BYOD:
(Bring Your Own Device)
Is Your Organization Ready?

December 2013

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario, Canada

BYOD:
(Bring Your Own Device)
Is Your Organization Ready?

TABLE OF CONTENTS

Commissioner and TELUS Foreword

Today across our nation, more than 27 million Canadians use mobile devices, including smartphones and tablets, to stay in touch, study, work and shop. With 63 per cent of all wireless service subscribers using a smartphone, Canada has the third highest level of smartphone penetration in the world. Thanks to the significant private investments of national wireless carriers such as TELUS, 99 per cent of Canadians from *coast-to-coast-to-coast* now benefit from world-leading wireless networks and technology.

The rising integration of technology into our lives is significantly changing the way we communicate, access information, and conduct our daily activities, resulting in the rapid emergence of trends that are being adopted faster than ever – in both our personal and professional lives. "Consumerization of IT" is the growing tendency for new information technologies to emerge, first in the consumer market and spread into business and government organizations.[1] As a result, Canada's business community is confronted with the escalating phenomenon of Bring Your Own Device (BYOD), which is generating new challenges in respect of information security, effective oversight and accountability.

The Information and Privacy Commissioner of Ontario and TELUS are partnering to present BYOD: (*Bring Your Own Device) Is Your Organization Ready?* Our partnership seeks to address this important and timely topic with each organization bringing complementary perspectives, expertise and practice leadership within the context of the implications of a BYOD policy on the mobile strategy of Canada's businesses.

This collaborative paper is intended to provide guidance on developing and implementing an effective BYOD and mobile development strategy. While both organizations acknowledge employee privacy issues, the principal focus of this joint paper is on an organization's information management risks and practical implementation guidance on addressing such risks.

Importantly, this is not a one-size-fits-all strategy. Once an organization makes the decision to adopt a BYOD policy, it is paramount to its successful implementation that it heeds the *Privacy by Design* principles and integrates them into its strategy. Consequently, the important principles of proactive leadership, applying systematic methods to embed privacy and security into mobile device management ecosystems, assuring end-to-end safeguards, and demonstrating operational results that accommodate and positively reflect legitimate objectives, are all critical components of a winning strategy and essential components of *Privacy by Design*.

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario

Darren Entwistle
President and CEO, TELUS

1 The emergence of consumer markets as the primary driver of information technology innovation is seen as a major IT industry shift, as large business and government organizations dominated the early decades of computer usage and development. http://en.wikipedia.org/wiki/Consumerization

1. Introduction

Canadian firms lead the world in BYOD: More than 75 per cent of Canadian businesses support employee-purchased smartphones and tablets in the workplace, according to a recent study.[2] Canadian companies outpace their global counterparts when it comes to adopting the BYOD trend and the deploying of consumer-type applications in the workplace.

At the same time, more than 58 per cent of Canadian organizations are losing corporate information through laptops, smartphones and tablets used by employees. Canada and Italy are tied for the number 1 spot in losing the most corporate data through employee-operated mobile devices.[3]

This poses a serious threat since data security is essential to information privacy. Indeed, without security, there can be no privacy. The PbD principle "End-to-End Security – *Full Lifecycle Protection*" prescribes the highest standard of data security possible. Personal data should be automatically and continuously protected throughout its lifecycle, *i.e.*, kept secure during all stages of collection, use, disclosure, and retention. Personal data should be protected by default wherever it travels or resides – on a mobile device, in a database, or somewhere in the cloud – there should be no gaps in protection or accountability for secure storage or transmission. Thus, PbD requires cradle-to-grave, secure lifecycle management of personal information, from end-to-end.

Assuring full lifecycle protection is a significant challenge for organizations today because their operations have become more data-intensive, more network-dependent, and more accessible than ever before. The explosion in the use of mobile devices such as laptops, smartphones, tablets, USB drives, and portable storage media, as well as the increasing use of personal mobile devices for business use, are causing a fundamental reassessment of how best to protect the modern enterprise's sensitive data, end-to-end.

As information processing technologies, business practices, and networked architectures become more complex and critical for enterprise operations, it is more important than ever to anticipate security risks as early as possible, and to mitigate those risks by building strong technical, administrative, and physical security practices right into the operational process of doing business, by default.

