SearchConsumerization

E-Guide

MOBILE DEVICE MANAGEMENT CHECKLIST

TechTarget

A WELL THOUGHT-OUT MOBILE device management strategy is a key ingredient for any successful mobility deployment. This expert E-Guide highlights a mobile device management checklist. Additionally, hear from a panel of experts who detail how to create an enterprise MDM policy and implement a comprehensive MDM system.

MOBILE DEVICE MANAGEMENT CHECKLIST

Lisa Phifer

Ideally, IT should be at least aware of every smartphone and tablet used in an organization, from activation to retirement. Accomplishing this requires a cohesive plan for mobile device management.

As business use of smartphones and tablets continues to grow, inadequate IT oversight and control is having negative effects. Up to one-third of companies acknowledge that smartphone use is being hindered or slowed because IT admins cannot manage the devices to the extent they would like, according to a 2012 Osterman Research study; the situation is even worse for tablets.

MOBILE DEVICES: OUT OF SIGHT, OUT OF MIND

For the past decade, IT departments turned a blind eye to mobile handhelds, believing that cell phones were too limited and PDAs saw too little use to warrant attention. But today's increasingly powerful converged mobile devices have blown past both barriers, leaving IT in the hot seat. After all, you cannot secure what you don't manage, and you cannot manage what you don't see.

Mobile device management (MDM) can help your business plug this gaping hole by enabling remote visibility and control over smartphones and other handheld devices carried by your workforce. But MDM can also be a frustratingly vague term, applied to a diverse collection of products. The first step is to define precisely what you want an MDM system to do for your mobile workforce. The following checklist can help you identify your needs and common MDM capabilities that could address them.

MOBILE ASSET INVENTORY

Clearly, your MDM must maintain a list of devices to be managed -- that is, your mobile asset inventory. But what should your inventory include, and how will it be maintained?

- **Device inventory:** What physical details do you need to track? Beyond the basics (device ID, hardware model, firmware version), an MDM can help you record and report on related assets like wireless adapters and removable memory.

Home

Mobile device management checklist

Ensure mobile device security through a mobile device management policy

- **Inventory classification:** How do you want to group those mobile devices? For example, an MDM might auto-classify your devices by mobile OS/version or state (e.g., unknown, authorized, provisioned, decommissioned).

- **Inventory maintenance:** How do you want to update your inventory to reflect adds, changes and deletes? An MDM might be used to periodically poll devices, check for changes at network connect, or carry out admin-initiated audits.

- **Physical tracking:** Do you need to know not just who carries each handheld but precisely where that device is located? With many smartphones now supporting GPS, location-based MDM features become feasible.

- **Database integration:** Do you already have inventory systems that manage other assets (e.g., desktops, phones)? If so, you may want to integrate managed mobile device records into a common database using inventory exports or reports.

MOBILE DEVICE PROVISIONING

Managing a device through its lifecycle begins with activation and provisioning. How will each new device become an authorized, capable member of your handheld fleet?

- **Supported platforms:** Device management depends on many characteristics, including operating system and vendor/model/version. What platforms (e.g., Apple iOS, Google Android, BlackBerry OS, Microsoft Windows Phone) and minimum models/versions (e.g., Samsung SAFE devices running Android 4+) must you support? Make device-independent management choices wherever possible and practical while establishing baseline acceptance criteria for specific business uses (e.g., hardware-encrypted devices with remote find/wipe capability).

- **Device registration:** How will you enroll mobiles to be managed? MDMs can help administrators register company handhelds (e.g., directory add) or let users register their own devices (e.g., enrollment portals), or some combination thereof.

- **Agent activation:** How will MDM software get installed and activated on each new device? Some mobile devices ship with native MDM (e.g., Apple iOS, BlackBerry OS); others may require employees to visit an app store or an IT-managed Web portal to download and install an MDM agent. The latter is often accomplished by texting or emailing a URL to each enrolled device to complete over-the-air installation.

- **Device configuration:** How will you override factory/carrier defaults? For example, you might want to require passwords, add registry keys, or rewrite menus to eliminate non-business applications. MDMs can apply your "standard config" to each device after initial activation or hard reset.

MOBILE SOFTWARE DISTRIBUTION

Many MDMs go beyond device inventory and configuration, providing tools that deliver and update mobile applications. This may not be Job 1, but it should be a close second.

