on the use that the organization is forced to consider securing alternative update mechanisms. The next most secure method is a configuration that is pushed to the user, but is executed at the user's discretion[14]. User-requested configuration creates a security risk and a need to prevent the user from using an un-authorised source through intent or ignorance, as does the inability on the part of the organization to prevent a user from performing an unauthorised update, download or installation[15].

Users can update software on the smartphone as well as updating the operating system software on the smartphone unless this can be restricted by the organization. Using non-authorized Application Stores can introduce unwanted issues into your enterprise[16]. Using an MDM solution can help to limit access to unauthorized App Stores. Use of file sharing applications should be limited where possible to prevent data loss. Patch management plays an important role in assuring the security of the mobile enterprise. Making sure that you are running the most up-to-date version of operating system on your smartphone should be a priority for your MDM solution.

Lightweight v. heavyweight applications are also a specifically relevant security concern, especially with regards on-board data storage. Client-based concerns are obvious to anyone that's ever used an application store, but HTML5 is very much a protocol-based solution for so-called 'client-less' solutions, with unique security benefits but with the risks[17] of data left in cache on a BYOB device under a SaaS model.

Virus-protection is as necessary for mobile devices as for any other device, and the differences in susceptibility of the various major mobile device platforms and the various tools for the management of this vulnerability are widely available in industry publications.

[14] And perhaps can only be postponed for so long and still allow proper function, which period can be made quite short and still be reasonable in the case of urgent security updates

[15] It is especially important to prevent user rights from having 'silent' update potential, where a compromised device can be forced to download further exploits without the knowledge of the user or the organization

[16] This is not BYOD; it is actually corporate-owned devices that are used.

[17] Compensated by outsourcing of the risk in turn for an enterprise-grade SLA by some organizations, a valid option if the contracted provider of the SaaS service can be held adequately accountable in combination with insurance to protect the organization from a breach, and if such are less expensive than an organizational MDM solution when considering potential impact to brand from publication or litigation of security issues

Data, Wipe and Lock

Monitoring device and data manipulation on the device and the ability to control same is inherently more secure. The most important case it the need to destroy at least the data on the device and its ability to access secured organizational resources, irretrievably[18].

The ability to lock and/or wipe smartphones is important for lost and stolen devices. This may be triggered by a simple detection mechanism, like entering a password incorrectly too many times. Using the MDM solution to push and enforce policies to the smartphone gives the enterprise more control over the mobile device where such ability exists.

The last key concept is 'containerization' of the organizational data on the device, with control over that container able to be exerted directly by the organization[19] without the user's involvement.

Connections

Only authorised connections are preferable for security, but in operational practice users must travel extensively or even globally with the assurance that the organizations data and access will be protected. Certificates based authentication[20], enforceable VPNs (virtual private network), and appropriate on-board protections for the device can help to level the risks inherent in diverse wireless, cellular and satellite, NFR and other connections.

Client based connection-protections (like certificates) can improve security.

Protocol-based connection protections (like HTTPS) can improve security.

Device-based connection protections (like firewalls) can improve security.

Combining these mechanisms for connection protection is better than any one alone.

Logical connections to ESBs (Enterprise Service Bus) or similar constructs that are not standards-compliant introduce an unpredictable order of magnitude of risk and are not properly within scope for this document. The team identified a number of interesting examples that would be good to see the TM Forum test, perhaps in cooperation with MITRE, OWASP, CERT, NIST or another organization, after which it should be reviewed as to whether the best interests of security would be served by publishing the results, or whether the safeguards for all the exploits discovered should first be deployed before announcement.

Lastly, each custom integration brings a separate order of magnitude greater risk. The core products for all service components receive at least an order of magnitude greater effective testing than customizations, so each added integration adds another order of magnitude of 'less tested' and less quantifiable risk to the organization.

[18] In some cases rendering the device unusable, even incapable of at most e911 use, possibly permanently

[19] Note the by preventing the organization from having access to the device via wireless or cellular connection and then extracting the data from the device can still be performed by a hacker unless the device has a 'self-destruct' on the container after a set period of time without verified connection to an approved network

[20] Implies secure and authentication certificate distribution and management is maturely in place

Encryption

On-device encryption is an important aspect of mobile devices. Drive level encryption is one alternative, but sometimes it is preferred for security to separately encrypt some data classes and classes of access on the device for added protection. Backups are a complicating factor for encryption. Data that is backed up off of the device should be encrypted to protect email, contacts, and other important data on the device. Other things to consider:

- Forcing HTTPS backups
- Data on storage media
- Data in transit
- Permitted applications (whitelist)
- Prohibited applications (blacklist)
- ENEPID – Everything not expressly permitted is denied
- EEDKW – Encrypt Everything Destroy Key Wipe
- BPAW - Bad Password Automatically Wipes
- Magnetic v. flash/solid state storage security
- Unpowered/low powered and/or unconnected device and data security
- Geo-location and Mobile Location exploits
- Data loss prevention
- Cross-containerization exploits (where applicable)

Strong alphanumeric and other normal password precautions apply unquestionably with equal force to mobile devices, but the most important topic related to passwords for this document is how they are stored on the device. Encryption and other protections for passwords are vital to prevent mobile devices from being a vector of attack information for penetration attempts on other portions of the enterprise by compromising the information from the mobile device itself. Encryption for the network connections via VPN, WiFi or another type of encryption must be considered for sensitive documents and communications.