Enterprises worldwide are facing increasing pressure to allow employees to use their own tablets and smartphones and connect them to corporate networks and systems as a result of several intersecting growth trends. These include:

- Widespread consumer adoption of new mobile device brands;
- The rapid evolution of device capabilities;
- The rapid evolution of cloud and virtualization technologies;

2 Nestor E. Arellano 05 Apr 2013, "Canadian firms leading world in BYOD: Study," Computing Canada, accessed at: www.itworldcanada.com/article/canadian-firms-leading-world-in-byod-study/47616

3 Nestor E. Arellano, 19 March 2012, "Canada, Italy lead in mobile data loss," IT Business, accessed at: www.itbusiness.ca/news/canada-italy-lead-in-mobile-data-loss/17158

- The explosive growth of mobile applications; and
- A growing tech-savvy segment, highly adept at using mobile technologies.

Being able to conduct one's work on a personally-owned mobile device offers many benefits – to both employees and employers. But this blurring of the personal and business use of a mobile device raises many privacy concerns which, if not properly addressed, may result in privacy breaches, effectively turning the many benefits of BYOD into losses to the organization.

The purpose of this paper is to provide organizations with information on how they may identify and address the different privacy and security concerns raised by the growing trend towards BYOD in the workplace. There is no one-size-fits-all approach that can be adopted in a uniform manner by all organizations. Each organization must consider and assess its own unique circumstances and take steps to address privacy and security concerns in a way that is most effective for that organization.

It is important to note, however, that not all of the privacy concerns raised by BYOD are unique. Some privacy concerns overlap with those already raised by the larger trend towards a more mobile workplace in general. Indeed, BYOD is but one recent development in this larger trend. Therefore, in order not to duplicate some of the work already done on the topic of safeguarding privacy in a mobile workplace, the scope of this paper is limited to the new and unique privacy concerns raised by the recent trend towards BYOD in the workplace.[4]

2. What is BYOD?

A BYOD program involves employees using their own mobile electronic communication devices to carry out work for their employer through remote access to the organization's intranet. One goal of a BYOD program is to enable the employee to be more productive and efficient by selecting a device that best fits his/her preferences and work purposes, while at the same time ensuring data integrity and protecting the organization's information from leakage or loss.

BYOD is, however, the tip of the iceberg for organizations. The term xYOD refers to a wider array of technology options beyond BYOD, such as HYOD (Here's Your Own Device) or CYOD (Choose Your Own Device).

In an xYOD program, hardware ownership, service responsibility, payment methodology and applications all need to be considered. Organizations should seek to standardize their processes and supporting technology to cover as many of the xYOD variations as possible, but be aware of exceptions that may exist when considering a framework like PbD. The table below illustrates some of the variations of xYOD that should be considered.

4 For information on how to identify and address general privacy concerns raised by the use of mobile devices in the workplace, see the Office of the Information and Privacy Commissioner of Ontario's brochure, *Safeguarding Privacy on Mobile Devices*, available at www.ipc.on.ca/images/Resources/up-mobilewkplace.pdf

Table 1

xYOD Type	Distinction	Hardware Owner	Who Contracts for Service	Who Pays for Service
"Bring" YOD (BYOD)	Personal device	End User	End User	End User
				Organization
				Shared
"Here is" YOD (HYOD)	Multiple mobile devices available but *assigned* based on user's role	Corporation	Corporation	Organization
				Shared
"Choose" YOD (CYOD)	Users given a choice of "selective" devices	Corporation	Corporation	Organization
				Shared
		End User	Corporation	Organization
				Shared
			End User	End User
				Shared

This use of an employee-owned mobile device in the workplace differs from the use of a corporately-provided mobile device, in two ways. The first is ownership. Whereas a corporately-provided mobile device is owned by the organization that issues it, a BYOD device — what we will refer to as a BYOD — is owned by the employee. This difference in ownership results in a difference in usages between the two kinds of devices. Because a corporately-provided mobile device is owned by the organization, there is likely to be a policy in place that forbids or severely restricts non-work-related uses. On the other hand, because a BYOD is owned by the employee and not the organization he or she works for, one may assume, if not explicitly stated in a policy, that the employee will be using the device for personal, non-work-related purposes in addition to work.

Second, this situation of BYOD, where a device is used for both personal and work purposes, means that two kinds of personal information will flow through the device, both of which will require proper protection on the part of the organization that employs the individual using a BYOD. On the one hand, the device will most likely process and have access to the personal information of the clients of the organization, i.e., those individuals with whom the organization has interacted and from whom it has legitimately collected and used personal information. On the other hand, the device will also most likely process and contain personal information about the employee to whom the device belongs as well as perhaps close associates of the employee, e.g., significant others, family members, friends, etc.

3. Privacy and Information Security Risks

An organization has an obligation to protect the personal information it has collected for legitimate purposes from unintended uses or disclosures, regardless of who owns the device used to process a client's personal information.

