Sleepless Nights Over BYOD
MDM Considerations for the Government IT Leader

Background

Businesses and governments largely drive the adoption of information technology (IT) – that is until 2011. Many experts agree that 2011 saw a tipping point that reversed the trend. Where employees once followed whatever businesses and governments prescribed to them for IT, employees now are the early adopters and are forcing businesses and governments to contend with the influx of personal devices brought into the workplace not only for personal use but also for work. Nowhere is this more prevalent than with mobile devices, including tablets and smartphones. So significant is this phenomenon that it has been dubbed the "bring your own device (BYOD)" movement.

The use of personal mobile devices in the workplace has caused sleepless nights for many IT professionals. Where once corporate- and agency-issued mobile devices could be configured for secured access to the network, rogue personal mobile devices are connecting without much regard to network security. While network security tends to be of primary concern, there are a number of other considerations when addressing BYOD, and they include both technical and legal factors.

Purpose

This white paper will outline both technical and legal considerations for the government IT leader when developing a strategy and plan for BYOD, as well as provide a shortlist of solution providers. It is not intended to be a detailed analysis but merely a straw-man document to be used for further discussion and analysis.

Technical Considerations

Until recently, government IT agencies had significant control over mobile devices, especially since all of them were procured, provisioned and managed by the agency. Unfortunately, the arrival of unmanaged personal mobile devices introduced a new threat to the network. There was no foolproof way to ensure the devices were secured like agency-issued devices. Agency-managed devices like BlackBerry devices were often secured using Research in Motion's BlackBerry Enterprise Server (BES). In order to ensure the same level of security on personal mobile devices, government IT agencies should consider the following factors.

> **Security/Access Controls:** Similar to other computing resources, mobile devices should be guarded against unauthorized access. Accordingly, strong password controls, inactivity timeouts, screen locks and failed password lockouts should be reviewed on the mobile devices.
>
> **Remote Lockout/Wipe:** In the event the mobile device becomes lost, the ability to remotely lock or wipe the device is helpful. Such capabilities should be considered to continue to safeguard against unauthorized access.

Encryption: Government agencies that manage sensitive data such as HIPAA or PII may want to consider encrypting the data on the mobile devices. This would render the data useless if the device is lost or stolen and places the government agency in the best position to be in compliance with certain legal requirements.

Device Management: With the variety of mobile devices being introduced, the management of those devices can quickly get complex, including patching every device and updating virus definitions. Government agencies may want to consider automating this function to lessen the burden on IT staff.

Data Management: Depending on the requirements, it may be too risky to allow data to be stored on the mobile device at all (especially if encryption fails or is not supported). In that event, the data may need to be configured for view-only access and retrieval.

With the variety of mobile devices being introduced, it is unlikely that the existing Mobile Device Management (MDM) solution used by government IT agencies will be able to accommodate all of the devices. It then stands to reason that the new MDM solution ought to be able to support a variety of mobile devices with diverse operating systems and carriers.

Legal Considerations

With agency-issued mobile devices, ultimate control of the device rested with the agency because, after all, the devices were owned by the agency. Subsequently, ensuring the mobile devices were compliant with agency policies and procedures was relatively trivial. With employee-owned mobile devices, this task becomes less trivial – to what extent does the agency have the authority to exert control over personal mobile devices? Does the agency have any authority to dictate what applications can and cannot be downloaded and installed on the device? If necessary, can the agency remotely wipe the device, including any personal pictures, videos and songs belonging to the employee?

Many private-sector businesses address these questions by requiring employees to sign user agreements before it will allow personal mobile devices to be connected to the network. These agreements, in general, allow the businesses to access the device to review it as needed or to remotely wipe the device with everything on it should it become necessary. Employees who refuse to sign the agreement are denied access to the network using their personal mobile devices. And, indeed, some have refused to sign, opting instead to carry two mobile devices: one for work and one for personal use.

Another legal issue to consider is liability, particularly for agencies that manage sensitive data. Private-sector businesses work extensively with their legal team to review their liability coverage in the event they have a data breach. Often times, BYOD policies increase liability insurance premiums, particularly around data/security breach coverage.

