CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Tablets and Mobile Computing

TECHNOLOGY SPOTLIGHT

Such devices offer the advantage of always having your computer with you. While the gains in flexibility are rewarding, their use increases security and privacy risks.

For example, you can flip on your tablet, scan and email an article to a colleague. Within seconds it appears in that person's email inbox. While a great advantage, the risk is that the article could have easily been proprietary corporate information.

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
Inability or difficulty in protecting business information on a lost or stolen mobile device.	Protect business data on the device by on-device encryption. Separate and isolate business application and data. Ensure the business has the ability to remotely wipe data if the device is lost or stolen. Implement mandatory use of a complex password.
The difficulty and challenges involved with securely integrating mobile devices with existing IT infrastructure (e.g. controlling access points, managing data leakage, and establishing controls to prevent users from downloading unsafe applications that contain malware into the business environment).	Development of mobile device security strategies that incorporate key elements of governance, education and monitoring. Upon connecting to a business network, procedures should require 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. Create security policies that require: • Transaction and event logging and monitoring; • Alarming for specific transactions and events; • Specific preventive and detective controls to identify and report questionable, invalid or erroneous transactions or events.
Increased use of mobile devices and their incorporation into business processes result in new concerns around device management, mobile platform development and mobile data management capabilities.	**Policy Operationalization**—creation of procedures to operationalize the mobile device policies. **Education**—implementation of 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. **Technology**—implementation of technology solutions 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.
The virtual universality of the Windows-based PC as a business platform will lessen as users increasingly opt for more portable tablets and smartphones. **An entity's investment in new or replacement technology will need to accommodate and sustain the new technologies associated with mobile devices.**	Identify the technical criteria for mobile devices to be considered for use in the business environment. Define the specific technology solutions that the entity will and will not support in terms of mobile devices and service level for each. Implement robust IT processes that support the variety of devices that the user community has or is allowed to connect.

Issues and Risks	Possible Mitigation
The cost to revamp or replace existing business processes and applications to enable them to interface with mobile technology may be significant.	Create or update the inventory of current systems and determine a timeline to take them mobile, based on technology architecture, availability of system documentation, and business needs and related factors. Consider options from full application rewrites to presentation layer modifications in terms of immediate conversion cost and ongoing maintenance and support. Abstract, as much as possible, to a core set of common application and data transport layer functions and test them thoroughly to create a re-usable library of trusted building blocks for efficient and effective migration to support additional mobile applications over time.
Business competitors can exploit mobile technology marketing and customer relationship opportunities quickly, even providing their customers and business partners with the software apps, and thereby usurp your traditional business initiatives and increase customer loyalty.	Identify client/customer mobility needs, identify possible technology solutions and create a mobile technology strategy. Based on the strategy, create tactical plans for the development of mobile apps for customer/client use. Provide clients/customers with these mobile apps to make it easier for them to access and conduct business with the organization. Consider options from full application rewrites to presentation layer modifications in terms of immediate conversion cost and ongoing maintenance and support. Abstract as much as possible to a core set of common application and data transport layer functions and test them thoroughly to create a re-usable library of trusted building blocks for efficient and effective migration to support additional mobile applications over time.
The volume and speed of change in mobile technology makes keeping pace difficult and costly. Investment in the "wrong" technology or failing to invest in the "right" technology can contribute to excessive cost write-offs or loss of market share.	Review and consider the possible mitigation strategies and initiatives as previously discussed above. Create a business case based on both implementing and not implementing mobile devices into business processes, and the impact of both scenarios on the business and its customers/clients.