Vulnerability

Every member of the team agreed that it was of no use to attempt to reinvent the several best-practice international references from respected organizations such as CERT, SANS, NIST and other. We have referenced this elsewhere in this document, with our thanks to those organizations.

Carrier practices

Carriers work to provide customers with a wide range of choice for mobile devices. That means working with mobile device vendors to ensure that the mobile devices work with the services that are being offered by the carrier. Firmware changes and interface changes may bring unwanted security issues to a device. Fixes to issues on mobile devices are often patched by the vendors themselves. Some carriers have the ability to push down patches to phones, however, some device vendors are now handling the updates to the OS themselves. The TM Forum and similar groups have some of the best opportunities to propose commercially reasonable common standards from a perspective without commercial self-interest or other relevant bias to affect the recommendations. Carriers can help with securing communication channels as well. Some vendors work with carriers to provide services like this[21].

Devices Modification (Jailbreak/Root)

Knowing if you have modified devices in the enterprise is an important factor. Jail-breaking, rooting[22] and unlocking[23] are the terms for the three most relevant[24] specific threats. As an example, when a hack came out for an older version of iOS, specifically the way it handled PDF files, it enabled hackers to create a way to 'jailbreak' the smartphone, allowing access to other (unauthorized) App Stores, exposing the device to other threats.

Applications that are downloaded from unauthorized sources allow for data leakage and enabling easier malicious behavior like premium SMS fraud, Long Distance (LD) Fraud, SMS Spam and Email. If an absolute necessity for your organization, separate management of encryption keys limits risks on modified devices and restricts data and access.

[21] Using PIN communication on Blackberry devices.

[22] Jail-breaking and rooting allow downloading from unauthorized sources for OS or application updates

[23] Not locked to a particular carrier

[24] Differentiated from the ability of a malicious party to compromise a single device electronically through direct means, which has always existed and is geometrically compounded in mobile devices by the increased number of microprocessors, radiOS, and other components that can be compromised

Metrics

Most metrics for mobile devices are similar to metrics for other devices. However, the rate of obsolescence, ubiquity of access, frequency of updates, degree of control over user downloads and many other vectors are both high risk and higher occurrence than for form factors of business devices that were used in the past[25].

Configuration

Hardware

- % of devices owned by the organization vs. BYOD devices
- % of devices where configuration is controlled by the organization (if BYOD is used, the configuration of the means of access to company resources and the local storage of company data
- % of devices where changes in configuration or installed applications can be detected by the organization

OS

- % of devices where lock after a short period of non-use and re-entry of login credentials is enforced
- Average number of days that the device configuration has not been updated[26] since the last release[27]. In general, more releases are better.
- % of devices where source of upgrades is controlled
- % of devices under central[28] and remote administrative controls[29]
- % of devices with enforced physical port protections[30]

Applications

- % of devices where source of applications is controlled
- % of devices using on-device or Security applications[31]
- % of devices with enforced virus detection and prevention
- % of devices and malware detection and blocking (IDS & IPS)

Wipe & Lock - Containerization

[25] Terminals, desktops, laptops

[26] Presuming that the update at least confirms and overwrites proper configuration for security, and if deviations have not been detected before, preferable captures those deviations during the update process

[27] For connected systems, manual update may be required, like a CD or DVD in-dash update for a vehicle system

[28] Central management is generally preferable to a heterogeneous solution of third party partial solutions

[29] In theory, user administered devices would prove less costly for the organization to support, but in practice the dubious quality thereby attained typically means that performance and cost-effectiveness are, like security, improved by central administration in a more predictable fashion

[30] Including variations in lockdown by device type, considering specifically the DISA STS guides

[31] Ex: ice cream sandwich(Android 4.0) facial recognition, Motorola Atrix fingerprint scanner, palm vein and retinal scanners, noting, however the defence-industry guidance that says biometrics, unless observed, are still not fully secure

- % of devices where the organization can with certainty wipe and lock the data on the device.[32]
- Number of devices where the organization can wipe and lock the data on the device.
- If BYOD is used, % of devices that have confidential corporate information and intellectual property.[33]