With BYOD, an organization has less control over the devices used to process clients' personal information than in the case of corporately-owned and issued mobile devices. For example, with BYOD an organization typically has less control over:

- The kind of device, e.g., smartphone, tablet, laptop, etc.;
- The make and model of the device;
- The operating system and applications installed on the device;
- The purposes for which the device is used;
- Where and when the device is used; and
- Who uses the device.

An overview and description of common risks to organizations associated with BYOD uses are provided in the table below. Risks in bold font are of particular relevance to this paper.

Table 2: Common BYOD Risks to Organizations

Risk Type	Risk	Description
Internal	Employees can be dissatisfied by the limited selection of supported devices	Employees favor flexibility and minimal restrictions on device use
	Organizations may be exposed to liability concerns arising from device usage or implications posed by reimbursements you provide to employees	Where and when devices are used could shift liability ownership to your organization, for example, employees working onsite, who lose their phone or have them damaged, may be entitled to full device replacement paid for by the employer
	Supporting too many devices and inefficient support processes can result in incremental costs	Devices are consumer-focused, have limited 'out-of-the-box' security, and come in a variety of different platforms and makes, which inhibits IT's ability to manage and control devices

Risk Type	Risk	Description
	Undisciplined use of devices by employees can expose your organization to additional security threats	**The consumerization of devices and resulting advancement of applications, app stores, data portability (e.g. on the cloud), etc., promote user behaviour that can be incongruent with what's ultimately best for your organization**
External	Competitors may possess productivity advantages if your BYOD program is not appropriately defined and executed	A BYOD program that contains high degree of control on device usage, platforms, and applications can impede potential productivity gains and ultimately result in competitive risks for your business
	Your organization may be exposed to regulatory risks that result from data breaches, information loss, etc.	**Poor management of end point data and sensitive information can lead to regulatory exposures that could be debilitating to your business**
	Mishandling of personal information can quickly become public knowledge and severely tarnish your brand and reputation	**Privacy issues are top of mind in today's business world, as organizations are increasingly accumulating and exploiting personal information. Compromising an employee's personal information can lead to severe consequences for your organization.**
	BYOD policies may infringe on employee rights, such as requirements for overtime pay	Employees that are participating in BYOD, and are contacted outside of normal working hours for work purposes, may be entitled to overtime pay
	Increasing level of device diversity and complexity may stress your abilities to manage these devices	Proliferation of multiple devices and platforms (as the result of consumerization) minimizes the feasibility of a simple and single solution to device management. Your organization, facing significant hurdles in effectively managing devices, may incur unforeseen costs and be exposed to security concerns.

Source: Deloitte (2012) Bring Your Own Device, Unlock value for our organization. www.deloitte.ca

In addition, significant risks fall upon individual clients and employees as a consequence of an organization's poor management and control of personal information.

All risks must be identified, acknowledged, measured and assessed, prioritized, and mitigated through an organization's systematic application of PbD principles, a comprehensive security program, and an appropriate mobile device management strategy, as outlined below.

4. Are You Ready? Towards a Privacy-Aware Mobility Strategy

A privacy-aware strategy that considers the needs of the employee and the organization is required to ensure that the use of new and powerful mobile devices is possible, while at the same time protecting both the employee and the organization. The following checklist will provide a starting point from which to evaluate readiness and capabilities for a privacy-aware BYOD program.

Table 3: Readiness/Capability Checklist

#	Control	Description
1	Acceptable Use Policy	Clear and concise definitions and statements of what is allowable on the device, once access to organizational data is permitted. Additionally, this can guide the behaviour of employees, such as incident response personnel and IT teams when dealing with personal devices.
2	Privacy Policy	Inclusive of mobile device use and behaviour expected from both employees and third parties acting on behalf of the organization
3	Statement of location of use	Where the devices are expected to be used
4	Decision on operation model for Mobile Device Management[5] (MDM) – Internal versus outsourced	This will impact who has access to corporate data and personal data

5 Mobile Device Management (MDM) is a software-based solution for managing mobile devices in the workplace that can establish configuration settings, apply policies, carry out remote diagnostics, track location information, control applications, provide reporting and analytics as well as inventory management and expense controls. In cases where BYOD is supported, it provides an implementation of ring-fencing or sandboxing. Depending on the vendor or implementation, functionality will differ. Some examples of useful BYOD functionality include:

- Control over which business applications are allowed, banned, or required by devices;
- Automated backup and remote wiping of ring-fenced business areas of devices; and
- Enforcement of various security measures, e.g., password protection, file encryption, etc.

