Member's Quarterly Winter 2018 Edition

Feature

Working Outside the Office: Privacy Concerns for Employers

Minimize data breaches and information insecurity

Michelle Henry
J.D.
Partner, Borden Ladner Gervais LLP

There have been many cases of massive data breaches, many involving incidents where an employee's mobile computing device containing personal information was lost or stolen. The increase in the number of data breach incidents can be attributed to a number of factors. For instance, many employers are incorporating flexible work arrangements in their workplaces, allowing more employees to work at home or locations other than their conventional office. Further, the increasing number of global companies means that employees are more often required to perform their job duties outside their conventional workplace. In addition to accessing personal and confidential information outside the office, employees are also required to travel with information in either electronic or paper format. Other common causes of data and privacy breaches are the insecure disposal or records and unauthorized access (i.e., snooping).

The fact is that while mobile computing devices can provide enhanced capabilities for employees, they also raise a number of privacy concerns for employers. Although many mobile devices are often stolen for the mere value of the device, personal information contained on these devices is increasingly being used for other purposes such as identity theft. Consequently, working outside the office means that employers must ensure that employees take additional steps to safeguard personal information contained on their devices.

Employers are strongly encouraged to develop policies for the protection of personal information when employees are working outside the office. The policy should provide safeguards for travelling with information, as well as safeguards for working outside the office and safe physical storage of files and other documents.

Privacy Commissions, including the Office of the Privacy Commissioner of Canada, have provided a number of guidelines for reducing the risk of a privacy breach, including the following recommendations:

- **Train employees.** While workplace policies are important, they can only be effective when employees are aware of them and the potential consequences of failing to follow the policy. Employers should have ongoing privacy and security training and awareness program so that employees fully understand their roles and responsibilities in protecting personal information.
- **Limit how employees store and save documents.** Increased employee mobility also means that employees are always looking for efficient ways to store and carry documents. Breaches due to loss or theft of unencrypted laptops, USB keys and other portable devices are now commonplace. Employers should ensure that employees use only encrypted devices to store information.
- **Protect personal information throughout its life cycle**, including the destruction of information at the end of its life cycle. Clearly set out your policies and procedures for secure destruction of personal information and ensure that they are followed. For instance, the OPC reports that it has seen a number of breaches caused by documents left behind in a move or thrown in the garbage, as well as by information not being properly erased from discarded or recycled electronics.
- **Limit access to personal information.** Employees' access to personal information should be limited to what they need to know to do their job and nothing more.
- **Maintain up-to-date software and safeguards.** While this may be viewed as common sense, it is worth reminding employers that, no matter how small you are, it remains imperative that you have a systematic and documented process that is properly implemented to proactively monitor your system, to mitigate threats, to ensure security-related patches are applied in a timely manner and to ensure software is properly updated.

Member's Quarterly Winter 2018 Edition

Feature continued

Developing a response plan is also extremely important and should include reporting requirements. Employees should be made aware that any loss or theft of personal information must be reported immediately. If personal information has been lost through theft, the police should also be notified. The loss or theft of personal information should also be reported to the applicable privacy commissioner. In some cases, individuals whose personal information was lost or stolen will have to be notified.

Given the risks to employers in the event of a data breach, the importance of implementing policies regarding the use of mobile computing devices and educating employees about maintaining the security and confidentiality of personal information cannot be overstated.

Michelle Henry is a Partner at the Toronto office of Borden Ladner Gervais LLP and can be reached at mhenry@blg.com.