Mobile Computing Controls

Controls can reduce the risk of disclosure of sensitive data stored on mobile devices.

Many controls can be enforced by mobile device management (MDM) systems and/or secure containers (a separately authenticated, encrypted area of the mobile device that is used to keep sensitive enterprise data segregated from the personal data) for enterprise and personal devices.

These controls include the following examples:

Device registration—All mobile devices authorized for business use should be registered in a database. Devices that are personally owned should be flagged. An enterprise can push updates or manage authorized devices and exclude personally owned mobile devices.

Tagging—Physically tagging the device with an asset ID may result in its return if it is lost; however, there is risk in identifying the enterprise that owns the device.

Physical security—If the device is stationary and permits it, use a cable locking system or a locking system with a motion detector that sounds an audible alarm.

Data storage—Only store content that is absolutely needed on the device. With the ability to remotely access central servers, the requirement to store any data locally should be questioned. If data are not stored locally, then a lost or stolen device will not be an issue. The data that are stored should be backed up on a regular basis, preferably to shared folders on the enterprise's file server.

Virus detection and control—The threat associated with viruses applies to all mobile devices. The enterprise should update the mobile device antivirus software to prevent perpetuation of malware.

Encryption—Mobile devices used to store sensitive or confidential information should be encrypted in accordance with the enterprise's information security policies, mandating use of a strong encryption mechanism.

Compliance—Mobile devices should comply with the security requirements as defined in enterprise standards. All mobile devices should require a password. Two-factor authentication can be used to further enhance security.

Approval—Mobile-device use should be appropriately authorized and approved in accordance with the enterprise's policies and procedures.

Acceptable use policy—A security policy should exist for mobile devices. The enterprise should have a policy that addresses mobile device use and specifies the type of information and kind of devices and information services that may be accessible through the devices.

Due care—Employees should exercise due care within office environments and especially during travel. Any loss or theft of a mobile device must be treated as a security breach and reported immediately in accordance with security management policies and procedures.

Awareness training—Employee orientation and security awareness training should include coverage of mobile device policy and guidelines. The training will allow propagation of awareness that mobile devices are important business tools when used properly and have risk associated with them, if not managed accordingly.

Network authentication, authorization, and accounting—IT functions should adopt a solution that allows them to tie devices connecting to the network with each user's identity and role, and then apply role-based policies to grant proper access privileges. This enables IT to differentiate access for different levels of employees, guests, or device type. It also lets IT take a proactive stance on tracking and monitoring how mobile devices are being used within the network.

Secure transmission—Mobile devices should connect to the enterprise network via a secure connection, such as over a VPN.

Standard mobile device applications—Configuration and use of the mobile device should be baselined and controlled. Only applications that either meet with the enterprise security architecture or are delivered as standard on the mobile device should be authorized for use, and all software applications must be appropriately licensed and installed by the enterprise's IT support team. MDM solutions support this.

Geolocation tracking—There are many debates about the privacy concerns of GPS tracking, but location capabilities inherent in mobile devices can be invaluable in the case of loss or theft.

Remote wipe and lock—Due to the nature of mobile devices, many device management solutions are focused on securing the device if it is lost or stolen. Some MDM solutions allow IT to send an alarm to the device to help identify the location for a user, and, if truly lost, IT can then remotely wipe and lock the device and/or container.

Secure remote support—Employees relying on personal devices to conduct work are often out of the office. Having a secure way to support and fix these devices from a remote location is imperative to maintain employee satisfaction. Depending on device type, remote support solutions allow help desks to configure devices, chat, transfer files, and remotely see and control the device. It is important to select a solution that supports a wide variety of devices and keeps all access and activity logs behind the enterprise firewall to ensure security.