#	Control	Description
5	Decision on mobile device camera use	Statement of where and when the camera capabilities of the device are permitted. This can be enforced technically via MDM technologies.
6	Data classification and extending it to mobile device use	Absolutely critical statement as to the sensitivity of the organizational data that will be permitted on the device. It is conceivable that restricted data should never land on a mobile device.
7	Consideration of Android solutions such as SE Linux, Samsung KNOX, Cisco AnyConnect, Aruba Workspaces, etc.	Recent announcements of elevated security solutions for Android need to be proven in pilot deployments. Where they are successful, they provide strong separation of personal and corporate data.

5. From Planning to Action and Results:

Practical Steps for Organizations

The PbD framework emphasizes a proactive, systematic, results-oriented approach. The following five critical process steps have been proven to help organizations develop a responsible, accountable and effective BYOD program from the ground up.

Step 1: Establishing Requirements – End-User Segmentation
Step 2: Technology Alignment and Device Choice
Step 3: Policy Development
Step 4: Security
Step 5: Support

Step 1: Establishing Requirements – End-User Segmentation

The first step in preparing your BYOD program is to organize or group your mobile workers into segments. Look for natural usage patterns, determine location requirements and review business requirements by segment including:

- Job criticality;
- Time sensitivity;
- Value derived from mobility;
- Data access; and
- Systems access.

Unfortunately, one size does not fit all, and users within an organization have different needs. Typically, four or five different segments are sufficient for developing an effective framework to help define the technology portfolio that will be accepted into your BYOD program.

It is helpful to define end-user segments by location/type of worker, for example:

- Frequent Traveler – road warrior
- Home Office Worker – full-time remote
- Day Extender – part time remote
- Field Sales Force – road warrior
- Field Force – full-time remote
- VIP – part-time remote

Application usage: Next, you'll need to capture the application usage, systems access requirements and data access requirements for each segment in order to align the best technology portfolio with user needs. This step will also lead to the definition of polices to help govern your BYOD program and ensure a secure and productive mobile connected workforce.

This is a good time to begin carrying out a Privacy Impact Assessment (PIA) – at the very outset of the BYOD project, when all relevant teams are involved, responsibilities are allocated, and requirements are being gathered. A PIA offers a systematic method for documenting facts, objectives, privacy risks and risk-mitigation strategies and decisions throughout the entire life of the project, and should be a central activity carried out by your mobile governance committee. If your organization doesn't have a mobile governance committee, it is important to establish one prior to BYOD program rollout. These committees are typically made up of end-users from each segment, line of business management, and IT management.

Step 2: Technology Alignment and Device Choice

Do You Want To Allow Every Type of Device?

In defining the technology portfolio and device choice that will be offered in your BYOD program, it is critical to ensure that you are solving the issues that need to be addressed today, as well as in the future. With the rapid evolution of the mobility landscape, your BYOD program must be flexible enough to fulfill your productivity objectives and still appeal to end-users.

With that said, it is important to build a technology portfolio that maps the user segments to appropriate devices, device types, services and access. The technology portfolio for each end-user segment should include devices, operating systems, communication options and user environment, training and support considerations. It should also map to the application roadmap. Developing your technology portfolio geared to the user segment matrix helps to simplify the process. Without the matrix, it can become complex, especially when end-users adopt devices with multiple operating system variants, something that is often the case with Android-based devices.

In addition, it is critical that the right devices and technologies align with operating environments. For example, you don't want to allow an employee-owned device that is not sufficiently rugged to be used in a harsh environment where there is a high likelihood that its lifespan will be cut short and the employee will become frustrated. For some segments, BYOD means supplementing an existing corporate-owned device with an end-user-owned device. In this context, you may want to consider options such as implementing software to segregate the private from the business use of the end-user-owned device, and restricting personal use of the corporate owned devices that you provide to your employees.

Also, for each end-user segment and technology portfolio offered, you will need to set up systems that determine the level of access devices will have to the network, applications and corporate data. MDM is essential to ensure policy compliance of devices connecting to the corporate IT infrastructure and to eliminate security threats. In order for this to be effective, you will need a MDM with baseline functionality that generally includes asset management, encryption, password policy, remote lock/wipe, and email/Wi-Fi/VPN configuration. When enhanced mobile security and data protection are required, MDM options can include functions like mobile antivirus protection and point-to-point encryption.

Another important organizational privacy/security-enhancing data management solution to consider is virtual desktop computing infrastructure (VDI). When paired with an enterprise private cloud environment, VDI allows central management of all data assets while turning every authorized mobile device into a secure "thin" client.[6]

The parameters defining the technology portfolio are a living set of standards that may change several times a year to maintain alignment with the application roadmap, device evolution and end-user segment needs, as well as security and data loss prevention. Therefore it is important to create standards that support architectural diversity as well as a secure environment. In addition, you need to develop your own internal architectural platform expertise and knowledge, or turn to industry experts for direction and input into the process.

