Is a Bring Your Own Device (BYOD) Program the Right Choice for Your Organization?

Privacy and Security Risks of a BYOD Program

Office of the Privacy Commissioner of Canada

Office of the Information and Privacy Commissioner of British Columbia

Office of the Information and Privacy Commissioner of Alberta

August 2015

Table of Contents

Purpose

Bring Your Own Device or BYOD as it is commonly known, is a popular arrangement for many private sector organizations in Canada. With BYOD, however, there is an increased blurring of the lines between professional and personal lives, with employee concerns that their privacy is at risk, not to mention issues associated with consumers' personal information.

Organizations considering BYOD need to protect the enterprise information accessed from and residing on employees' mobile devices. Achieving an implementation strategy that effectively protects the enterprise information and complies with customers' and employees' privacy rights under federal and provincial legislation is a challenging exercise that involves policy, training and technical solutions.

To assist organizations, the Office of the Privacy Commissioner of Canada, the Alberta and British Columbia Information and Privacy Commissioners[1] have published these guidelines to address what organizations should consider when determining whether and how to implement BYOD.

Introduction

BYOD is an arrangement whereby an organization authorizes its employees to use personal mobile devices, such as smartphones and tablets, for both personal and business purposes. While many organizations may already allow employees to use corporate-issued devices for personal uses, in BYOD scenarios employees use their own devices for both work and personal purposes. A BYOD program can therefore blur the lines between business and personal use of a mobile device, and raise serious privacy and security concerns.

There are a number of driving factors for the adoption of BYOD programs. For example, mobile devices are now being used to carry out business functions that used to be performed using desktop computers. As well, there is an upward trend in the adoption of a diverse collection of mobile devices, such as smartphones and tablets, by individuals who are often interested in adopting the personal device of their choice for both business and personal uses. This makes a BYOD program an attractive cost management strategy and a potential means to improve employees' satisfaction and productivity. The desire to use such devices is often motivated by device-specific features that may be missing in other devices, user familiarity, or compatibility with other services that the individual uses.

Although a BYOD program can be part of an organization's cost reduction strategy, it could prove to be very costly if not properly and securely implemented. In the event of a privacy breach, an organization could potentially suffer from significant harm, including financial loss, loss of competitive advantage, and/or damage to reputation. This is especially true as the types of information that can be stored in a personal device used in the context of a BYOD program can range from important business documents, consumer personal information (including sensitive information like customer financial information), and employee personal information.

This document focuses on key privacy and security risks that should be considered when making decisions regarding a BYOD program, including whether it is appropriate for an organization to implement a BYOD program. Regardless of which province they operate in, all organizations are obliged to ensure that the personal information about customers and employees is not disclosed in an unauthorized manner and that it is securely stored.

NOTE - There are other alternatives to BYOD that have emerged, such as corporately-owned personally enabled (COPE) devices, which is where employees are issued enterprise devices for both professional and personal use. COPE may be an attempt to mitigate some of the privacy and security risks associated with BYOD, but is not necessarily more secure, as it still involves the use of a single device for professional and personal use.[2] The privacy risks associated with COPE are not covered in this document.

1. Obtaining Senior Management Commitment to Address Privacy and Security Risks

Senior management commitment is vital for an organization to be able to put in place the right skills and tool sets for unique BYOD challenges. Senior management should clearly demonstrate a commitment to identify and fully address privacy and security risks, and undertake a need and resource assessment to determine what skills and tools are required to address the unique privacy risks for its operations. Without senior management support, it may be challenging to acquire the necessary resources, implement appropriate risk mitigation strategies, and develop appropriate policies and procedures.

2. Conducting a Privacy Impact Assessment (PIA) and Threat Risk Assessment (TRA)

A Privacy Impact Assessment (PIA) and Threat Risk Assessment (TRA) should be conducted to identify and address risks associated with the collection, use, disclosure, storage, and retention of personal information. These assessments should address risks associated with the use of the underlying technology, as well as risks associated with the implementation of a BYOD program as a business process.

For example, an organization may find it desirable to restrict the use of applications (apps) and interactions with unapproved cloud services. An organization may also find that it may want to limit the use of devices for BYOD to certain employees in specific positions.

