

Mobile Apps

TECHNOLOGY SPOTLIGHT

Many businesses are exploring the use of apps as part of their technology solutions. By most accounts there are more than 500,000 apps available for mobile devices.

Most are developed by independent organizations and while many are subject to review by the mobile device manufacturer, users should be cognizant of their responsibility to ensure the proprietary quality and integrity of the application prior to adopting it for use within their organization. Many apps are designed for personal use; others have a more business focus. However, when apps are downloaded and integrated into a business process, the degree of reliance placed on them must be considered. How much due diligence, oversight and control considerations would you associate with a 99¢ app, let alone a free one?

Exercise caution when using apps in a business context.

Description

An app is a term used to describe an application program that can be downloaded to an iPhone, iPad, PlayBook or similar device.

Frequently the mobile devices on which the apps are run are owned by an employee or contractor and not the business despite being used for business purposes (see also BYOD).

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

Importance

Mobile apps, when they form an integral component of a business process, such as scheduling meetings, sending email messages, maintaining a contact list or performing front-end accounting processes, are a reflection of the business and its image.

Some apps may not have the required level of documentation to permit the business to adequately assess the app's features and capabilities and its appropriateness for a specific business process.

Apps are available from a number of sources, some of which may be questionable and even result in malware being inadvertently downloaded to the mobile device and ultimately the business's technology infrastructure.

Business Benefits

Businesses may benefit from integrating apps into certain business processes, particularly those that are customer facing:

- Restaurants can benefit from point of presence apps that identify their business in various searches and provide information and menus for perusal;
- Mapping apps that allow patrons to locate your business;
- Restaurant apps that allow patrons to make reservations;
- Tax apps that ease the process of collecting information.

The key is customers will know what the business does, where it is located and how they can get there. In addition, they can obtain and use this information anytime and from anywhere.

Issues and Risks	Possible Mitigation
Apps may be used for inappropriate, unproductive or inessential purposes.	Develop policies and procedures regarding the use of apps for business purposes, including specific criteria that must be met.
Employees may be unaware of the apps that the business is using to promote to their customers/clients, and their purpose.	Inform employees of business apps that are available to customers and clients to download, and their purpose. Encourage customers to use company apps as a means of marketing the business and gaining customer loyalty.
Employees may download inappropriate apps to business devices. There is not a list of apps approved for use on company or user-owned devices.	Create a list of apps suitable for the business and approved by the company. Inform employees of business apps that they may download and their purpose. Only permit employees to download apps from the approved list. Create a corporate secure app store and inform employees that the approved apps may be downloaded from the company's secure app store.

Issues and Risks	Possible Mitigation
<p>Employees may identify and request additional apps.</p>	<p>Develop and implement consistent policies and procedures to evaluate app requests and assess potential solutions. If appropriate, approve their use and add the new apps to the list of apps allowed for business use.</p>
<p>Commonly requested/used apps are not identified, tested and pre-approved.</p>	<p>As appropriate, identify commonly used apps based on criteria such as business, industry, technology, etc., to test and pre-approve.</p> <p>Create a business app store whereby employees and contractors can obtain information on apps and download pre-approved apps.</p>
<p>Apps that are not aligned with the business objectives, strategy or image may be requested.</p>	<p>Create policies and procedures to evaluate apps from business, technical, security and privacy perspectives.</p> <p>Create policies and procedures for the self-provisioning of business apps from the business app store.</p>
<p>Consistent policies and procedures have not been developed to address the identification, selection, acquisition and use of apps for business purposes.</p>	<p>Create policies and procedures to evaluate apps from business, technical, security and privacy perspectives.</p> <p>Integrate the policies with those of the app store.</p>
<p>Lost or stolen devices that contain apps may present a security embarrassment or reputational risk to the business.</p>	<p>Install software that entities have pre-approved and that enables the business to remotely wipe sections of the employee or business device should it be lost or stolen.</p> <p>Protect data on the device by on-device encryption, secure applications and the enforcement of password complexity policies.</p> <p>Use only apps that comply with the organization's security policies.</p>
<p>The integrity, functionality, performance or security of the mobile apps that are downloaded to the mobile devices are not easily verifiable.</p>	<p>Establish policies and procedures regarding the selection of apps, the requirements and standards that must be met and the qualifications of app vendors.</p> <p>Create a process to test apps and approve them for business use.</p> <p>If practical and necessary limit the uses that can be made of products acquired from the app stores.</p>

Issues and Risks	Possible Mitigation
<p>Protection is needed against inadvertently downloading malicious codes or untrustworthy apps that may compromise data or expose sensitive data to a malicious user or provide unauthorized access to sensitive information.</p>	<p>Create an employee awareness program to promulgate app policies, procedures and standards.</p> <p>Apply similar antivirus strategies used on desktops (e.g., preventing unauthorized downloads, checking apps for malware before installing).</p> <p>Install reputable antivirus software.</p> <p>For corporate apps, obtain from a trusted source (either app vendor or open source with signed/bound code).</p> <p>Create a policy supported with procedures requiring testing to meet business standards prior to approval.</p> <p>If practical and necessary limit the uses that can be made of products acquired from the app store.</p>
<p>Inappropriate or illegal apps may be downloaded to business phones or tablets.</p>	<p>Create specific policies, procedures and technology solutions to limit the apps or type of apps that can be downloaded to a business tablet.</p> <p>Develop a technology solution to wipe unapproved apps from business devices.</p> <p>If practical and necessary limit the uses that can be made of products acquired from the app store.</p>

The matrices accompanying each Technology Spotlight are designed to create interest and awareness of some of the benefits, risks, issues and risk-mitigation strategies and techniques and are not designed to provide an exhaustive list of issues, risks or solutions. Readers are cautioned to seek professional assistance when addressing these technologies.

2012 © The Canadian Institute of Chartered Accountants