One area that is often overlooked is the deployment of wireless local area network (WLAN) access points on corporate campuses to support the rapid growth of mobile connected devices. With BYOD supporting device proliferation, you'll want to make sure your corporate environment supports WLAN device connectivity in order to contain your wireless data costs.

Step 3: Policy Development

Upon deciding that a BYOD program will exist within your organization, it is essential that the enterprise establish the acceptable behaviours for both the employees and the third parties acting on behalf of your organization, as early

6 A "thin client" is a "machine that relies on the server to perform the data processing. Either a dedicated thin client terminal or a regular PC or mobile device with thin client software is used to send keyboard and mouse input to the server and receive screen output in return. The thin client does not process any data; it processes only the user interface (UI). The benefits are improved maintenance and security due to central administration of the hardware and software in the datacenter." Source: www.pcmag.com/encyclopedia/term/52832/thin-client

as possible. Enterprises will generally use policy statements to codify these requirements.

Policies must be created and validated with the key stakeholders in IT, the business units, legal counsel and ultimately the individuals who will be required to comply with the policy. If users are willing to use their own self-selected device for the benefit of the enterprise, they must be required to agree to an Acceptable Use Policy. In conjunction with this, the enterprise must manage and direct the behaviour of the users of the devices to respect the policy or face disciplinary action.

A BYOD policy is a critical ingredient for effective governance, and the creation of the policy can be a trigger point for refreshing your corporate mobile policy to ensure that your organization is in compliance with applicable legislation. As part of developing your policy, you should also create a BYOD authorization and usage form that employees should be required to agree to and sign in order to participate in the BYOD program. If a personal device needs to be confiscated for discovery purposes, or if a device is lost and needs to be wiped, for example, the BYOD authorization should serve to limit the liability of the corporation when it needs to carry out certain actions that involve employee-owned devices.

You will also need to consider the confidentiality and/or privacy obligations that your organization is subject to — including your employees' rights to privacy and reasonable expectations of privacy — and make sure that these rights and obligations are clearly understood by everyone involved in formulating the BYOD policy. For example, your organization may have to preserve and retain company documents on employees' personal devices for discovery purposes. In order to respect the privacy of employees, while meeting the discovery obligations of your organization, your policy should contain measures that effectively distinguish between company documents and personal documents on employee-owned devices so that only the appropriate documents fall under the preservation and retention requirements of your organization. In addition, while uses of employee-owned devices may need to be monitored for specific business purposes, it is important to note that these purposes do not extend into the personal lives of your employees. Thus, wherever possible, tracking of personal mobile device uses should be minimized and subject to informed employee consent.

The policy should also extend to third parties acting on behalf of your organization. Your organization remains accountable for the behaviour of all third parties who manage and/or process personal information on your behalf. If you are considering use of a third party to implement any part of your BYOD policy or program, consider whether:

- The third party has appropriate security measures to protect any personal data involved;
- You have a written agreement with appropriate privacy and security provisions with the third party; and
- The third party will be accessing personal data from outside your jurisdiction, or storing it outside your jurisdiction.

Implement a Formal BYOD Policy: When you are sure of what you want to do and how, draft appropriate policies and procedures. It may be best to have more than one policy rather than trying to cover too many things in one unwieldy policy.

Consider coordinating several distinct policies that may lead to better awareness and understanding on the part of your employees.

You should also consider whether there is a need for a social media policy if BYOD leads to an increase in use of social media.

Essential components of a general BYOD policy should reflect a variety of considerations, including:

- Information security concerns;
- Data protection concerns;
- Confidentiality issues;
- Ownership issues – both of the device and of information contained on the device;
- Information regarding any tracking/monitoring – when is this permissible?
- Considerations regarding termination of employment – what to do if/when an employee leaves?
- Guidance regarding how to assess the security of Wi-Fi networks; and
- Acceptable and unacceptable behaviour.

It is also important to define the following specific criteria for your different segments:

- The systems each user segment will be allowed to access and the method of access;
- Where corporate data will reside and how data loss prevention will be handled;
- Corporate or individual liability;
- Financial responsibility and processes for handling equipment and service transactions;
- Risk mitigation and MDM deployment on end-user devices; and
- Compliance with applicable legislation.

Out of sight, out of mind is not an acceptable approach with BYOD programs. Once a policy has been developed and implemented, it must be effectively communicated and managed on an ongoing basis in order for it to be effective. End-users need clear and concise communication and guidance on what is, and what is not, allowed, as well as feedback on their compliance. In addition, if an individual's role in the organization changes such that they fall into a different end-user segment, they need to understand that the BYOD policy changes along with their change in role.

