OCTOBER 2015

CYBERSECURITY BULLETIN

Borden Ladner Gervais

PRIVACY COMMISSIONERS ISSUE GUIDANCE FOR BYOD PROGRAMS

In August 2015, the Privacy Commissioners of Canada, Alberta and British Columbia issued guidelines entitled "Is a bring your own device (BYOD) program the right choice for your organization?" (the "Guidelines") to assist organizations to determine whether and how to implement a BYOD program that effectively protects an organization's information and respects the privacy rights of employees and customers. The Guidelines are important for all organizations that permit their employees to use their own computing devices for both business and personal purposes.

BYOD

Bring your own device (BYOD) – also called bring your own technology (BYOT), bring your own phone (BYOP) and bring your own PC (BYOPC) – refers to a practice of permitting employees to use their own computing devices (e.g. smartphones, tablets and laptops) for both personal and business purposes. BYOD programs are perceived to result in productivity gains, increased worker satisfaction and cost savings. BYOD programs can also present significant risks relating to privacy protection and information security, because each BYOD device is connected to the organization's IT infrastructure and to the user's personal IT services (e.g. the user's home network and Internet access services), and is used to access both the organization's sensitive and regulated data and the user's personal data.

THE GUIDELINES

The Guidelines remind that Canadian personal information protection laws require an organization to safeguard personal information in the organization's custody or control (including personal information of the organization's customers and employees) from risks such as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction. The Guidelines also remind that an organization is accountable for personal information collected, used or disclosed by the organization's personnel using BYOD devices. The Guidelines caution that a BYOD program might not be the right solution for an organization.

The Guidelines include the following recommendations for developing and implementing a BYOD program:

- **Senior Management Support:** The organization should obtain senior management commitment to identify and address privacy and security issues.
- **PIA / TRA:** The organization should conduct a privacy impact assessment (PIA) and a threat risk assessment (TRA) to identify and assess the scale and scope of privacy and security risks presented by a BYOD program, and to determine whether a BYOD program is appropriate for the organization.
- **BYOD Policy:** The organization should develop, communicate, implement and enforce a BYOD policy that clearly establishes the respective rights and obligations of the organization and of BYOD users. The Guidelines specify numerous issues to be addressed in a BYOD policy, including restrictions regarding certain kinds of employee functions or roles and certain kinds of data.
- **Training:** The organization should properly train (including readily-available training resources and periodic refresher training) all BYOD stakeholders (e.g. BYOD users and IT administrators) so that they can identify and manage security and privacy risks.
- **Mobile Device Management:** The organization should consider implementing mobile device management (MDM) software to manage mobile devices used under the BYOD program. The use of MDM software should be addressed in a BYOD policy and confirmed in an agreement between the organization and each BYOD user.
- **Communication / Storage:** The organization should consider limiting the kinds of sensitive data that may be accessed by BYOD devices, and using technologies to avoid or minimize the need to store organization data on BYOD devices and to segregate the organization's data from the user's personal data.
- **Encryption:** The organization should consider using encryption to protect the organization's data while in transit (to and from BYOD devices) and at rest (on BYOD devices).

- **Asset Management:** The organization should maintain an up-to-date inventory of authorized BYOD devices and applications that may be installed on BYOD devices.
- **Software Management:** The organization should establish policies and procedures to approve operating systems and applications that may be installed on BYOD devices, and to manage the installation, configuration, updating and removal of operating systems and applications.
- **Authentication and Authorization:** The organization should use authentication (e.g. device authentication and user authentication) and authorization procedures.
- **Malware:** The organization should use protection (including technologies and user education) against malware that might be installed on or transmitted by BYOD devices.
- **Incident Management:** The organization should establish and regularly test and update a documented incident management plan, so that security incidents and privacy breaches involving BYOD devices are detected, reported, contained, recorded, investigated and corrected in a consistent and timely manner.

COMMENT

BYOD programs may provide various benefits, but they also present significant business and legal risks, including losses and liabilities resulting from the unauthorized use or disclosure of an organization's sensitive or regulated data and liabilities for violating privacy rights. An organization can manage and mitigate those risks by designing and implementing a BYOD program that is suitable for the organization and its particular circumstances. The Guidelines provide helpful guidance for any organization considering a new BYOD program or assessing an existing BYOD program. ■

AUTHOR

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

Borden Ladner Gervais

BORDEN LADNER GERVAIS LLP
LAWYERS | PATENT & TRADEMARK AGENTS

Calgary
Centennial Place, East Tower
1900, 520 – 3rd Ave S W, Calgary, AB, Canada T2P 0R3
T 403.232.9500 | F 403.266.1395

Montréal
1000 De La Gauchetière St W, Suite 900, Montréal, QC H3B 5H4
T 514.879.1212 | F 514.954.1905

Ottawa
World Exchange Plaza, 100 Queen St, Suite 1300
Ottawa, ON, Canada K1P 1J9
T 613.237.5160 | F 613.230.8842 (Legal)
F 613.787.3558 (IP) | ipinfo@blg.com (IP)

Toronto
Scotia Plaza, 40 King St W, Toronto, ON, Canada M5H 3Y4
T 416.367.6000 | F 416.367.6749

Vancouver
1200 Waterfront Centre, 200 Burrard St, P.O. Box 48600
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415

blg.com