Mobile Device Security Considerations

Overview
Mobile devices are powerful and affordable. Their ease of use, small size, and functionality increases security risks to organizations using the devices. Security controls reduce risks and are typically grouped into three categories, Administrative Controls, Technical Controls, and Physical Controls.

Administrative Controls
Administrative controls include policies, procedures, plans, agreements, and related safeguards that reduce risks. Examples of administrative safeguards are listed below.

Policies. Policies and procedures demonstrate support for and commitment to information security. Examples of policies that control risks related to mobile devices include:

- Bluetooth Policy
- Bring Your Own Device and Technology Policy
- Disposal Policy
- Mobile Device Policy
- Password Policy
- Patch Management Policy
- Securing Information Systems Policy
- Securing Sensitive Information Policy
- Wireless Access Policy

Security Training. People, not technology vulnerabilities, can be the biggest threat to an organization. Staff should receive security awareness and education training appropriate for their job duties and responsibilities. Important safeguards include:

- Security Awareness and Training Plan
- Security Awareness and Training Policy

Incident Response. Organizations must maintain the privacy and protection of sensitive information. An effective approach to managing risks includes a proactive approach to dealing with security incidents, replacement of a lost device, etc. Documents that identify and manage incident related risks include:

- Audit Trails Policy
- Incident Response Plan
- Incident Response Policy
- Logging Policy
- Security Monitoring Policy

Agreements. Organizations should controls risks related to third party service providers. Examples of mobile device related service providers include hardware and software vendors, outsourced help desk, and mobile application software developers. Documents that manage risks related to service providers include:

- Agreement with service provider
- Personnel Security Policy
- Third Party Service Providers Policy

Technical Controls

Technical controls include device access controls, configurations, security mechanisms, updates, and other related safeguards.

Access Controls. Device access controls can include a Personal Identification Number (PIN), password, pattern, face recognition, and other similar technologies (collectively termed Password).

- Passwords – devices should require a Password at start up and after a period of inactivity. Where possible, users should select, and mobile applications should require, complex Passwords.

Configurations. Ensure mobile devices are configured for security.

- Applications – configure the device to not allow the installation of applications from unknown sources.
- Encryption – encryption should be activated, requiring a Password or other code each time the device is turned on. Where possible, the external SD card should also be encrypted.
- Security Policy Updates – devices may include a set of updatable policy files designed to help protect device data. As new threats are detected, updates to the security policies on the device can help prevent new attacks. Ensure the policy update feature is enabled instead of waiting for the next scheduled software upgrade.

Applications. Security applications help enhance the protection of sensitive information.

- Lock Applications – applications such as App Lock and Smart Lock use passwords or pattern locks to restrict access to apps, contacts, folders, SMS, e-mail, gallery, settings, and calls.
- Communications – Virtual Private Network (VPN) applications protect sensitive information by encrypting data before transmission.

Protection Software. A mobile security application such as Lookout, avast! Mobile Security, 360 Mobile Security, or McAfee Mobile Security should be installed to protect against a variety of threats. Examples of security features include:

- Applications – assesses installed applications as well as updates to applications to ensure they are safe.

- Backups – backups up important files, contacts, call logs, and other information.
- Browsing – protects against suspicious websites that could infect a device or steal personal information.
- Privacy – reviews applications to determine features used (e.g. location, contacts, messaging).
- Remote wipe – if the device is lost or stolen, the user can lock the device or delete personal data.
- Theft protection – identifies the location of the missing device, sounds an alarm, and can send an e-mail with photo and location of the device.
- Updates – security updates to the protection software are automatically downloaded to the device.

Updates. The operating system and applications are vulnerable to attacks. Ensure the user is notified when software updates and patches are available.

Physical Controls
Physical controls include safeguards that restrict physical access to the device as well as steps taken if the device has been lost, stolen, or compromised.

Physical Access. Devices should be protected to reduce the risks from environmental threats and hazards as well as opportunities for unauthorized access.

- Procedures should be developed to protect the device from unauthorized physical access, tampering, and theft.
- Procedures should identify when additional physical safeguards are needed to protect devices that access, receive, transmit, process, or store sensitive information.
- Staff should be trained on procedures to be followed when a new device has been obtained.
- Staff should be trained on procedures to be followed when a device has been lost, stolen, or compromised.

Mobile Device. Organizations that are especially concerned about security may want to consider a secure phone platform such as Silent Circle's Blackphone with PrivatOS and Silent Suite.

Other Security Considerations
Security should be integrated as a part of the total solution when rolling out mobile devices into business units. Consider an end-to-end pilot test that simulates the organization's environment.

- Configuration. If the organization allows the mobile device to be used for both personal and business use, configure the mobile device with both personal and business applications and data.

- Data. Test the solution storing data on the mobile device local storage, SD card, and servers.
- User Interaction. Test the mobile device in a realistic environment to determine signal strength, user response times, manual and automated locking of the device, etc.
- Administrative Controls. Evaluate the effectiveness of written policies, procedures, security training, and incident response plans.
- Independent Evaluation. Consider allowing outside personnel to evaluate the device and configuration to identify any misconfigurations, software conflicts, etc.

The role of Chief Security Officer (CSO) should be formally identified.

- The Chief Security Officer (CSO) is responsible for security throughout the entire organization. The CSO oversees and coordinate security efforts across the enterprise including Information Technology (IT), Production and Operations, Human Resources (HR), Accounting and Finance, Legal, Communications, Facilities Management, Sales and Marketing, and other groups.
- The CSO is responsible for overall corporate security strategy, security architecture development, and security initiatives. As the company's senior security officer, the CSO has enterprise-level responsibility for all security policies, procedures, guidelines, standards, evaluations, roles, and corporate security awareness.

Mobile application security audits help manage risks to systems and sensitive data.

Publication Information

Altius IT is a security audit, security consulting, and risk management firm. Our experts have over 30 years of experience in the Information Technology and are recognized as experts in our field. We are certified by the Information Systems Audit and Control Association (ISACA) as a Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Controls (CRISC), and Certified in the Governance of Enterprise Wide IT (CGEIT). For more information please visit www.AltiusIT.com.