- **Software packages:** How will you bundle related applications for purposes of configuration and delivery? MDMs can help you define and deploy those packages, helping to resolve platform, memory, and application dependencies.

- **Application distribution:** Do you want software and updates to be downloaded from public app stores (e.g., Apple iTunes, Google Play), pushed transparently to managed devices by an enterprise app store, or some combination thereof? Each mobile OS enforces its own rules regarding user permissions required to install and update apps, but MDMs can help IT automate related processes (e.g., prompting users to install required public apps).

- **Mobile optimizations:** Must your strategy accommodate unreliable or limited WANs? Some MDMs offer compression, incremental updates, and bandwidth management (attempting or resuming installation only over fast, low-cost links).

- **Change control:** How often will your mobile applications need patching or update? Define how deployed packages will be maintained so that changes are applied without resulting in user pain or weeks of effort to fix failed updates.

MOBILE SECURITY MANAGEMENT

On handhelds, device and security management tend to converge. Many MDMs offer basic security features that are missing from mobile OSs or related to device tasks.

- **User authentication:** How will you authenticate users before granting access to mobile devices? Some MDMs can be integrated with enterprise directories while addressing mobile needs like network-disconnected authentication.

- **Password policy enforcement:** How many login attempts will you allow before requiring reset? Can emergency calls bypass authentication? Many MDM agents can enforce these and other password policies that go beyond OS-provided PINs.

- **Remote device wipe:** Do you need the ability to wipe clean a remote mobile device? For example, an MDM can often delete data or hard-reset a lost smartphone on next server connect or upon receipt of an SMS “kill pill.”

- **White/black lists and device restrictions:** An MDM involved in application management may require certain business applications and ban other applications. Similarly, an MDM that controls device settings can help you disable risky interfaces and wireless options.

- **Secure communication:** How will sensitive MDM traffic (e.g., configuration changes, software packages) be protected? Some MDMs provide their own secure channels rather than relying on OS or third-party protocols.

MOBILE DATA PROTECTION

Data just might be the most sensitive corporate asset on any mobile handheld. MDMs can help you preserve and protect that mobile data.

- **Data encryption:** Do you want to enforce policies that use hardware or software encryption to prevent unauthorized access to data stored on mobile devices? Most contemporary mobile devices provide hardware encryption capability; others can enforce your policies by installing or activating third-party encryption (e.g., secure data lockers, self-encrypting enterprise applications).

- **Backup/restore:** How will you prevent data loss when a mobile device is damaged or stolen? Most mobile devices support scheduled over-the-air backup of selected settings and content to a cloud backup service for subsequent restoration by authorized users. Consider whether you also need to back up enterprise application data to an IT-controlled backup server.

- **Data tracking:** Do you need to maintain an audit trail of corporate data copied to and from mobile devices? Some MDMs can control and report on sensitive files transferred during over-the-air synchronization or onto removable media.

MONITORING AND HELP DESK SUPPORT

Mobile device total cost of ownership can far exceed hardware/software purchase. Over time, MDM should pay for itself by reducing maintenance and support costs. How?

- **Self-help:** Can some admin tasks be cost-effectively shifted away from IT? Some MDMs offer self-help portals for user-initiated device enrollment, password reset or recovery, optional package download, and data restoration from backup.

- **Diagnostics:** When problems arise, what will your help desk need to see? MDMs can play a big role by providing not just intended settings but real-time status and health information (e.g., memory, battery, network connectivity).

Home

Mobile device management checklist

Ensure mobile device security through a mobile device management policy

- **Remote control:** When remote users need assistance, what can your help desk really do? Many MDMs include remote-control features (e.g., screen sharing) that let support staff interact with an off-site handheld in real time.

- **Audit and compliance:** Do you need to prove that mobile devices comply with your stated policies and/or industry privacy regulations? MDMs can help you automate remote assessment, remediation, and compliance reporting.

- **Activity reports:** How much insight will you need into mobile user activities, including interaction with business servers and networks? Most MDMs provide historical reports -- but look closely to see whether they capture what you need to know.

Your company probably does not need everything on this checklist, and any single MDM product is unlikely to cover all of these bases. Instead, treat this checklist as though it were a menu, introducing you to a foreign cuisine. Some considerations are simply variations on traditional desktop management needs, while others may be new and unfamiliar. Try a few MDMs to gain field experience with mobile user and device requirements before settling on an enterprise mobility management strategy for your workforce.

