Best practices for mobile data protection

This expert e-guide presents five essential best practices for securing employee-liable mobile devices and tablets that will allow you to safely embrace the trend toward using personal devices for business.

Sponsored By:  

ArcSight
An HP Company
Best Practices for Mobile Data Protection

Table of Contents

Top 5 mobile data protection best practices

Resources from ArcSight
Top 5 mobile data protection best practices

By Lisa A. Phifer

According to a recent Juniper Networks Inc. survey, 40% of workers reported using their own mobile devices for both personal and business activities; of those, 80% admitted to accessing their employer's network without permission.

Unless enterprises implement controls to prevent loss, theft or misuse of these employee-liable devices, any one of these security events could put considerable business data at risk.

Practices for protecting data on corporate-liable mobile devices are well known, from enforcing encryption, to wiping lost devices. But the business data associated with employee-liable devices must be safeguarded without relying on IT procurement or ownership, while respecting user expectations for personal privacy and choice.

Let's take a look at five essential data protection best practices for securing employee-liable mobile devices and tablets.

1. Mobile device locks

Device locks are IT's first line of defense against unauthorized access to business data and accounts stored on an employee's mobile device or tablet. However, consumer devices purchased by employees don't always have sufficiently strong device locks. Furthermore, users may reset complex passwords that make personal devices hard to use. These business needs can be addressed with a three-phrase approach:

- Implement a process to let users enroll their own mobile devices and tablets, checking them against minimum requirements. This prevents business use of sub-standard devices while embracing those that can support IT-defined security policies.
- Auto-configure enrolled devices to enable built-in PIN or password locks, enforce complexity rules and auto-lock idle devices. Aim for rules that reduce business risk without being too heavy-handed.
• Implement over-the-air device configuration monitoring to ensure settings have not been altered. For example, checking every time a device tries to access a corporate account to block/remediate non-compliant devices.

These practices can be implemented for employee-liable mobile devices using either Exchange ActiveSync (EAS) or a multi-OS mobile device manager (MDM), available from companies such as AirWatch, BoxTone, Good Technology, MobileIron, Odyssey Software, Inc., Sybase, Inc. and Zenprise. Employers that do not have an MDM and do not want to install one can use hosted MDM services.

2. Remote data wipe for mobile devices

When a previously enrolled device is lost/stolen or its owner leaves your company, remote data wipe can prevent all future use of business data and accounts stored on it. However, wiping an employee's personal device should not be done without explicit permission and ideally should not impact personal data or inconvenience the user. These business needs can be addressed as follows:

• As a condition of device enrollment, employees should be required to formally consent to an acceptable use policy. That mobile device policy should define (among other things) situations in which IT can invoke remote wipe, how wipe will impact personal device use and data, and data backup/restore responsibilities.
• Consider using data encryption tools that compartmentalize business data, accounts and applications. For example, use a self-encrypting corporate messaging application that saves email, contacts, calendars and other data to an authenticated, encrypted sandbox that can easily be removed without wiping the entire device.
• Implement processes to remotely wipe employee-liable devices. To deter evasion techniques, complement confirmed over-the-air command with auto-wipe after repeated login failure, prolonged offline use or SIM/USIM card removal. Be sure to watch out for corporate data left behind on removable media on devices (e.g., Android).

Basic over-the-air remote wipe can be implemented using EAS, any MDM, or numerous free/inexpensive applications designed for personal use (e.g., Apple MobileMe, McAfee...
WaveSecure). However, greater IT control and visibility can be achieved by using an MDM for this practice: For example, reporting on which devices were wiped, or auto-removing enterprise applications and accounts previously installed by the MDM.

3. Mobile locationing and tracking

During any mobile device's lifetime, considerable information may be recorded about its usage, including geographic location. On-going tracking can help IT recover lost devices quickly or generate roaming alerts to warn IT about possible thefts. However, employee expectations of privacy may inhibit on-going tracking. Furthermore, some consumer devices may not be readily located (e.g., disconnected or disabled devices). Finally, costs may be considerable if tracking involves frequent SMS messages.

To address business needs while addressing personal and cost sensitivities, determine whether on-going tracking is really necessary for employee-labile devices. If so, describe business rationale and practices for location tracking in your acceptable use policy, requiring employees to consent when enrolling personal devices for business use. If locationing is really only needed to recover a lost device, state this in your acceptable use policy – and then stick to that narrow use case.

On demand/as-needed locationing services are freely available for every major mobile OS (e.g., Apple MobileMe, Lookout Find My Phone (Android), Microsoft My Phone, and BlackBerry Wheres My Phone). But here again, more centralized visibility and control can be obtained by using an mobile device manager to implement this practice.