Yet another potential legal consideration is overtime hours. With employees able to access agency email or data on personal mobile devices afterhours, it builds a case for overtime hours

for qualified employees. While this does not apply to all employees, the few that it does apply to warrant some consideration. Certainly if overtime hours are justified, then this is of no concern. However, in the cases that they are not, many organizations simply program their MDM to suspend email and data access after hours for employees that do not need the access.

MDM Solution Providers

A number of technical solution providers have emerged to address the BYOD movement, particularly around the MDM space. Gartner offers some very useful guidelines on capabilities to rate and review and provides its own detailed analysis and rating available directly from its website (www.gartner.com). Several critical capabilities are used by Gartner in evaluating various MDM solutions, including:

Device Diversity: The degree of diversity in mobile devices and mobile OS platforms that the considered MDM product can handle.
Policy Enforcement: The ability of the MDM product to enforce policies around eligible devices, applications, mobile communication expenses and separation of personal versus corporate content.
Security and Compliance: A set of mechanisms to protect corporate data on a device, corporate backend systems and preserve compliance with regulations.
Containerization: A set of mechanisms to separate corporate from private content (data, applications) on a device and apply a range of actions to control the corporate footprint.
Inventory Management: A set of mechanisms to provision, control and track devices connected to corporate applications and data.
Software Distribution: A set of mechanisms to distribute applications and software upgrades to mobile users over the air, avoiding tethering to a PC.
Administration and Reporting: Capabilities for IT administrators to manage mobile deployments and users.
IT Service Management: Capabilities to grant mobile service levels to mobile users.
Network Service Management: Specific capabilities to monitor and optimize costs.
Delivery Model: Ways to deliver MDM capabilities to customers (e.g. on-premise, hosted or cloud).
Aside from these capabilities, a government agency's use case must also be considered. Will employees access emails only, or will they also access other data on their personal mobile devices? Is the data being accessed highly regulated and protected or not? Once again, Gartner offers a very detailed analysis, review and rating by use case.

For government agencies as well as many private-sector businesses, it is most cost effective to use hosted or cloud-based MDM solutions, instead of building the capability in-house especially with the quickly changing landscape around mobile devices. Moreover, hosted or cloud-based solutions typically do not require the substantial up-front investment that on-premise solutions do. With that in mind, vendors to consider include: AirWatch, MobileIron and Sybase. Other notable vendors include: BoxTone, Excitor, FancyFon, Fiberlink, Mobile Active Defense, Tangoe and Zenprise. Many of these vendors provide additional useful resources on their websites, including case studies, white papers and client testimonials.

Conclusion

The BYOD movement is here, and it's here to stay. Government IT leaders must strategize and plan now in order to accommodate and manage the influx of personal mobile devices. While there are numerous technical and legal factors to consider, the employee must not be overlooked. IT leaders who overlook or ignore the human factor will inevitably find their jobs that much harder. Time and time again, employees will circumvent IT policies and procedures if they are cumbersome and hinder work. It is in the government IT leader's best interest to work with employees and take into account the human factor, while developing an MDM strategy and plan that reflects all technical and legal requirements.

Links and Resources

1. US Department of Health & Human Services HealthIT Mobile Devices Roundtable: Safeguarding Health Information http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__mobile_devices_roundtable/3815
2. FDIC Mobile Banking: Rewards and Risks – http://www.fdic.gov/regulations/examinations/supervisory/insights/siwin11/mobile.html
3. Gartner Critical Capabilities for Mobile Device Management (ID Number: G00213877) – http://www.gartner.com
4. Gartner Magic Quadrant for Mobile Device Management Software (ID Number: G0021101) – http://www.gartner.com
5. Gartner Survey Shows BYOD is Top Concern for Enterprise Mobile Security – http://www.gartner.com/it/page.jsp?id=2048617
6. HIMSS Mobile Privacy & Security Toolkit – http://www.mhimss.org/resource/mhimss-mobile-privacy-security-toolkit
7. Intel Healthcare Information at Risk: The Consumerization of Mobile Devices – http://www.mhimss.org/resource/healthcare-information-risk-consumerization-mobile-devices
8. NIST Guidelines for Managing and Securing Mobile Devices in the Enterprise – http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf
9. The White House The Mobile Opportunity – http://www.whitehouse.gov/blog/2012/01/12/mobile-opportunity