ENSURE MOBILE DEVICE SECURITY THROUGH A MOBILE DEVICE MANAGEMENT POLICY

Jenny Laurello

When members of the audience at the American Society for Association Executive's (ASAE) Technology Conference & Expo were asked how they created their mobile device management (MDM) policy, "We Googled it" was the primary answer, and this is not uncommon. Using a template and altering it for an organization's specific purpose is an increasingly standard practice for small and large companies alike that are taking the "why reinvent the wheel?" approach.

But Renato Sogueco, CIO of the Society of American Florists, chose a different path when creating his company's mobile device management policy.

"I wrote [our policy] from scratch. I listened to what we needed and created a policy that fit those needs. Before we had it, I felt powerless. These devices were invading our security. All of these small, shiny things. But guess what happens to small, shiny things that can do a lot? Aside from internal threats, these devices can get lost and stolen. We needed a way to reach out and physically touch a device if we needed."

Policy creation was essential for more than just allowing his organization's IT team to be able to "hit the nuke button," though, Sogueco said during his panel presentation, "Key Issues in Considering Mobile Device Policy and Implementation," during the ASAE conference last week in Washington, D.C.

"What made me develop a policy was change," he said. "It felt like I was continually taking punches with all of these new devices. First it was BlackBerry, then the iPhone and Android, then tablets. So I decided to proactively go on the offense. Doing nothing was no longer an option."

FRAMING THE MDM POLICY AND SYSTEM

A mobile device management policy is only as good as the sum of its parts, though, and even more important as a component of a larger mobile device management framework.

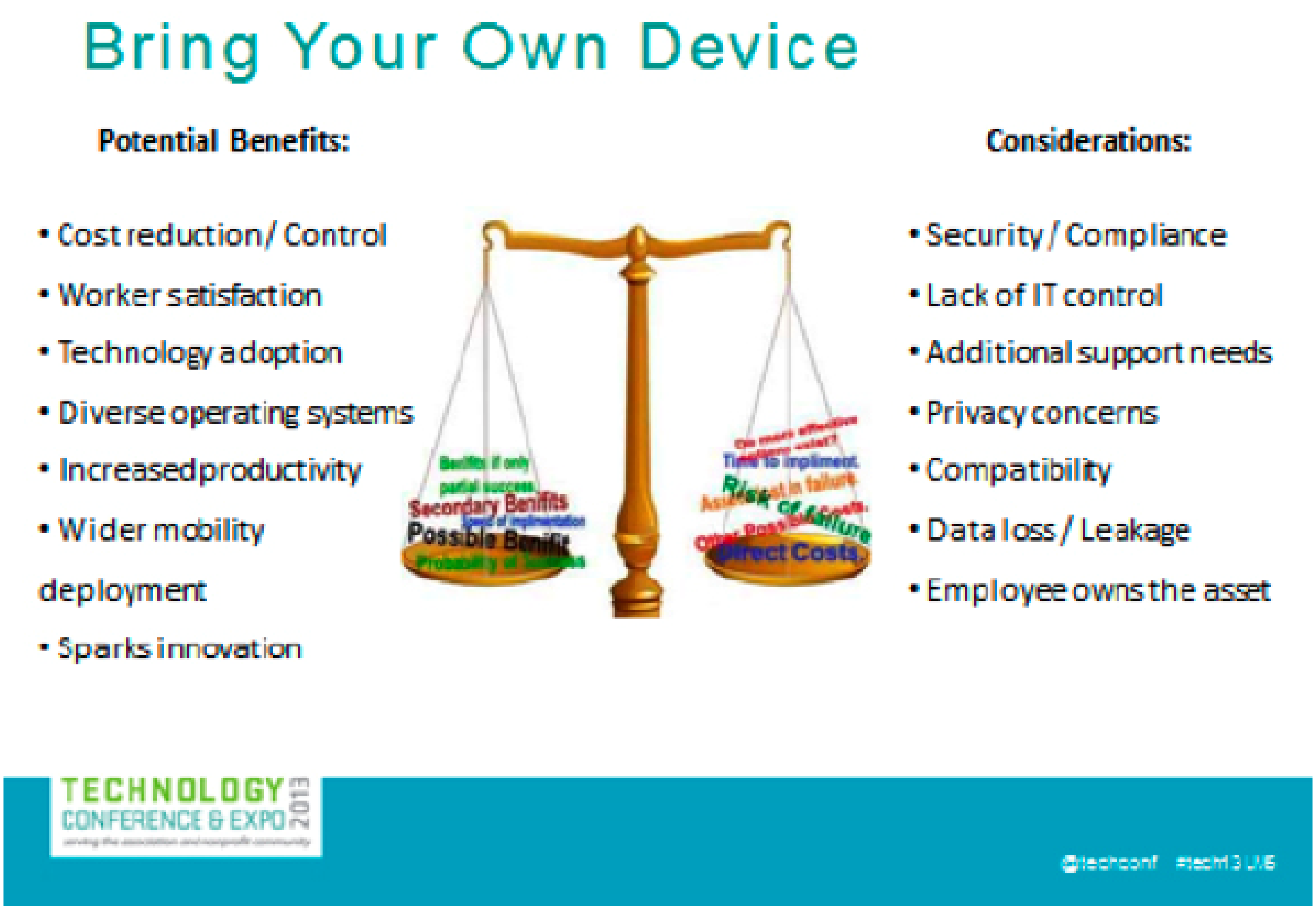
Larry Covert, director of IT for ASAE, spoke about the evolving scope ofMDM, highlighting the need to also focus on mobile content management and mobile application management.