Different organizations collect, use, disclose, and retain varying types and amounts of personal information, and the sensitivity of information can vary among businesses in different sectors and even between organizations in the same sector. As such, every organization has specific privacy and security risks that need to be considered when contemplating a BYOD program, and a review of those risks may reveal that a BYOD program may not necessarily be the right solution for an organization.

While an organization may be eager to implement and adopt a BYOD program, it is important for an organization's senior management to consider whether such a program is appropriate for its organization. Using a single device to carry out both personal and business functions potentially introduces privacy and security risks that could impact both personal and corporate information. It is therefore important to assess the scale and scope of the privacy and security risks a BYOD program poses for an organization in order to determine if it is an appropriate program for that particular organization.

3. Developing, Communicating, Implementing and Enforcing a BYOD-Specific Policy

While many organizations have mobile device and security policies, it is advisable to develop, communicate, implement, and enforce a BYOD-specific policy. The policy should clearly establish the obligations and expectations of BYOD users and the organization.

The BYOD policy should be developed in consultation with appropriate departments within an organization such as information technology (IT), information management (IM), legal, finance, and human resources. The resulting policy should be easy to understand and enforceable. It should also be properly communicated to all BYOD users and kept up-to-date.

An organization is accountable for its customers' personal information and that of its employees. This includes information collected, used, or disclosed via a BYOD program. A BYOD policy should address a number of issues, including:

- User responsibilities;
- How personal information in an organization's control may be subject to reasonable and acceptable corporate monitoring on a BYOD device, and how BYOD users are informed of these monitoring practices;
- Whether geo-tracking information generated by the mobile device will be tracked by an organization;
- The privacy practices an organization has adopted in respect of the employee's personal use of a BYOD device;
- Training for BYOD users;
- Acceptable and unacceptable uses of BYOD devices;
- Sharing of devices with family members or friends;
- Application (app) management;
- Data/voice plan responsibility;
- Device and information security requirements; and
- Access requests.

A BYOD policy should also identify any restrictions to the program, such as:

- Approved devices, operating systems, operating system versions, and cloud services;
- Employee functions and roles that may not be appropriate candidates for a BYOD program;
- Classes, categories, or types of information that are not appropriate; and
- Access controls for which BYOD users can retrieve certain classes, categories, or types of information.

The policy should also examine the issues of legal discovery, how access requests received by an organization would be handled, practices related to investigations or litigation concerning information on a BYOD device, and what happens to information on the device in the event that an employee leaves the organization. It should also address the responsibilities of the organization and employees for devices that exit a BYOD program (including if an employee changes their device, if a device is reported lost or stolen, or if an employee leaves an organization).

In considering all of the above issues, an organization should implement a BYOD program in a manner that factors in the organization's information management requirements while balancing the privacy expectations of employees using the devices.

4. Pilot Testing a BYOD Program Prior to Roll-Out

If an organization decides to move forward with a BYOD program, it is advisable to pilot the program prior to rolling it out to the entire organization. Such a pilot project presents an opportunity to assess the risks and benefits of the program and how a BYOD program could impact the organization. It may also be a good idea to start with a single mobile platform before considering expanding the implementation to cover other platforms. Based on the results of the pilot, appropriate steps should be taken to address identified gaps prior to full implementation and training materials.

5. Develop Training Materials and Programs

Training is a vital component for implementing a successful BYOD program. Both IT professionals and users require appropriate training. IT professionals require training in relation to the implementation and use of appropriate technical security controls including Mobile Device Management (MDM) software. Users require training to understand the organizations' expectations as outlined in appropriate policies. Among other things, the training materials should adequately address privacy and security, and training opportunities should be regularly delivered and updated. Users must have the opportunity to ask questions related to the use of their devices, and provide resources for obtaining assistance in the event that they have questions or concerns in the future.

Training should cover a number of issues to educate BYOD stakeholders to be able to manage risks that include, but are not limited to, the following:

- Mobile device administration;
- Storage and retention;
- Encryption;
- Patch and software vulnerability management;
- Managing apps and app configuration;
- Authentication and authorization;
- Malware protection and response;
- Incident management; and
- Asset management and inventory control.