Encryption

- % of devices with removable or hardwired encrypted
- % of devices using encryption for organizational traffic
- % of devices using separate encryption by application/access

Vulnerability

- Number of security evaluations preformed per year[34]in context with business requirements, based on best practices and standards.[35]
- Longevity of the security program of a vendor or partner for mobile devices specifically, not just security in general[36]
- Annual re-training of staff depends on vulnerabilities[37] unique to both the work and the device[38]

Modified Devices (Jailbreak/rooting)

- % of devices for which modification via jailbreak or rooting can be detected[39]

Connections

- % of devices where the organization has control over connections permitted to and from the device[40]

[32] Please see Appendix C
[33] Please see Appendix C
[34] Evaluations can be performed either annually(1), quarterly (4), or monthly (12)
[35] Impact for different business models and customers changes security requirements significantly
[36] Please refer to the TM Forum Human Factors Security QSG
[37] For a more comprehensive list of risk behaviors please refer to the TM Forum Human Factors Security QSG
[38] E.g. 'don't interact with SMS', don't give your device to someone else to configure, don't click on links in suspect e-mails or SMS's (for good security behaviors look at SANS/NIST)

[39] By examining the OS and looking for other expected pattern deviations
[40] An example could be using a VPN for communications.

Appendix A: Elements Required to be Controllable[41] for Security

All physical input, power inputs that also accept data, and memory card slots/ports, including:

- Wi-Fi / Bluetooth / Near-Field Communication / Any other Radio, specifically including:
    - Serial port
    - Headset
    - Hands free
    - Phone book
    - In vehicle
    - In-dock
    - Discoverable
- GPS Receiver
- Infrared (legacy)
- Microphone
- Camera
- Other peripherals (card readers, biometric devices, sensors, bar code scanners, etc.)

Processes:

- Over-air provisioning
- USB tethering
- Auto-connect to known Wi-Fi or other connections
- Personal hotspot/any kind of broadcast
- VPN split tunnelling
- Audio Recording
- Video Recording
- Location Services
- SMS, MMS
- USB Mass Storage Mode
- Availability of information on the device with the device locked – convenience features
- Security of Emergency/E911 services on the device
- Availability of data outside of application (example, contact info outside contact app)
- Remotely/centrally enforced configuration parameters
- Device unlock, with alternative methods including patterns, biometrics, passphrases and combinations, complexity, verifiability
- Duration of activity before device lock
- Web proxy URL
- Remote disable and wipe (date only, OS + data, is the device usable for E911 afterward, or dead?) % of devices supporting IMS, 3GPP, GSMA, which implies RCS support
- % of devices supporting IMS, 3GPP, GSMA, which implies RCS support

[41] Able to be enabled or disabled in a controlled fashion by the organization, carrier or user

Appendix B

Bring Your Own Device (BYOD)

Bring your own device (BYOD) is the ability to use a personal device on a corporate network. It allows users to carry one device instead of multiple devices. It allows businesses to save the cost of giving devices to users for business use. The promise of BYOD is business cost savings, while allowing users the freedom to use their device on the corporate network. The business could give access to corporate email and corporate files in a secure environment while the user may have to give up a little freedom on their device.

BYOD would be managed by policies pushed to the smartphone/tablet. This gives the ability of the business to manage the device appropriately. The business would have to have a little bit of control when it comes to the device; things like remote wipe and locking. This is managed by policies that will be pushed down to the device. Other things to consider are password/pin locking as well as Anti-Virus protection software.

Security will still have to play a role in securing the device. The device effectively becomes an extension of the corporate network. Password/pin locking is critical to securing the device. Some MDM solutions have the ability to create a separate secure container on the device that would be encrypted and allow for that section only to be wiped. Patching of mobile devices is another key area. If a threat or vulnerability is present, you need to be able to quickly patch these devices to mitigate the risk.

In order for BYOD to be effective, you will also need agreement from the user that you can have the ability to wipe and update the device as required. This could be as simple as having the user accept a terms and conditions document that tells them what the business can do to the device and a complex as yearly written test as proof of compliance.

Below is a list of things to consider when looking a BYOD comparing the difference between corporate devices and personal devices:

Company Devices

These are devices that the company pays for and allows you to use. Again, policies and procedures will help deal with most of the issue that will come out of this. Some types of things here that you may want to look at:

- Device manipulation policy
- Jail-breaking/rooting/unlocking policy
- Fair Use policy
- Downloading application policy
- Password/passcode lock policy

Personal Devices

People no longer want to carry two or three devices to the office. Having a BYOD policy in place will allow for users to have access to email and some applications via a web interface, or possibly on an internal app store. As mentioned earlier there are steps that should be taken to ensure the security of the environment if this is a chosen method of connection. Here is a list of some of the things that you can do to help in the personal device space.