Issues and Risks	Possible Mitigation
The ability to develop user interfaces to accommodate the different operating systems, screen sizes and application functionality to handle inputs and outputs for the target devices and to manage the customer experience requires business and technical skills that may not currently be available to the organization.	When considering responses to creating mobile device initiatives, include personnel considerations: availability, skill, training and related costs. Create or update the inventory of current systems and determine a timeline to take them mobile, based on technology architecture, availability of system documentation, and business needs and related factors. Consider options from full application rewrites to presentation layer modifications in terms of immediate conversion cost and ongoing maintenance and support. Abstract as much as possible to a core set of common application and data transport layer functions and test them thoroughly to create a re-usable library of trusted building blocks for efficient and effective migration to support additional mobile applications over time. Ensure staff receives training that includes a range of technologies. Create relationships with technology consultants to provide additional support when required.
Mobile devices are, by their very nature, easily lost or stolen or can be used by a perpetrator to masquerade as a valid user. **The need for mobile user identification and authentication will require more robust approaches and techniques.** **The entity's security strategy may not adequately support the requirements of a mobile computing environment.**	Develop a security strategy, supported with policies, procedures and technology solutions designed to protect data on such devices, when they hold non-public data: • Remote deletion of data; • Robust passwords supported with encryption; • Use a dumb device; i.e. all the data is actually on internal servers (e.g. private cloud); • Compartmentalize the corporate apps and data within the mobile device; • Mobile device hard drive encryption; • Two-factor authentication.
Existing infrastructure and network bandwidth may not be sufficient to accommodate the increased volume and volatility of transactions and the functionality that mobile computing requires.	Develop network strategy from end point to business servers. Consider carrier capability, capacity and QoS, as well as carrier technology path (e.g. CDMA to HSPA/HSPA+ to LTE). Ensure carrier and other network service provider service contracts address the ability to manage traffic volumes and spikes, data throttling, capacity management, scalability, availability and redundancy. Implement vendor management policies and standards for all vendors and service providers in the information and network supply chain. Implement application and network monitoring in order to identify where bottlenecks exist and manage them.

Issues and Risks	Possible Mitigation
The relationships and cost sharing in the mobile space among the key participants may not be clear. **Device manufacturers, network providers, app developers and payment processors all play a part in the value proposition that needs to be clarified to enable the customer to understand the costs of the service.**	Develop implementation packages that identify the expectations, services, content, operations, legal and other requirements that must be considered, as well as the mandatory requirements that must be met, and include these in standard contracts. Develop a comprehensive network strategy that incorporates the costs associated with all participants in the supply chain and identifies the value proposition to each stakeholder. Consider carrier capability, capacity and QoS, as well as carrier technology path (e.g. CDMA to HSPA/HSPA+ to LTE). Ensure carrier and other network service provider service contracts address the ability to manage traffic volumes and spikes, data throttling, capacity management, scalability, availability and redundancy. Implement vendor management policies and standards for all vendors and service providers in the information and network supply chain. Implement application, network and vendor monitoring in order to identify where performance, contractual, compliance, security and other issues exist, and implement processes to manage them.
The integrity, functionality, performance or security of the mobile apps that are downloaded to the mobile devices are not easily understood or verifiable by users.	Implement employee training on mobile computing policies (the policies are only as effective as employees' awareness of the policy) and related procedures. Develop baseline criteria for software, including vendor selection, vendor support, level of documentation, etc. Corporate applications should be encapsulated or compartmentalized on the mobile device, separate from user applications and data. Obtain corporate apps from a trusted source (either an app vendor or open source with signed/bound code). Assess the apps based on predefined criteria, including risks, security and control, as well as privacy.
Corporate policies that were developed and implemented in prior years may not be adequate to deal with the issues of mobile computing.	Upon connecting to the business networks, procedures should require initial and/or regular/continuous checks on device configuration against corporate standard, with the ability to remotely change or update settings prior to allowing the session to continue.

Issues and Risks	Possible Mitigation
Protection is needed against inadvertently downloading malicious codes or untrustworthy mobile apps that compromise data or expose sensitive data to a malicious user.	Apply similar antivirus strategies used on desktops (e.g., preventing unauthorized downloads, checking apps for malware before installing). Install and maintain reputable antivirus software. For corporate apps, obtain from a trusted source (either an app vendor or open source with signed/bound code). Test the apps based on risk, such as positive testing (tests the app does what it is supposed to do), negative testing (tests the app does not do anything that it is not supposed to do) and destructive tests (tests that attempt to cause the app to fail).
Inappropriate apps may be downloaded to corporate tablets.	Implement specific policies, procedures and technology solutions to limit the apps or type of apps that can be downloaded to a business tablet, and the sources from which business apps can be obtained.
Tablets and mobile devices may become contaminated with malicious code.	Establish technology-based solutions to routinely monitor access and scan mobile devices and remove malicious code and unapproved or questionable apps.