With the speed of change in mobile technologies, it is important to manage the policy lifecycle and review the policy on a regular basis to ensure that it meets the needs of your organization. This is an important task for the mobile governance committee inside your organization.

The policy lifecycle stages your organization will need to manage on an ongoing basis consist of the following:

- Deployment;
- Education;
- Review;
- Monitoring;
- Enforcement;
- Risk Mitigation; and
- Response to Non-compliance of Policies.

Lastly, make sure your BYOD policy is enforceable against your employees and third parties acting on your behalf, and follow through enforcement.

Step 4: Security

It is no surprise that security is one of the most common concerns when developing a BYOD program. According to the 2011 TELUS - *Rotman Joint Study on Canadian IT Security Practices*, laptop or mobile device theft was the second most common type of security incident or breach and was reported by 22 per cent of organizations. When you consider the significant costs of addressing and recovering from data breaches, including regulatory penalties, mobile device security needs to be considered and dealt with diligently.

Each device is an endpoint that can become a security threat, the nature of which varies based on the type of data being accessed and the type of device being used. Therefore, a minimum starting point for any security program is a MDM solution with sufficient use of the policies available within that system.

For BYOD programs to work, it is critical that the mobile ecosystem is effectively secured. This requires a thorough assessment of the operating environment and includes the development of a solution that provides for:

- Asset and identity management;
- Local storage controls;
- Removable media controls;
- Network access levels;
- Network application controls;
- Corporate vs. personal app controls;
- Permissions;
- Authentication;
- Password settings;
- Move, add and change management;
- Device health management;
- Unauthorized usage alerts;
- Data loss prevention; and
- Web and messaging security.

Particular attention should be given to assessing and documenting risks in:

- Information security (operating system compromise due to malware, device misuse, and information spillover risks);
- Operations security (personal devices may divulge information about a user when conducting specific activities in certain environments); and
- Transmission security (protections to mitigate transmission interception).

The task of ensuring adequate security for business and personal information will be facilitated if you have already specified levels of information security for each category of data, application, and user segments that address privacy obligations, confidentiality obligations, and the secrecy associated with your trade. Salient technical issues to consider include:

- How will you ensure your employees' own devices have appropriate anti-virus, password, encryption and firewalls?
- Consider PINs, passwords and the ability to ring-fence data;[7]
- Consider Mobile Device Management options; and
- How will you ensure that any loss, theft or misuse of the device is reported back to you?

Once the administrative controls are in place, it is important that technical and procedural compliance checks be put into place. There will always be a segment of the user base that will deliberately, though not necessarily maliciously, subvert security and privacy controls. That group must be controlled with technical detection and preventative controls. Containerization solutions offered by some third party vendors on mobile operating systems provide one means of separating personal data from an organization's data; essentially protecting both. Other MDM solutions provide a means to manage the data arriving on the device — even what may be collected by the device. Technical controls will be what auditors look for, primarily to ensure that organizations are performing their due diligence responsibilities with regard to protecting sensitive data and personal privacy, thus reducing overall liability for the organization.

You may also wish to consider BYOD in the context of your data retention policy. Consistent with data subject rights, corporate obligations and written policies, your organization may need to keep records of which employees worked on what projects, and whether they are using their own devices. These records may be relevant for ensuring compliance with your privacy obligations for personal information access requests, and in supporting and enforcing records retention and destruction requirements, wherever the data may be stored. Ensure that any segregation software, if used, allows you to wipe out only the business information.

7 **Ring-fencing or Sandboxing:** Ring-fencing or sandboxing is a technique used to delineate an area of a device for a particular purpose. In the case of BYOD, this technique can be used to enforce a separation between personal and business uses of the device by allowing only specific applications and areas of the file system to be used for work-related purposes. Although the employee owns the device, these applications and areas of the device would, in effect, be controlled by the organization. As a result, the organization could mandate the use of applications in line with its BYOD or mobile device policy. The separation of the device into personal and business areas also allows for the business information stored on the device, including any personal information of clients, to be deleted or wiped in the case of a change in employment or device without affecting the employee's own applications or personal information.

Ensure that you have consent before you delete any employee's private information held on the device. It would be prudent to document the process for employees to safeguard their personal data if/when the organization wipes the device.

Step 5: Support

End-user segmentation plays a critical role in defining the support levels that will be required as part of your BYOD program. Factors such as job criticality, time sensitivity and the value mobility delivers all help quantify the service levels and investment required to support each segment in your BYOD program, as well as your corporate mobility program and every combination in between.

For users who require high availability and whose jobs are highly time-sensitive, you will want to consider a service level that provides for issue resolution typically within two to four hours, as well as potential on-site support and same day or 24-hour device replacement, based on their location.

