mcmillan Privacy Bulletin

November 2015

Bring Your Own Device ("BYOD") Programs: Strategic Considerations to Reconcile Security and Privacy Issues

A Bring Your Own Device ("BYOD") program permits employees to use their own personal electronic devices, such as smartphones and tablets, for both business and personal purposes. This arrangement is becoming increasingly popular among Canadian organizations as a strategy to reduce costs and increase both productivity and employee satisfaction. Despite some of the benefits, BYOD arrangements raise serious security and privacy concerns if not properly and securely implemented.

Earlier this year, the Office of the Privacy Commissioner of Canada, along with the British Columbia and Alberta Information and Privacy Commissioners (together the "Commissioners") issued a joint guideline entitled "Is a Bring Your Own Device (BYOD) Program the Right Choice for Your Organization?" (the "BYOD Guideline"). The BYOD Guideline contains important recommendations that would enable organizations to reconcile organizational security concerns with their obligations pursuant to applicable privacy law.

The following highlights some of the recommendations in the BYOD Guideline for developing and implementing a robust BYOD program.

Senior Management Support

The BYOD Guideline considers senior management support critical to the implementation of an appropriate BYOD policy. A fully committed management team is equipped with the resources and authorization necessary for overcoming the procedural challenges and implementation of a risk mitigation strategy.

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

PIA and TRA are project-based assessments tailored for specific privacy and security needs of different organizations. They identify risks associated with the collection, use, disclosure, storage and retention of personal information. These assessments enable organizations to determine whether a BYOD program effectively reconciles security requirements with privacy obligations.

Developing and Implementing a BYOD-Specific Policy

The BYOD Guideline recommends that organizations develop a BYOD-specific policy that clearly addresses the obligations and expectations of program participants. It is important to widely communicate the policy to internal departments and end-users. A BYOD policy should cover issues such as the responsibilities of the organization and employees, the scope of monitoring, acceptable and unacceptable uses of BYOD devices, security requirements and access requests. Appropriate training should be provided for both users and IT staff to clarify the expectations outlined in the policy.

Mitigating Risks Through Containerization

Containerization is a risk mitigation strategy through which a BYOD device is divided into two containers or compartments: one for storing organizational data and the other for personal information. Organizations are recommended to take advantage of Mobile Device Management (MDM) software products to restrict the flow of information between each container.

Addressing Encryption, Software Vulnerabilities and Authentication Process

The BYOD Guideline recommends encryption of the flow of information between BYOD devices and the organization's network. It is also good practice to communicate the encrypted data via a secure connection such as a Virtual Private Network (VPN). Organizations should develop procedures that clearly establish areas of responsibility for software patch management, operating system

updates, and protection against vulnerabilities and malicious activities. Additionally, an effective authentication process for BYOD devices and containers is necessary to verify the identity of a user prior to granting access to organizational information.

Formalizing a BYOD Incident Management Process

Organizations should put in place a formal incident management process to address potential security incidents and privacy breaches. The process should include reporting, detection, identification, investigation and timely correction of incidents.

Takeaways for Organizations

Organizations that adopt a BYOD program must develop a carefully constructed policy and procedure that reconciles the benefits of flexibility with the need for security of organizational data and requirements under applicable privacy laws. In the event of a complaint regarding a BYOD program, organizations can expect the Commissioners to consider whether the organization has implemented the recommendations set out in the BYOD Guideline in determining whether the complaint is well-founded.

by Mitch Koczerginski and Omeed Mousavi, Student-at-Law

For more information on this topic, please contact:

Toronto Mitch Koczerginski 416.865.7262 mitch.koczerginski@mcmillan.ca