4. Stored data encryption on mobile devices

In some cases, device lock plus remote wipe are sufficient to mitigate risk on personal devices used for limited business tasks. A mobile device used to check innocuous email without saved attachments, or a tablet used only for remote desktop access may not store business data requiring persistent protection. However, workers who deal with sensitive information or require greater functionality require stored data encryption. Unfortunately, some consumer devices don't support full device encryption. To address this business need, take the following steps:
• Extend the aforementioned enrollment process to check personal mobile devices against stored data encryption requirements, using the worker’s authenticated identity to determine mobile data needs and risks. If encryption is required but a device cannot support it, provide instructions to help the worker obtain a suitable device – perhaps even an IT-secured corporate-labile device if the situation warrants.

• Auto-configure enrolled devices to enable full device encryption and removable media encryption wherever possible. Where needs and risks warrant, deploy self-encrypting applications to provide another layer of protection for corporate data, segregated from personal data. Finally, configure device settings and applications to minimize the amount of corporate data stored on the device.

• Use over-the-air device configuration monitoring to ensure continued compliance with all stored data encryption policies. In addition, watch for devices that exhibit signs of tampering (i.e., rooted Androids, jailbroken iPhones), as these may harbor Trojans that can access and transmit otherwise-encrypted data to remote attackers.

To accomplish the first step, integrate your enrollment process with your corporate directory, authenticating employees with existing logins and using group affiliations to determine business need and risk. For the second step, deploy secure mobile applications, such as Good for Enterprise and NitroDesk TouchDown, or substitute Web portal or remote desktop access to reduce on-device storage for employees that don’t really need offline/disconnected access to business data.

5. Mobile activity monitoring and audit

Note that ongoing monitoring plays a role in all of these best practices. It is not enough to configure an employee-labile device and hope business data stays secure. Even though IT may not choose or own employee-labile mobile devices, the employer still needs to monitor and audit business data and activities to ensure compliance throughout their lifecycle. However, this must be done over-the-air, without intruding on personal usage.

• Start by monitoring the workplace for employee-labile devices used for business without IT permission. Network access controls, device fingerprinting tools and wireless/wired network IPS are all good tools to help IT spot mobile devices or
tablets that fall into this category. Some of these monitoring mechanisms can even prevent corporate access by unknown devices.

- Next, log every business system interaction involving enrolled mobile devices, including email/contact/calendar synchronizations, Web sessions, VPN connections, over-the-air configuration updates and MDM application installations. These records are important for routine reporting and audit purposes, and should be retained long after a device is wiped or de-enrolled. Ideally, devices should be identified in a way that prevents spoofing or cloning – for example, device certificates installed using SCEP.

- Finally, perform periodic compliance checks for each enrolled employee-liable device. At minimum, checks may be done during normal interactions (e.g., using EAS to verify settings whenever email is synchronized). However, MDM products often provide richer mobile device auditing and reporting capabilities – in some cases, scheduled and on-demand retrieval of device settings and auto-comparison to IT-specified policies.

By implementing these five essential mobile device data protection best practices, many employers will find they can safely embrace the trend toward using personal mobile devices for business. Stay focused on business data and establishing minimum controls needed to protect that data. For example, few users would consent to a white list policy that prevented them from installing personal applications. However, many users might accept – and even welcome – IT assistance in wiping a personal device that's been stolen. To maximize acceptance and side-step pitfalls, identify a test group and use it for an initial rollout of proposed policies and controls, making any necessary refinements before beginning a broad rollout.
Find the cybercriminal.
(Never mind. ArcSight Logger already did.)

Stop cybercriminals, enforce compliance and protect your company's data with ArcSight Logger 4.

Just downloaded the customer database onto a thumb drive.

Learn more at www.arcsight.com/logger.
Resources from ArcSight, an HP Company

Protecting the Security and Availability of Next Generation Telecom Services

Addressing FSA Requirements with ArcSight IdentityView

ArcSight Protection Suite for NERC CIP Compliance

About ArcSight, an HP Company

ArcSight (NASDAQ: ARST) is a leading global provider of cybersecurity and compliance solutions that protect organizations from enterprise threats and risks. Based on the market-leading SIEM offering, the ArcSight Enterprise Threat and Risk Management (ETRM) platform enables businesses and government agencies to proactively safeguard digital assets, comply with corporate and regulatory policy and control the internal and external risks associated with cybertheft, cyberfraud, cyberwarfare and cyberespionage.