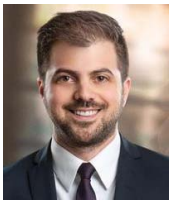
Privacy Breach Reporting: Supplying the Stick for Your Own Beating?

October 7, 2018

Author



Guillaume Laberge

Partner, Lawyer

Since the EU's *General Data Protection Regulation* ("GDPR") came into force in May 2018, the government of Canada has decided to align its security breach legislation with these new EU standards. Thus, as of November 1st 2018, organizations and businesses in Canada will be required to comply with sections 10.1 to 10.3 of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), as well as with the new *Breach of Security Safeguards Regulations*, which create a federal mandatory breach reporting regime for Canada's private sector.

However, a preliminary issue with respect to the application of these new provisions may arise regarding the extent to which they apply to private sector organizations within provinces that have adopted legislation which the federal government has found to be "*substantially similar*" to PIPEDA.

These new regulations, although applauded for providing increased protection for personal information, also have the corollary effect of imposing several hefty obligations on Canadian businesses and organizations. Such obligations include the requirement to: (i) conduct a risk assessment to determine whether the breach poses a "*real risk of significant harm*" to affected individuals; (ii) give notice to affected individuals and the Privacy Commissioner "*as soon as feasible*"; and (iii) keep records of all breaches (even those that do not meet the reporting threshold) for at least 24 months.

The record keeping policy is an important compliance mechanism of the new regulations and will inevitably result in increased costs and new challenges for businesses and organizations dealing with private information.

It seems undeniable that these new regulations will also increase the already growing interest in

cyber-risk insurance in Canada. However, it is very likely that prospective cyber liability insurers will demand access to the breach records of their future clients in order to properly assess the risk. Businesses considering the possibility of outsourcing certain services to a service provider may also consider requesting access to the service provider's breach records as part of their due diligence. Likewise, parties to a corporate transaction may also wish to review the breach records to help determine the risks associated with the transaction.

One thing is now certain: denial is no longer an option for cyber security risk management. Businesses will have to ensure that they adopt safeguard measures and internal procedures that will allow them to adequately detect, react to, and defuse security breaches. Technology security specialists and lawyers will be valuable allies to help organizations and businesses navigate these new waters.