CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Bring Your Own Device (BYOD)

TECHNOLOGY SPOTLIGHT

Strategies and techniques for evaluating the benefits, issues, risks and possible mitigation for Bring Your Own Device (BYOD)

Traditionally, businesses considered information technology a service they owned and provided through their infrastructure. However, consumerization is changing that. Employees, contractors and customers want to interact with businesses using their own technology, how they want, when they want. Businesses that are more comfortable with traditional ways may be missing out on significant employee satisfaction and market opportunities.

The benefits of BYOD include happier and more productive employees, reduced costs in acquiring and maintaining devices and software and the ability to contact employees any time. For example, when Cisco Systems Inc. allowed its employees to bring in their Macs, which employees paid for and serviced, the company's costs went down 25% and user satisfaction went up 200%.

However, the use of different platforms, operating systems and versions of personal productivity software and ensuring that employee and contractor devices are appropriately secured and protected present support challenges, additional costs and increased risks. Employees and contractors who own, maintain and control their devices should adhere to the organization's policies and procedures dealing with the protection of the devices and the business data they contain. But employees may lack concern or knowledge about security and privacy when using their devices for business purposes.

This publication was originally published by The Canadian Institute of Chartered Accountants in 2012.
It has been reissued by Chartered Professional Accountants of Canada.

Businesses must realize that the users' equipment is theirs and they are not under the same degree of direct business control, resulting in new issues of security and control, contractual relationships, legislative and industry compliance and employee adherence to corporate policies and procedures. Organizations may be hard pressed to ensure the protection and use of these personally owned devices meet their current control standards. Furthermore, there may be a lack of legal and moral clarity regarding how far the enterprise can go to enforce its standards of control over devices it does not own.

Organizations contemplating a BYOD strategy should develop comprehensive policies and procedures for the use of such devices. They could include specifics for the protection, use, storage, maintenance, archiving and destruction of organization information. 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.

Description

Bring your own device: allowing employees to bring their personally owned devices to use for work. The use of non-entity-owned devices will become an integral part of the entity's technology strategy and infrastructure.

Importance

Businesses are responsible for the information entrusted to them by their stakeholders (e.g. customers, employees, etc.). They are also responsible for protecting the assets and intellectual property of the organization.

Trust in the business relies on the entity's security and control over that data.

Extending and maintaining effective security and control over non-owned technology presents businesses and governments with new and significant issues and concerns.

Business Benefits

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

- Reduced investment in technology to support workers;
- Happier, more satisfied and more productive workers;
- Greater employee adoption of technology and more innovative uses;
- Creation of an infrastructure able to accommodate various platforms, thereby allowing the business to adopt varying degrees of outsourcing.

Issues and Risks	Possible Mitigation
Entity lacks specific policies, procedures or guidance to address the BYOD issues and guide 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' personal devices may be used to store confidential corporate or personal information, thereby increasing the potential for misuse.	Implement policies that limit users from storing such information on BYOD technologies.
Employee-owned devices may not have appropriate security features and may not comply with corporate security requirements.	Entity to adopt a policy that any devices carrying corporate data are subject to the company's information security policies and monitoring tools as well as periodic review by management. Connection to the corporate network should perform initial and/or regular/continuous checks on device configuration against corporate standard, and where necessary be able to fix settings prior to allowing the session to continue.
Employees may lend or otherwise permit others, such as family members, to use their devices while the devices contain entity information that may be restricted or confidential.	Effective employee training on BYOD policies (the policies are only as good as employees' awareness of the policies). Corporate applications should be encapsulated or compartmentalized, separate from user applications and data.
Employee-owned devices may be lost or stolen, thereby placing organizational business information at risk.	The right to install, modify or reconfigure the BYOD should be obtained from the employee or contractor as part of the user agreement. Connection to the corporate network should perform initial and/or regular/continuous checks on device configuration against corporate standard, and be able to fix settings to allow the session to continue.
Entities may not know exactly whom they are provisioning or onboarding when a contractor or employee brings a device to work.	Ensure the contractor or employee is the sole owner of the device. Enroll contractors and employees using two-factor authentication, possibly using the device identifier.

Issues and Risks	Possible Mitigation
Privacy risk may result from personal information on a BYOD. The entity must address control and ownership questions over data (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?).	Identify and document, by information type, specific legislative, regulatory, contractual or other obligatory requirements concerning the data and whether accessing data with, or storing data on, a BYOD meets those requirements. Develop, implement and promulgate effective policies of use and ownership as well as minimum security software and procedures.
Inability to control non-business use of employee or contractor devices.	Corporate applications should be encapsulated or compartmentalized, separate from user applications and personal data. The organization's business data should be encrypted.
Ensuring effective backup of information stored on employee or contractor devices.	Session initiation should include automatic data synchronization with corporate databases. If devices are continuously connected then regular backups, in pull or push mode, should be configured.
Employees or contractors may subscribe to a commercial backup service, such as Carbonite, and inadvertently violate laws and agreements as a result of including the organization's information in such backups.	Configure the device to automatically synchronize the organization's files on employee and contractor devices to ensure that such information is backed up as part of the organization's standard processes. Configure the device to exclude organization files in employee-initiated commercial backup.