6. Demonstrating Accountability

In a BYOD scenario, device management or administration presents significant challenges. Mobile device owners have administrative rights on their devices and are thus able to configure the device, modify or change device settings, or install and uninstall software or apps at any time. While this may be reasonable where the individual owner is only using a device for his or her own purposes, the issue of device administration is complex when a single device is used for both business and personal purposes.

In a BYOD program, if an employee has full administrative rights for all the information on the device, an organization may not be able to appropriately demonstrate accountability for the information under its control or in its custody. In addition, connecting a personal device to an organization's network may pose significant privacy and security risks, such as corporate network security integrity.

If an organization still wishes to proceed with a BYOD program, it should consider implementing MDM software to manage mobile devices that connect to the corporate network. MDM functionality typically includes over-the-air distribution of apps, data, and configuration settings. MDM solutions should ensure optimization of device functionality and the security of mobile communications.

Before installing MDM software on a BYOD device, the expectations of both the user and that of the organization should be documented in a BYOD policy. An agreement should be signed between devices owners and the organization that clearly articulates specific device administration activities that the organization can perform on BYOD devices.

7. Mitigating Risks Through Containerization

As a risk mitigation strategy, organizations should consider partitioning each device into two compartments or containers, a process that is often referred to as "containerization". One container should be used for business purposes, while the other container is for the employee's personal use. The containers should be created such that corporate information is logically separated from the employees' personal container and the flow of information between each container is restricted.

The chosen MDM software should ensure the organization can effectively manage and protect the container that holds the personal information in the organization's control, and any corporate approved apps. While containerization may reduce potential privacy and security risks, it does not eliminate these risks. Vulnerabilities from the personal container could potentially spill over and compromise the corporate container, and vice-versa.

Only corporate approved and authorized apps should be installed within the corporate container. In the event that an employee leaves the organization, an employee updates their personal device, or if a device is reported lost or stolen, the organization should be able to erase the container that holds corporate information, whether the device is in an organization's physical possession or remotely, in accordance with the organization's BYOD policy.

If a mobile device is "jailbroken" or "rooted", privacy and security controls can be by-passed. To "jailbreak" or "root" a device means to remove restrictions on a mobile device and allow the user elevated administration level privileges. The user can then install and uninstall specific apps that he or she will not normally be able to. Therefore, it is important to ensure a device has not been jailbroken prior to, or during, its use in an organization's BYOD program. This topic should also be covered in BYOD policies.

8. Identifying Policies and Procedures for Storage and Retention

An organization should have policies in place that govern the storage and retention of personal information in its custody or under its control. Ideally, personal information under an organization's control should be stored within an organization's corporate network, or within approved devices, and not directly on a BYOD device. An organization's use of a "*thin client*"[3] could prevent information from being stored directly on a BYOD device. A "thin client" is an IT system (such as a remote desktop service) where a device acts as a screen that displays - but does not store - information held on corporate servers.

This can help address retention concerns, since all personal information in the organization's control would remain on its servers and not on multiple personal devices brought into the workplace. Storing personal information in corporate servers will also enable the organization to meet access to personal information requests mandated by applicable legislation.

9. Implementing Encryption for Devices and Communications

Encryption requirements should be clearly addressed in a BYOD policy. Areas of consideration include device encryption, container encryption, and the encryption of the communication channels between devices or mobile apps and the corporate network. Ideally, remote connectivity to the corporate network should be done via a secure connection such as a Virtual Private Network (VPN).

For all encryption solutions, industry standard encryption algorithms should be used at a minimum, and should be in keeping with legislative privacy requirements to safeguard personal information.

In the case of user-enabled encryption, the encryption key is managed by the user and this could be problematic if the key is compromised or lost. Users should be provided with appropriate education on key management. To mitigate this risk, the encryption of a BYOD device might be centrally managed by an organization's IT department. Containerizing BYOD devices can allow an organization to manage the encryption in the corporate container. Based on available resources and operational requirements, an organization could encrypt the corporate container entirely, and/or encrypt specific data prior to storage in each corporate container (file encryption).

