Bring Your Own Device (BYOD) Strategy for a Mobile Workforce

TECHNOLOGY SPOTLIGHT

"A well-designed Bring Your Own Device (BYOD) strategy and implementation will ensure that personal IT devices boost employee productivity and satisfaction rates without increasing costs."

– A.T. Kearney BYOD Study[1]

Use of Personally Owned Devices at Work Increasing

Several converging trends have created an expanding group of virtual and remote employees with different mobility needs. Traditionally, businesses considered information technology a service they owned and provided through their infrastructure. However, consumerization is changing that. Employees and customers want to interact with businesses using their own technology, how they want, when they want. Employees also want the flexibility of working remotely. Businesses more comfortable with traditional ways may be missing out on significant employee satisfaction, productivity, innovation, and market opportunities. On average, Bring Your Own Device (BYOD) implementation can generate US$350 of value per mobile employee[2] because 53% of employees feel more productive when they have their own devices.[3]

BYOD allows employees to use their personal devices at work. The use of non-entity-owned devices will become an integral part of the entity's technology strategy and infrastructure. With BYOD, businesses must realize the employees' equipment is not under the same degree of direct business control as corporate-owned devices. This results in new issues of:

- security and control
- contractual relationships

1 www.atkearney.co.jp/documents/10192/585432/Bring+Your+Own+Device.pdf

2 https://blogs.cisco.com/news/new-analysis-comprehensive-byod-implementation-increases-productivity-decreases-costs

3 https://go.apperian.com/rs/300-EOJ-215/images/Apperian%202016%20Executive%20Enterprise%20Mobility%20Report_FINAL_20160216.pdf?aliId=16373787

- legislative and industry compliance
- employee adherence to corporate policies and procedures.

Mobile device management (MDM) has risen to prominence along with the rising adoption of BYOD by businesses to help address some of the issues companies face with BYOD. As with traditional IT asset management tools, MDM solutions provide businesses with the ability to manage policy, inventory, and security of their employees' personal mobile devices.

While BYOD shifts device ownership to employees, the responsibility to protect corporate data and ensure the use of these personally owned devices meets organizational control standards remains with the business.

Importance

As employees embrace workplace mobility, mobile devices are becoming a treasure trove of corporate information. Therefore, CPAs in risk or oversight roles must help their businesses protect these assets and intellectual property by ensuring proper security and control over that data. A recent study found that over 60% of small business owners agree that the risk of data breach is higher when employees work remotely and 40% of senior management and business owners reported human error or accidental loss by employees as the main cause of a data breach.[4]

Because mobile devices are especially prone to accidental loss, businesses have established policies, procedures, and on-device software for corporate-owned devices to mitigate the risk of data loss. But what about personally owned devices? Extending and maintaining effective security and control over personally owned devices presents organizations with new and significant challenges.

Business Benefits and Considerations

Businesses can benefit from pursuing a BYOD strategy in various ways, including:

- reduced hardware, support, and telecommunication costs
- better workplace flexibility leading to higher job satisfaction and employee happiness
- improved productivity for employees as they are more familiar and comfortable with their own personal devices
- increased responsiveness of employees as people generally carry their own personal devices with them all the time.

4 www.shredit.com/en-us/about/press-room/press-releases/shred-it-study-exposes-employee-negligence

However, organizations contemplating a BYOD strategy need to develop comprehensive policies and procedures for the use of such devices. These could include specifics for the protection, use, storage, maintenance, archiving and destruction of corporate information. Third-party MDM solutions (e.g. IBM MaaS360, Microsoft Intune, Soti MobiControl, Duo Beyond, etc.) can help businesses administer and manage employee-owned devices. Organizations should also consider providing appropriate support and best-practice security guidance to employees to help them identify and resolve problems with their personal technology used for business purposes.

The following table summarizes the potential risk areas and mitigation strategies for BYOD-enabled organizations.

Risks Areas	Risk Mitigation Strategies
Entity lacks specific policies, procedures or guidance to address the BYOD issues and assist employees and others working in a BYOD environment.	• Develop, implement and monitor comprehensive and effective BYOD policies and procedures. • Support the policies and procedures with appropriate guidance and training.
Employees' personally owned devices may be used to store confidential or private corporate information, thereby increasing the potential for misuse, loss or disclosure.	• Implement policies that limit users from storing such information on unsecured personally owned devices. • Create a "corporate profile" on the personal device to restrict storage of data, or separate data into personal and corporate applications. • Session initiation should include automatic data synchronization with corporate databases. • If devices are continuously connected, regular backups in pull or push mode should be configured.
Inability or difficulty in protecting business information on lost or stolen personally owned devices.	Adopt a policy that any devices carrying corporate data be subject to the company's information security policies and monitoring tools as well as periodic review by management. Examples of security polices to enforce may include requiring: • MDM solutions be installed to help manage and enforce policy and security rules • on-device encryption and regular back up of business data • your business to be able to remotely wipe data if the device is lost or stolen • mandatory use of a complex password that is to be regularly changed and enable multifactor authentication.

Risks Areas	Risk Mitigation Strategies
The entity must address control and ownership questions over data (e.g., does the data belong to the business or the individual and what are the legal and / or contractual obligations of the entity to protect that data?).	• Develop, implement and monitor comprehensive and effective policies and procedures that address data ownership and controls on a BYOD device. • Develop and implement corporate data classification controls and apply the corresponding protection mechanisms to the BYOD data. • Develop policies and procedures for the review and cleansing of corporate applications and data when employees leave.
Employees or contractors may subscribe to a commercial backup service and inadvertently violate laws and agreements as a result of including the organization's information in such backups.	• Configure the device to exclude organization files in employee-initiated commercial backup. • Create a compartmentalized "corporate profile" on the personal device to restrict storage of data, or to separate data into personal and corporate applications and prevent personal backup services from accessing corporate data.
Increased demand on IT resources will be required to support a large array of personally owned devices.	• Implement an approved list of supported devices that employees can bring to work. • Clearly define the level of support provided for personally owned devices. Limit such support to business-use cases only.
Increased use of mobile devices and their incorporation into business processes result in new concerns about device management, mobile platform development and mobile data management capabilities.	• Create procedures to operationalize the mobile device policies. • Implement user awareness of security, usage and other policies and related procedures thereby ensuring a clear understanding of the expectations and boundaries around appropriate use of mobile devices in the workplace. • Implement technology solutions such as MDM to support policies and procedures to ensure initial and / or regular / continuous checks on device configuration against corporate standard, with the ability to change or update settings prior to allowing the session to continue.

Conclusion

Demands for workplace mobility will only increase from here on. Businesses should have strategies to help their employees succeed in this new work environment. Having an effective BYOD strategy is an important starting point for achieving that.

This publication is part of the **Technology Spotlight series**.

The entire series covers technology trends that impact CPAs and are available on our website.