@ISACA
RELEVANT, TIMELY NEWS
Volume 22, 24 October 2012

5 Considerations for Choosing an MDM Solution

By John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP

Many professionals are being asked to provide recommendations for evaluating mobile device management (MDM) solutions. A number of vendors, solutions and technologies are available in the global marketplace that provide a broad range of MDM capabilities and solutions. This is a rapidly growing area, so here are 5 important business and technical elements to consider.

1. **What levels of capability and control are actually required?** Each enterprise will have its own view on the level of control and access that it would like to have on mobile devices. Often security professionals seek a broad and extensive range of capabilities and controls when choosing an MDM solution. In many cases though, enterprises require and/or desire only a basic set of controls for the majority of their users and use cases. The best way to find a balance between these two differing points of view is to perform a threat and vulnerability analysis of your mobile device solutions to identify the appropriate control objectives and functionality.
2. **What MDM functionality can you actually support and use on an ongoing basis?** MDM solutions are constantly being advanced with new functions and capabilities. Some beneficial and appealing features, such as security analytics and mobile application management, may require full-time staff and extensive resources to be effectively utilized. Dedicating full-time, or even significant amounts of part-time, staff is often not desirable or even possible for many enterprises.
3. **If you are managing personally owned devices, what level of capability do you want to have on these devices?** MDM solutions can assist enterprises in providing operational support and security policy enforcement for the use of personal mobile devices to access corporate resources (bring your own device [BYOD]). Technologists and information security professionals are quick to point out the benefits of their use for this purpose, but often overlook the legal and cultural impacts that MDM solutions can create. It is important to consult with all stakeholders during the requirements-gathering stage of evaluation to ensure that you have an understanding of the limitations or controls each would like put in place for the use of MDM solutions. This will ensure that your enterprise is not exposing itself to unwanted liability, risk and privacy concerns. It will also help to ensure that the users are educated about your capabilities and amenable to the level of control you have on their personal devices in a BYOD scenario.

4. **Are your current MDM solutions good enough?** When evaluating MDM solutions, it is important to evaluate the current solutions' capabilities, whether in use or available. Many enterprises find that these solutions, while not ideal, meet a majority of their MDM business requirements and technical control objectives. Microsoft Active Synch, for example, is offered to enterprises as part of their Microsoft Exchange Server implementation. Active Synch provides MDM functionality, such as password policy enforcement, requirement for use of encryption for data at rest and in transit to the Exchange Server, and remote device data wipe for Active Synch-enabled mobile devices. For many enterprises, this level of capability and functionality is considered acceptable for the majority of their mobile-user population. While more advanced MDM solutions may be considered ideal because they provide features above and beyond this level of functionality, the total cost of ownership associated with them (e.g., license, maintenance, infrastructure, staff and support costs) may make the acceptable solution more palatable.
5. **Can the MDM solution effectively manage the mobile devices you want to support?** MDM solutions typically require software agents that require highly privileged access to the mobile device's operating system and associated applications to be installed and active on target devices. Unfortunately, some of the most popular mobile devices severely limit the functionality of most MDM software agents. While many MDM solution vendors are attempting to overcome these challenges, they are unlikely to be successful without a shift in strategy and approach from the mobile device manufacturers. It is important to ensure your minimum business and technical requirements can be met by the MDM solution for all popular mobile platforms that you plan on leveraging, especially if you plan to implement a BYOD approach to their use in your enterprise.

John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP, is the president of IP Architects LLC.