Is BYOD a fit for your firm?

Accompanying the explosive rise in the variety and functionality of consumer electronic devices, such as mobile phones, tablets, and laptops, is users' desire to bring those devices into the workplace. This preference may have a positive and negative effect for employers. Employees generally invest more in their own devices and tend to be more productive when working on devices of their choice rather than a firm-issued device. Employers, however, need to ensure the security and confidentiality of their data if employees store it on these devices.

While an employer may dictate the type of devices and permitted applications on firm-issued devices, they may exert only a limited degree of management of personal devices.

To manage personal devices and clarify expectations between end users and corporate IT departments, firms should create a BYOD (Bring Your Own Device) policy.

BYOD policies may vary depending on a user's role within an organization but typically should define items they affect, including permissible devices, acceptable applications, expense reimbursement/stipend agreements, accessibility to firm resources, and, most important, security and privacy.

A well-defined BYOD policy allows employees to enjoy the flexibility of being able to select and upgrade their devices without affecting their employer's IT budget or compromising network security and stability. Although many BYOD sample policies and templates are available on the Internet, development of your BYOD policy may need to include input from department managers and your legal, IT, and HR departments.

While we may assume most users will do their best to abide by the rules in a BYOD policy, the only way to monitor and enforce any defined policies is through the deployment of an MDM (Mobile Device Management) solution. An MDM solution can ensure that a mobile device meets defined prerequisites and enforce policies prior to granting a device access to the corporate network. Sample prerequisites and policies might include:

- Enforcement of password restrictions
- Verification that the appliance has anti-virus installed
- Verification that the appliance has not been jail-broken
- Verification that only approved applications have been installed
- Restricted hours of access to corporate resources
- Disabling of features such as cameras or wireless networks during work hours

An MDM solution may also provide access to a customized application store that serves only pre-approved, pre-paid applications. Additionally, configuration profiles for email and wireless network settings may be pushed to mobile devices, ensuring consistency across devices and thus simplifying troubleshooting and support issues. Via an MDM solution, IT personnel can perform a factory reset or a selective wipe of components on a lost or stolen phone.

MDM solutions are available as in-house or hosted solutions from several vendors, including Cisco/Meraki, Good, Microsoft, MobileIron, MaaS360 (IBM), and Kaseya. While all these products are

feature-rich, functionality, features, and costs vary widely, from free, hosted solutions to in-house systems requiring several servers and ongoing maintenance.

The pros and cons of BYOD vary from one firm to another. While one firm might save money by eliminating the need to purchase devices for its staff, another may expend additional financial and personnel resources to purchase and manage an MDM solution. BYOD is not a fit for everyone, for example: if an employee leaves a firm, so does his/her mobile device—and the associated phone number. If the employee used that number for sales or as a source of client contact, the issue may be serious enough to negate the adoption of BYOD for a particular service or department.

When considering BYOD for your firm, you should examine current practices to determine to what extent your firm and employees could benefit from the implementation of BYOD, from a technical, financial, or emotional perspective. If your firm decides to incorporate BYOD, be sure to have conversations with IT and HR departments (or consultants) to ensure your BYOD policy follows best and common practices, and the MDM solution you select satisfies your firm's needs.

Stan Rabin is vice president of technical services at Keno Kozie Associates, a leading national IT consulting firm specializing in the legal community for more than 25 years. Stan has more than 20 years of experience in the design, implementation, and support of local and wide area networks. He focuses on assisting clients in evaluating their technology with specific attention to design and implementation of data center and disaster recovery environments.