10. Addressing Patch and Software Vulnerabilities

Protecting against software vulnerabilities and malicious activities is another area of a BYOD program that, if not properly managed, could lead to serious privacy and security problems. If a BYOD program is pursued, organizations must clearly establish areas of responsibility for patch management and updates. If the responsibility to patch or update the operating system is left in the hands of device owners, it may not be done in a timely manner, if at all.

Attention should be given to both the Operating System (OS) as well as mobile apps that run within the device. In an "uncontainerized" device, user-installed apps and corporate apps share the same environment. Even if corporate apps have security patches installed, security vulnerabilities from user-installed apps could compromise personal information.

Organizations should consider whether it is appropriate to allow devices that are not appropriately patched or updated to connect to the organization's network.

If an organization centrally manages updates and patches, however, there may be a requirement to allow limited connections in a controlled manner to deliver relevant software updates. These practices and requirements should be periodically updated and clearly communicated to BYOD users and IT staff.

The personal information security requirements under British Columbia's *Personal Information Protection Act*, Alberta's *Personal Information Protection Act* and the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) require organizations to take reasonable steps to safeguard the personal information in their custody or control from such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

All our respective Offices have developed a joint tool *Securing Personal Information: A Self-Assessment Tool for Organizations* to help organizations address their security standards and practices.[4]

11. Managing Apps and App Configuration

With regard to apps management, if an organization implements a BYOD program, it should have a list of approved apps that can be installed, and a policy and procedure to manage how apps should be installed, updated, and removed. Centrally managing and coordinating this process can facilitate consistency with corporate policies.

Organizations should also carefully consider how apps operate when conducting their risk assessments. Misconfigured apps can lead to data leakage or unauthorized disclosure of personal information through various channels including email, SMS, call logs, contacts, etc. Some apps automatically store copies of data in the cloud while others do not require user authentication or have the option to keep users signed-in. Such configurations leave information vulnerable to compromise.

12. Supporting Effective Authentication and Authorization Practices

Authentication is the process of verifying an individual's identity prior to granting that individual access to a resource. Authorization occurs after successful authentication to allow users access to specific information within an application, according to designated permissions. Effective authentication and authorization are essential to ensure effective security controls and for demonstrating accountability. Each organization should consider balancing security and privacy with usability. The following areas of authentication should be considered.

- **Device authentication**: If a BYOD device is allowed to connect to the corporate network, such a connection should be done via an appropriate remote access method such as a VPN. An organization should also ensure each device is appropriately and securely authenticated prior to granting access to the network.

- **Container authentication:** This process can help restrict access to the corporate container to authorized individuals. By implementing authentication controls over the corporate container, an organization can mitigate the risk of unauthorized access and disclosure of personal information.

- **User Authentication:** By using MDM software, the use of strong passwords can be enforced. BYOD devices should be configured to require each user to authenticate prior to accessing the device using a strong password, or other form of authentication, approved by the organization. Although users may select their passwords or passcodes, centrally managing and coordinating this process by an organization can facilitate consistency with corporate policies. Users should be provided with guidelines for password selection and maintenance, and the organization should undertake periodic review to ensure effective user authentication is in place as required. As a safeguard, BYOD users could be authenticated using multi-factor authentication. For example, with two-factor identification, this can involve something that a BYOD user knows (such as a password) and something that the BYOD user has (such as a token, public-key certificate, or biometric).

Mobile apps that process personal information from the corporate container could also be configured to require separate user authentication. Additionally, apps should be configured to timeout after a predefined period of user inactivity and should require users to re-authenticate prior to regaining access. App features that allow users to stay logged on indefinitely should be disabled.

13. Addressing Malware Protection

Malware attacks have significantly evolved over the years in many environments, including mobile devices. Mobile devices may also have limited abilities to detect and prevent attacks. In addition, people may access information from electronic devices more quickly than when they had to rely on desktop computers, and may not take the time to read or review security and privacy-related information, particularly on small screens. These factors makes mobile devices attractive malware targets.

Common malware include worms, viruses, ransomware, adware, and trojan horses. Malware can spread through a variety of common mobile device uses including SMS (Short Message Service), email, and through web links.