For day extenders who are not performing mission-critical tasks, self-service support through the support line may be sufficient.

These two examples demonstrate the range of support that may be required for BYOD programs. It is important to set the expectation of support levels with each user and establish the process by which they communicate incident requests. If users attempt to use an unauthorized support channel, they must be quickly redirected.

Support costs are a significant component of end-user operations and corporate operations expenses. Deviating from the established support channels can dramatically increase the total cost of the BYOD program.

Support levels should also be reassessed on a frequent basis with the mobile committee to ensure that your mobile connected workforce remains productive.

6. Conclusion

The technology related to BYOD is moving quickly, and the focus will become less about MDM and more about Mobile Content Management[8] (MCM). Organizations will need to totally rethink the way they manage their data. This will, in turn, protect intellectual property and assets. Taking a holistic approach to data management will be key. Personal cloud storage will usher in a time where the device accessing the data will become irrelevant and users will have a collection of devices all accessing the same storage point. How that data is secured will become the primary focus. As users introduce more consumer applications within the enterprise, the likelihood for a major security issue increases. Mobile apps will eclipse traditional applications. Corporate IT/Security departments will also be required to rethink their role within this process. No longer will they be the gatekeeper between the user and the infrastructure. They will need to move towards a place where they facilitate the access and the data that users are requesting while at the same time, protecting corporate information assets.

BYOD is an unstoppable trend, offering new benefits and risks – notably data security risks — to organizations of all sizes. Fortunately, we do not need to sacrifice privacy at the expense of security — abandon zero-sum models in favour of the doubly-enabling positive sum. It is possible to manage both benefits and risks in an optimal way by adopting a comprehensive PbD approach. Five key steps to an effective BYOD policy are outlined in this document. When applied, these steps demonstrate foundational PbD principles such as proactivity, embedded methods, positive-sum results, and end-to-end security safeguards with no loss of functionality.

Note: The views expressed in this paper are intended to provide general guidance only and are not intended to be specific recommendations for any particular organization or type of organization. The Information and Privacy Commissioner of Ontario and TELUS make no claims as to the reliability or accuracy of any information contained herein and accept no responsibility for any errors or omissions.

8 A Mobile Content Management system (MCMs) is a type of content management system (CMS) capable of storing and delivering content and services to mobile devices, such as mobile phones, smartphones, and PDAs. MCM systems may be discrete systems, or may exist as features, modules or add-ons of larger content management systems capable of multi-channel content delivery. Mobile content delivery has unique, specific constraints including widely variable device capacities, small screen size, limited wireless bandwidth, small storage capacity, and comparatively weak device processors.

A Synopsis of BYOD and Your Organization

Introduction

As an emerging enterprise mobility trend, BYOD will require organizations to investigate the available options and develop a cohesive response for their user community. BYOD, as a user initiated phenomenon, will often force organizations to adapt quickly. Organizations need to prepare in advance and recognize that the diversity of implementation options will have a ripple effect throughout their organization. While common IT project requirements like security and compliance can be expected, privacy considerations will impose their own set of requirements.

Successful BYOD Programs

A five-step process is recommended for developing a cohesive strategy that will meet the needs of users and the organization when it comes to privacy and other deliverables. While developing a user-orientated program, organizations should take the opportunity to streamline and validate the process they use with respect to corporately paid devices. Here are the five steps recommended for a successful BYOD program.

Step 1: Requirement Documentation

- Not all users are alike — start segmenting users and identifying groups with common needs such as: what systems do they use or how mobile do they need to be?
- Engage your Privacy Office from the outset to ensure their participation in this project.

Step 2: Technology Selection

- How do you want to manage your users and their data access? While a MDM system provides a minimum level of control, other options like Virtual Desktops or on-device software may be used to enhance security and data privacy.
- Make sure your corporate environment supports WLAN device connectivity and management.

Step 3: Policy Development

- Policies need be created by a delegation of company resources, not just IT. Key participants would include: HR, Legal, Security and Privacy.
- End-users need clear and concise communication on an acceptable-use policy, before entering a BYOD program.

Step 4: Security

- MDM technology is only effective if policies are established, implemented and supported.
- While traditional IT security standards may be the starting point, mobility will have its own set of unique capabilities that need to be addressed.

Step 5: Support

- The non-standardized nature of BYOD users will increase the frequency of support calls. Process and capabilities need to be established early to ensure success.

Conclusion

BYOD programs can provide significant benefits to an organization, ranging from higher user satisfaction to greater productivity working with advanced devices. The nature of new technology and processes can pose a risk to an organization if not correctly managed. Using the five principles presented above, organizations can minimize risk concerns around data security and user privacy.