- Enforce AV protection on the device
- Annual testing for policies
- Ensure that the device is up to date (latest patch level) before connecting
- Wipe and lock Policy
- Lost or stolen device policy
- Modification policy
- Password/passcode lock policy
- Privacy Policy
- Restricting the data stored on and the access provided to personal devices versus corporate owned and controlled devices (if any)
- Increased user security education if BYOD is used.
- Use of SaaS (Software-as-a-Service) instead of file transfer
- Preference for HTML5 applications in some cases
- Enforced use of company VPN
- Containerization
- Partial Encryption

Appendix C: Legal, Information Assurance and Classification

When talking about mobile devices, MDM, and BYOD there are considerations regarding the ability to wipe a device, the type of data that is stored on it and containerization.
TM Forum members and their customers operate across multiple geographies. Consequently, there are many jurisdictions that govern the legality of wiping a device, so it’s inappropriate for this document to discuss the legality of wiping a device. Furthermore, there could also be privacy implications to wiping a device that contains personal information as well as corporate information. In some jurisdictions where corporate devices include personal usage, there may be issues with wiping the device as well. Containerization may solve some of these issues. Since containerization separates the personal environment from the corporate environment, a wipe of the corporate container can be done without affecting the personal environment. Another important item to consider is the classification of documents. Some types of classification allow for public access and others do not. The company must define what it deems public, private, confidential, and in some cases intellectual property. Creating these definitions will help to provide guidance on when a device can be wiped and when there are potential issues.

Administrative Appendix

This Appendix provides additional background material about the TM Forum and this document. In general, sections may be included or omitted as desired, however a Document History must always be included.

About this document

This is a TM Forum Guidebook. The guidebook format is used when:

- The document lays out a 'core' part of TM Forum's approach to automating business processes. Such guidebooks would include the Telecom Operations Map and the Technology Integration Map, but not the detailed specifications that are developed in support of the approach.
- Information about TM Forum policy, or goals or programs is provided, such as the Strategic Plan or Operating Plan.
- Information about the marketplace is provided, as in the report on the size of the OSS market.

References

Australian Defence Signals Directorate Top 35 Mitigation Strategies: http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
SANS 20 Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines: http://www.sans.org/critical-security-controls/
Verizon 2011 Data Breach Investigations Report: www.verizonbusiness.com/about/events/2012dbir/index.xml
TM Forum's Business Process Framework (eTOM): www.tmforum.org
Security Compliance Audit Automation: http://www.tmforum.org/BusinessAgreements/SecurityCompliance/48393/article.html

Document History

Version History

Version	Date	Author	Comments
0.1	June 14	Blake Lindsay, Bell Canada	Draft
0.2		Mike Carpenter, TOA Technologies	Draft

0.3		Blake Lindsay, Bell Canada	Draft
0.4		Mike Carpenter, TOA Technologies	Draft
0.6		Blake Lindsay, Bell Canada	Draft
0.63	July 30	Mike Carpenter, TOA Technologies	Draft – content and cross-analysis from Baltimore and references added
0.7	Aug 11	Blake Lindsay, Bell Canada	Made minor changes to the document
0.72	Aug 16	Blake Lindsay, Bell Canada	Made major modification to the structure and flow of the document
.7x - .9x	Aug/Sept	Blake Lindsay, Bell Canada, Mike Carpenter, TOA Technologies	Factored in team comments, added BYOD section, carrier practices and metrics
1.0	Oct 2	Christy Coffey	Clean-up for formal release.
1.1	Oct 10	Alex Hamerstone, TOA Technologies	Additional Clean-up
1.2	24 Oct 2012	Alicja Kawecki	Minor formatting/cosmetic corrections prior to posting and Member Evaluation

Release History

Release Number	**Date Modified**	**Modified by:**	**Description of changes**
<<Release Number >>	DD/MMM/YY	<<name>>	Description e.g. first issue of document

Company Contact Details

Company	Team Member Representative
Bell Canada	Blake Lindsay
TOA Technologies	Mike Carpenter
MITRE Corporation	Susan Schreiner
Ministry of Defence, DSTL	Martin Huddleston

Acknowledgments

To Blake Lindsay, Bell Canada and Martin Huddleston, DSTL, our executive sponsors, ***many thanks for your guidance, leadership, and support.***

This document was prepared by the members of the TM Forum Cyber Ops for Security Management project team:

Mike Carpenter, TOA Technologies, Editor and Team Leader
Blake Lindsay, Bell Canada, Editor and Executive Sponsor
Christy Coffey & Jenny Rottinger, TM Forum

Additional input was provided by the following people:

BC Eydt, DISA
Susan Schreiner, MITRE
Alex Hamerstone, TOA Technologies
Pamela Abbott, Brunel University
Larry Frank, Booz Allen Hamilton
Patrick Curry, BBFA