Some MDM software may contain malware protection components, but an organization should ensure the implementation of such protection is in compliance with the company's security policies and standards. Malware protection should be addressed in a BYOD policy and the agreement signed between device owners and the organization.

In order to address the risks associated with malware, an organization should ensure that its network security is regularly monitored, tested, and updated. An organization's network that is compromised could potentially compromise all devices that connect to it - including those that participate in its BYOD program.

In addition, an organization should educate its BYOD users to mitigate risks associated with malware. Users should be reminded to exercise judgement as to the online sites they visit, and made aware of the dangers of clicking on suspicious links or viewing suspect SMS.

For example, malware has been observed in many free apps made available on the Internet. This risk reinforces the importance of organizations ensuring only corporate approved apps are installed within corporate containers, and that these apps are installed in accordance with the policies and procedures outlined by the organization.

14. Formalizing a BYOD Incident Management Process

It is important to recognize that things can go wrong despite the steps taken to identify and address privacy and security risks. An incident management process ensures security incidents or privacy breaches are detected, contained, reported, investigated, and corrected in a consistent and timely manner.

Each organization should have a documented incident management process. The process should be tested/exercised on a regular basis to ensure team members retain their skills and that the process works.The process should clearly outline the expectations and responsibilities of the organization and employees regarding incident management. It is critical that security incidents or privacy beaches are reported as soon as they are discovered to the organization's privacy officer. The incident management process should be covered during BYOD training.

Asset and Inventory Management

In order to have control over the management of BYOD devices, it is important to maintain an up-to-date inventory of authorized mobile devices and apps participating in the BYOD program. Such an inventory is particularly important during incident response. For instance, if a device is reported lost or stolen, information from the inventory list could assist in taking mitigating actions such as restricting the device from connecting to the corporate network.

Also, such a list could be used to prevent rogue devices from gaining access to the corporate network or information. Good inventory also demonstrates accountability and facilitates BYOD device enrollment and un-enrollment.

Conclusion

Despite some of the benefits that allowing personal devices into the workplace can bring, there are many challenges associated with considering and implementing a BYOD program. Such challenges could also be expected to multiply in a multi-platform environment. Therefore, it is important for organizations contemplating a BYOD program, as a first step, to identify and assess potential privacy and security risks in order to determine if it is an appropriate program to implement.

An assessment should not only explore whether the benefits for the organization and its employees are worth the risks. It should also factor in the costs in terms of human and financial resources to implement, monitor, and update all aspects of the BYOD program, including the privacy and security considerations.

As an additional challenge, no single technological or policy solution can address all risks. BYOD solutions are varied, not unlike those in the areas of data and information management. The complexity of a BYOD program is the integration of both personal and enterprise applications and data within a single device.

If an organization chooses to put in place a BYOD program, it should be implemented on a case-by-case basis, with an organization being able to demonstrate that it can safely, securely, and responsibly address the unique privacy and security issues for that organization.

Additional Resources

Getting Accountability Right with a Privacy Management Program and *Securing Personal Information: A Self-Assessment Tool for Organizations* are joint publications of the Office of the Privacy Commissioner of Canada, and the Offices of the Information and Privacy Commissioners of Alberta and British Columbia.

The Office of the Privacy Commissioner of Canada has developed a number of tools that will be of use to organizations to learn the basics about privacy and privacy legislation. These include: *Privacy Toolkit: A Guide for Businesses and Organizations*; *Privacy Questionnaire: Is Your Business Ready*? and a video for small- and medium-sized organizations entitled *PIPEDA for Business: What you need to know about protecting your customers' privacy*.

The Information and Privacy Commissioner of Alberta has developed the following documents which will be of assistance: *Guide for Businesses and Organizations on the Personal Information Protection Act*; *Information Privacy Rights*; and *10 Steps to Implement PIPA*.

The Information and Privacy Commissioner of British Columbia has also developed similar tools relating to BC's private sector legislation including: *What are My Organization's Responsibilities Under PIPA?* and *A Guide for Business and Organizations to BC's Personal Information Protection Act*.