"The MDM scope is growing all the time, and if these devices are on your network, you must look at them now, or it could end up costing you a whole lot more in the future." Covert also added that MDM is "beyond data loss considerations. You need to look at brand and organizational reputation."

Home

Mobile device management checklist

Ensure mobile device security through a mobile device management policy



Bring Your Own Device

Potential Benefits:

- Cost reduction / Control
- Worker satisfaction
- Technology adoption
- Diverse operating systems
- Increased productivity
- Wider mobility deployment
- Sparks innovation

Benifits if only partial success
Secondary Benifits
Possible Benifits
Probability of success
Time to implement
Risk of failure
Direct Costs

Considerations:

- Security / Compliance
- Lack of IT control
- Additional support needs
- Privacy concerns
- Compatibility
- Data loss / Leakage
- Employee owns the asset

TECHNOLOGY CONFERENCE & EXPO 2013

@techconf #techf13 LIVE

Figure 1: BYOD benefits and considerations

The panelists also touched on the necessary considerations when developing a bring your own device (BYOD) policy. While there are many benefits to the proliferation of employee-owned devices in the workplace, there are also many security, privacy and IT support factors to consider (see Figure 1). When faced with employee resistance to ultimate IT administrative control over a personal device in the workplace, Sogueco said that “these are the rules of the game. If they don’t want to adhere to them, then don’t bring [your devices].”

Even though 86% of organizations cited data security as a top concern, according to a 2012 survey on employee-owned device management strategies from SoftwareAdvice.com, and most had a mobile device management policy in place, using a specific MDM system is far less common, with lack of resources and mobile framework immaturity being chief among the reasons.

What does an MDM system do, exactly? The panel defined it as “software that secures, monitors, manages and supports mobile devices deployed across enterprises for both company-owned and employee-owned devices.” Why is it important? Security maintenance is the critical overlay, but MDM systems are beneficial and a growing necessity for many reasons, as the panel highlighted:

- Increase the scale of mobile deployments
- Gain real-time visibility into a mobile environment

