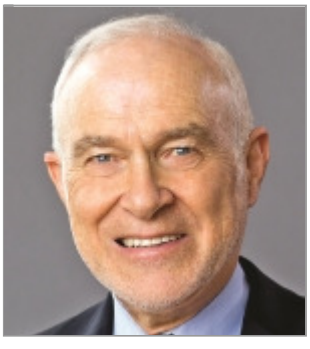
THE LAWYER'S DAILY

The Lawyer's Daily | 111 Gordon Baker Road, Suite 900 | Toronto, ON M2H 3R1 | www.thelawyersdaily.ca
Phone: (905) 415-5889 | Fax: (905) 479-3758 | John.Carson@lexisnexis.ca

Business

Proposed breach regulations refocus risk management, incident response protocols

By **David Young**



David Young

(October 16, 2017, 8:54 AM EDT) -- Publication of the federal government's proposed *Breach of Security Safeguards Regulations* on Sept. 2, for a 30-day consultation period, provides important guidance to organizations and their internal compliance personnel. The proposed regulations, while potentially subject to adjustment following the consultation, provide a significant road map as to the full scope of the new incident breach reporting provisions under the *Personal Information Protection and Electronic Documents Act* (PIPEDA). These provisions will create new liability risks and compliance costs for organizations.

The final regulations, together with the new PIPEDA rules, will come into force in the spring of 2018.

The new PIPEDA breach reporting rules were enacted under the *Digital Privacy Act*, passed by Parliament in 2015 but not yet in force. They will require organizations to report to the Office of the Privacy Commissioner of Canada (OPC) any breach of security safeguards involving personal information that poses a "real risk of significant harm" to individuals and notification of the breach to those individuals. They also require notification of other organizations and government entities where such notification could reduce or mitigate the risk of harm. Finally, the new rules require organizations to maintain records of *all* breaches, irrespective of whether or not they are reported.

Reports to the OPC must include: a description of the breach and the cause, if known; when it occurred; personal information affected by the breach; the number of persons at risk; and steps that the organization is taking to reduce the risk and to notify affected persons. When notifying individuals the organization must also indicate steps that it can take to reduce the risk or mitigate the harm as well as information about the organization's complaint process and the right to file a complaint with the OPC.

The new breach reporting rules will align significantly with those under the European Union's General Data Protection Regulation (GDPR) which also comes into force in the spring of next year. This alignment will be important in ensuring PIPEDA's equivalent protection status under the EU's privacy laws, a requirement for the free flow of personal information between Canada and Europe.

The new rules will have the effect of shining a light on an organization's breach response procedures. To ensure full compliance with the new rules and to address the potential risks of non-compliance, a review and likely enhancement of those procedures will be required. At a minimum, such procedures must encompass investigation and assessment of a breach and the risks posed by it, taking steps to mitigate the effect of the breach, notification of

affected individuals and reporting to the OPC, and creating a record of such steps available for inspection by the OPC.

It will be critical for organizations to ensure effective and efficient internal reporting and escalation of breaches including training of employees. More broadly, the new rules will dictate a new focus on management of legal risks, compliance and incident response, as well as a review of the organization's information security and data governance systems.

Not only will the mandated records be available for inspection by the OPC, but they also may be accessible to litigation parties through discovery as well as to third parties conducting due diligence on the organization such as in a potential acquisition, or in connection with contracting for provision of services by the organization.

Failure to comply with the new breach reporting rules can result in penalties of up to $100,000 per offence and, potentially, a civil claim under PIPEDA's private right of action. More significantly, the new breach reporting framework will provide potential litigants, including class action plaintiffs, with greater scope for launching and pursuing significant monetary damage claims against affected organizations. These potential exposures will dictate not only enhancement of response procedures but also a heightened focus on enterprise risk management including threat and risk assessments, security controls and the need for cyber liability insurance.

The new record-keeping requirement is significant in that in effect it requires the organization to document all actions taken in response to a breach, including investigation and assessment. While the act contains no definition of a "breach of security safeguards" for which records must be kept, it is expected that guidance from the OPC will provided in this regard. Guidance also will be provided regarding the nature of records required to be kept.

While it can be expected that some adjustments will be made to the proposed regulations following the now-concluded consultation, it is unlikely that there will be major changes. Consequently, organizations and their internal compliance staff should be using the guidance provided by the proposed regulations not only to understand the key specifics of the mandatory reporting, notification and record-keeping requirements but also the impact on their internal breach response procedures and more broadly their risk management and data governance systems.

David Young is principal at David Young Law, *a privacy and regulatory counsel practice in Toronto*.

P*hoto credit / BeeBright ISTOCKPHOTO.COM*