Appendix A: Strategic Considerations for BYOD

Senior Management Support	- Obtain senior management support to identify privacy risks, implement risk mitigation strategies, and develop appropriate policies and procedures.
Conduct a Pilot, Privacy Impact Assessment (PIA), and Threat Risk Assessment (TRA)	- Determine if a BYOD program is the right type of practice that your organization can securely implement. - Pilot it prior to implementation to analyze the risks, determine if it still is the right choice for your organization, and address any resource gaps.
Developing, Communicating, Implementing and Enforcing a BYOD-Specific Policy	- Develop a policy by consulting widely across an organization. Identify how the policy and procedures will be reviewed, updated, communicated, and enforced.
Develop Training Materials and Programs	- Identify the specific training tools needed for BYOD users and IT staff. - Update training periodically.
Mobile Device Administration	- Develop a strategy that identifies what devices, operating systems, and operating system versions will be supported. - Factor in practices such as device containerization, or the use of a "*thin client*".
Communication and Storage	- Identify what information can be sent and stored on approved BYOD devices. Determine classes and sensitivity of information allowable.
Encryption	- Implement policies and procedures to examine issues such as device encryption, container encryption, and the encryption of the communication channels between devices or mobile apps and the corporate network.
Patch and Software Vulnerability Management	- Clearly outline how devices and software will be updated, and the roles and responsibilities of BYOD users and IT staff. - Develop procedures and training to address technical and social engineering attacks related to malware and other attacks.
Asset Management and Inventory	- Maintain an up-to-date inventory of authorized mobile devices and apps participating in the BYOD program. - Develop a list of approved apps that can be installed, and a policy and procedure to manage how apps should be installed, updated, and removed.
Authentication and Authorization	- Outline a process of authenticating an individual's identity prior to granting that individual access to a resource. - This includes device, container, and user authentication.
Incident Management Process	- Put in place an incident management process that covers the reporting, detection, identification, investigation, and correction of incidents. - Regularly test the incident management process and update accordingly.

For more information, please contact:

Office of the Privacy Commissioner of Canada

Office of the Privacy Commissioner of Canada
30 Victoria Street – 1st Floor
Gatineau, QC K1A 1H3
Toll-free: 1-800-282-1376
Phone: (819) 994-5444
Fax: (819) 994-5424
TTY: (819) 994-6591
www.priv.gc.ca

Office of the Information and Privacy Commissioner of Alberta

Office of the Information and Privacy Commissioner for Alberta
#9925 – 109 Street NW, Suite 410
Edmonton, AB T5K 2J8
(780) 422-6860 or 1-888-878-4044
Fax: (780) 422-5682
generalinfo@oipc.ab.ca
www.oipc.ab.ca

Office of the Information & Privacy Commissioner for British Columbia
Protecting privacy. Promoting transparency.

Office of the Information and Privacy Commissioner for British Columbia
PO Box 9038, Stn. Prov. Govt.
Victoria, BC V8W 9A4
(250) 387-5629
Toll Free Vancouver: (604) 660-2421
Elsewhere in BC: 1-800 663-7867
Fax: (250) 387-1696
info@oipc.bc.ca
www.oipc.bc.ca

ENDNOTES

---

[1] The Personal Information Protection and Electronic Documents Act (PIPEDA) and substantially similar provincial laws, including, Alberta's Personal Information Protection Act (PIPA); and British Columbia's Personal Information Protection Act (PIPA). *Although the* specifics of all three pieces of legislation may differ, they are all deemed to be substantially similar in content and contain the same fundamental principles.

[2] Ryan Kalember, "*Weighing COPE vs. BYOD? Don't Forget Key Security Factor: FILE*" Computerworld, July 24th, 2013.

[3] For a description of "*thin client*", please see the reference to Software as a Service (SaaS) in: National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145, "*The NIST Definition of Cloud Computing*", pg. 2. September 2011.

[4] The Office of the Privacy Commissioner of Canada (OPC), The Office of the Information and Privacy Commissioner of Alberta, and The Office of the Information and Privacy Commissioner British Columbia, "Securing Personal Information: A Self-Assessment Tool for Organizations".