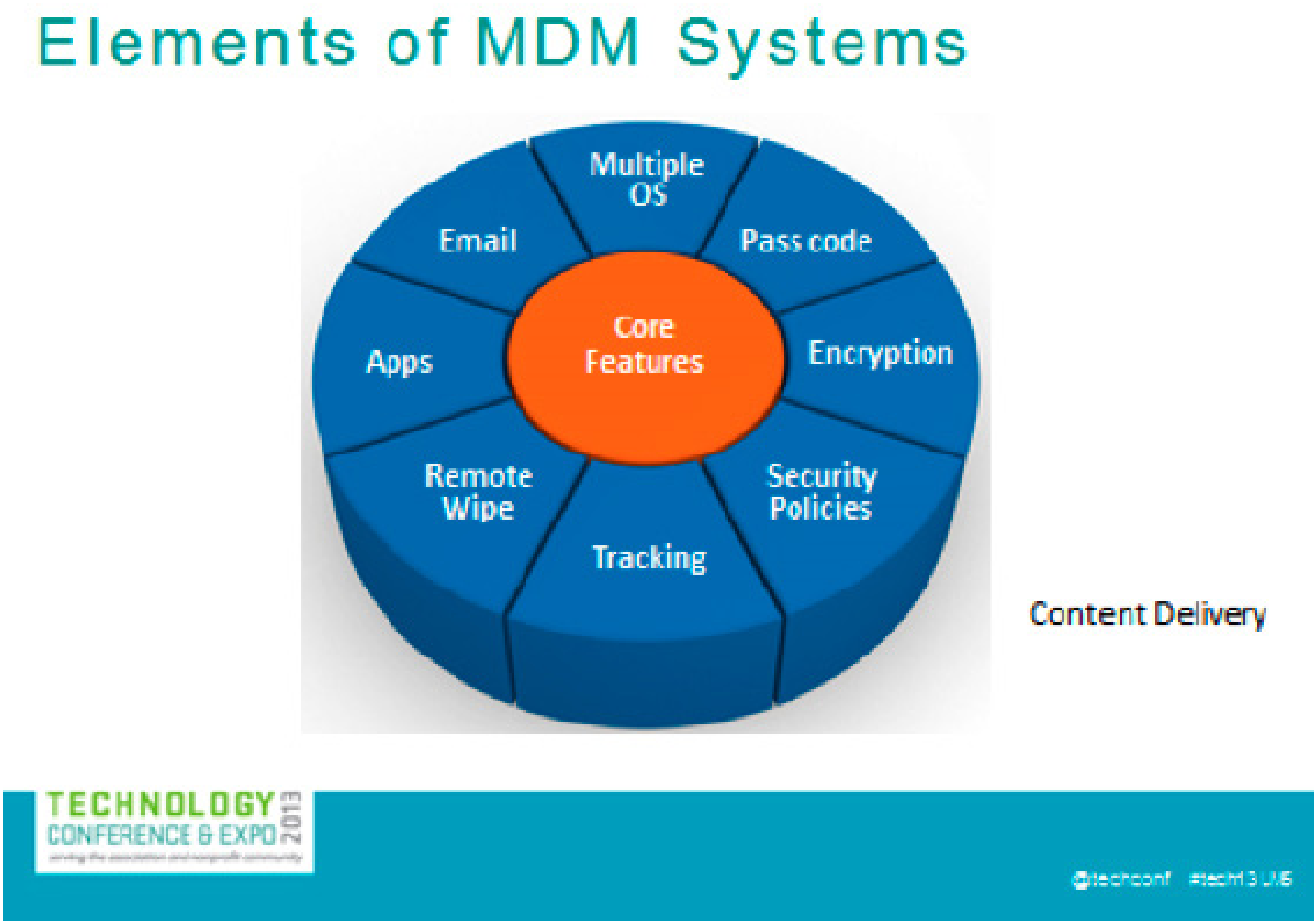
- Administer consistent policies across devices
- Enforce enterprise security and compliance
- Protect data transmitted to and from devices
- Complete enterprise data loss prevention (DLP)
- Automate processes and issue resolution
- Analyze and report critical device information

While MDM systems comprise a few key elements, there is by no means a one-size-fits-all solution." All robust MDM systems need a few core features, but it's really a matter of what you want to turn on, and what you want to pay for," according to Patrick McGugan, director of business management services at ARG Inc. McGugan also noted that each of these elements must be built for the management and protection of content, a necessary underlying consideration when evaluating and choosing an MDM system. (See Figure 2.)

Home

Mobile device management checklist

Ensure mobile device security through a mobile device management policy



Elements of MDM Systems

Core Features

Multiple OS

Pass code

Encryption

Security Policies

Tracking

Remote Wipe

Apps

Email

Content Delivery

TECHNOLOGY CONFERENCE & EXPO 2013

serving the association and nonprofit community

@techconf #tech13[illegible]

Figure 2: MDM system must haves

Another critical component of a comprehensive MDM policy framework is an acceptable use policy that includes safety measures that shield against employer liability. The panelists highlighted a few typical elements included here based on their experiences:

- Employees are not allowed to use cell phones for work-related business while operating any vehicle.
- Before placing a cell phone call, employee must be stopped and using a hands-free headset.
- Employees are required to attend mandatory cell phone training and sign a contract showing that they understand the policy.
- Employees that disobey the policy will be disciplined.

Home

Mobile device management checklist

Ensure mobile device security through a mobile device management policy

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.