Resources

Absalom, R. (2012). International Data Privacy Legislation Review: A Guide for BYI Policies; Enterprise Mobile Strategy must account for parameters set by local data privacy laws.

Arellano, N. (2013). "Canadian firms leading world in BYOD: Study," *Computing Canada*, accessed at: www.itworldcanada.com/article/canadian-firms-leading-world-in-byod-study/47616#ixzz2e8r8WwE9

Arellano, N. (2012). "Canada, Italy lead in mobile data loss," *IT Business*, accessed at: www.itbusiness.ca/news/canada-italy-lead-in-mobile-data-loss/17158

Arthur, C. (2013). "iOS v Android: app revenues, downloads and country breakdowns," The Guardian, accessed at: www.guardian.co.uk/technology/appsblog/2012/dec/04/ios-android-revenues-downloads-country

Aruba Networks. *The Clearpass Access Management System Overview.*

*Brodkin, Jon. "Megaupload wasn't just for pirates: angry users out of luck for now". *Arstechnica.com.* Retrieved 22 January 2012.

Cavoukian, A. (2007). *Fact Sheet 12: Encrypting Personal Health Information on Mobile Devices*, Office of the Information and Privacy Commissioner, Ontario, Canada.

Cavoukian, A. (2008) *Safeguarding Privacy in a Mobile Workplace*, Office of the Information and Privacy Commissioner, Ontario, Canada.

Cavoukian, A. (2010), *Privacy by Design, The 7 Foundational Principles*, Office of the Information and Privacy Commissioner, Ontario, Canada.

Cavoukian, A., & Prosch, M. (2010). *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users*, Office of the Information and Privacy Commissioner, Ontario, Canada.

Cavoukian, A. (2011). *Mobile Near Field Communications (NFC) "Tap 'n Go" Keep it Secure and Private*, Office of the Information and Privacy Commissioner, Ontario, Canada.

Cavoukian, A. (2011). *Safeguarding Personal Health Information When Using Mobile Devices for Research Purposes*, Office of the Information and Privacy Commissioner, Ontario, Canada.

Deloitte (2012). *Bring your own device: Unlock value for your organization.* www.deloitte.ca

Digital Services Advisory Group and Federal Chief Information Officers Council (2012). *A Toolkit to support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs*, accessed at: http://www.cio.gov/byod-toolkit.pdf

Flood, G., & Week, I. (2013). *BYOD Threats Concern British Privacy Regulator.*

Hernan Barros, D., Security Solutions, TELUS, & Walid Hejazi, A. P., Rotman School of Management, University of Toronto. (2013). *TELUS-Rotman IT Security Study*.

ICO (UK). (2013). *Bring your own device (BYOD).*

ICO (UK). (2013). *New survey highlights worrying lack of guidance from employers on use of personal devices.*

Irving, J.-M., & TELUS. *"Bring Your Own Device" (BYOD) to work.*

Kaneshige, T., & CIO. (2013). *CIO Takes Action to Solve BOYD's Privacy Problem.*

Klein, K. (2013). "Mobile Apps are drawing greater scrutiny," *Privacy Scan.*

McCarthy, V. (2013). *Study: BYOx Next Big Headache for CIO's, Security Officers.*

Milrad, L. (2013). *10 legal challenges to creating a BYOD policy.*

Olvet, T. (2012). *Enabling the Mobile Enterprise in an Era of Rapid Change, IDC Analyst Connection.*

Petersen, R. (2012). *Federal Government Develops Toolkit for Bring Your Own Device.* Retrieved from http://www.educause.edu/blogs/rodney/federal-government-develops-toolkit-bring-your-own-device

Scan, P. (2013). *BYOD raises competing privacy obligations.*

Souppaya, M., & Scarfone, K. (2013). *Guidelines for Managing the Security of Mobile Devices in the Enterprise.*

Sophos CTO Gerhard Eschelbeck outlines the following tips in a recent whitepaper. http://tinyurl.com/bsfg8sd

TELUS. (2012). *Bring Your Own Device (BYOD) Cookbook.*

TELUS. (2012). *Enterprise computing: A Rapidly Changing Paradigm.*

Willis, D. (2013). *Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes.*

Office of the Information and Privacy Commissioner, Ontario, Canada
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8
Telephone: 416-326-3333
Fax: 416-325-9195
E-mail: info@ipc.on.ca
Website: www.ipc.on.ca

TELUS
25 York Street
Toronto, Ontario
Canada M5J 2V5
Website: www.telus.com/mms
www.telus.com/BusinessSecurity

Privacy by Design: www.privacybydesign.ca

December 2013

Information and Privacy Commissioner, Ontario, Canada

TELUS