@ISACA
RELEVANT, TIMELY NEWS
Volume 21, 12 October 2011

5 Information Risk Management and Security Tips When Adopting a BYOD Strategy for Mobile Devices

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

1. **Bring your own device (BYOD) means that the user has the final say about what happens on the mobile device**—BYOD strategies for mobile devices have numerous financial and technological advantages for organizations, but also introduce risk management and security concerns. It is important to remember that the user has the authority and ability to modify the configuration, applications and technical controls used in these devices. The best defense for an organization is to define technical controls that are required to be present and operating on personal mobile devices that are used to connect and interact with the organization's network. Organizations should also implement capabilities to verify that these technical controls are in place and operating as intended whenever personal mobile devices attempt to access or interact with the organization's network.
2. **Limit access for employee-owned mobile devices compared to corporate-issued and -managed mobile devices**—Typically, an organization has more authority and control over devices it owns and manages compared to those that are employee-owned. Organizations should consider limiting the access of users using personal mobile devices to low-risk capabilities when connecting to the enterprise network such as e-mail, employee directories and internal web browsing. Individuals who have business needs to access sensitive data or applications should be issued corporate-owned and -managed mobile devices. This will allow the organization to have more control and flexibility in how it manages risk and secures devices for high-risk users while still gaining the financial and technological gains of the BYOD strategy for other users.
3. **Certify mobile devices and associated capabilities for use**—Only mobile devices and operating systems that have been tested and certified for their ability to meet an organization's information risk management and security capabilities should be able to access and interact with its network. This testing and certification process should identify and confirm the ability for the organization to install, enable, verify and maintain technical controls required to meet its data and technical security requirements. The testing should be performed on typical configurations used by employees for their devices and should include common and popular add-on applications to ensure that they are representative of realistic operating conditions.

A list of certified, acceptable devices, operating systems and applications should be communicated to the organization's user population proactively and be easily accessible for future reference.

A second list should be developed and distributed that identifies popular mobile devices, operating systems and applications that have been evaluated, but are not certified to be connected to or interact with the organization's network. This list should also provide a clear explanation of the reasoning for not certifying these items as well as information about when reevaluations are projected to occur. This will ensure that individuals included in a BYOD environment are aware of both certified and prohibited devices, operating systems and applications prior to any purchase or request to connect and interact with the organization's network.

4. **Update policies and standards to incorporate BYOD mobility requirements**—Information risk management and security policies and standards provide users with guidance and insights on how an organization expects them to operate and behave when connecting and interacting with its network. When adopting a BYOD strategy for mobile solutions, it is important to update these policies, standards and supporting documentation to incorporate control objectives and requirements that are unique to personally owned mobile devices and capabilities. These updates can include an organization's right to examine and audit devices, install and maintain technical security controls, limit or adjust functionality, and adjust access and use capabilities based on current threats and risk—regardless of whether the solution is currently connected to the enterprise network.
5. **Educate users about the organization's technical security control capabilities and impacts on their personal mobile solutions**—Many users are concerned about the level of access and restrictions that an organization's technical security controls can enable on their personal devices. In a BYOD-enabled environment, it is important that a user understands the capabilities and limitations of these technical controls to ensure their continued use and acceptance.

   The most common user concerns about technical controls implemented by an organization on personal mobile devices is the ability for the organization to access, modify, monitor, restrict or delete data and communications (including personal data and communications) on devices without the user's permission or prior notification. User education is the key to overcoming these concerns. Ensuring that a user understands the capabilities, use cases, and inherent personal and business benefits that these technical security controls provide will often make users feel more comfortable about the existence of the controls and encourage their continued use. It is also important to communicate information about the governance

processes and capabilities that are in place for these technological controls. This will ensure that a user understands that they will be used only when warranted by the organization and that proper procedures and oversight capabilities are in place to ensure that the controls are not abused.

For additional information related to mobile devices, see the ISACA publications ***Securing Mobile Devices***; ***Mobile Computing Security Audit/Assurance Program***; and ***Geolocation: Risk, Issues and Strategies***.

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