November 13, 2019

ARTICLE

Mandatory Breach Reporting: Lessons from Year One

The federal Privacy Commissioner (OPC) recently published a blog post detailing certain trends that have emerged in the first year since mandatory breach reporting came into effect for organizations subject to the *Personal Information and Electronic Documents Act* (PIPEDA), as well as certain tips for organizations for responding to a breach.

On November 1, 2018, breach reporting in certain situations became mandatory under PIPEDA. As we detailed in our previous bulletin, "Canadian Personal Information Security Breach Obligations – Preparing for Compliance", an organization that suffers any "breach of security safeguards" involving personal information under its control must maintain a record of the breach. If the breach presents a "real risk of significant harm to an individual", the organization must also promptly report the breach to the OPC and give notice of the breach to affected individuals, certain other organizations and government institutions. Since November 1, 2018, an organization's knowing contravention of the personal information security breach reporting, notification (to individuals, but not to organizations or government institutions) and record-keeping obligations is an offence punishable by a fine of up to $100,000.

Mandatory Breach Reporting by the Numbers

- In the year since mandatory breach reporting came into effect, the OPC received over 680 breach reports. This was six times more than it received in the year prior, when breach reporting was not mandatory. The OPC expressed that this volume was significantly greater than what it had been expecting in light of the Alberta privacy commissioner's experience when mandatory breach reporting was implemented under its *Personal Information Protection Act*.
- Based on the breach reports received, over 28 million Canadians have been impacted by a data breach over the last year.
- Unauthorized access was involved in 58 per cent of reported breaches, many of which were the result of social engineering hacks, such as phishing and impersonation, and employee snooping. More than 20 per cent of the reported breaches were the result of accidental disclosure, such as where documents containing personal information were accidentally sent to the wrong person or left where they could be seen by unauthorized people, and other reports involved documents or devices being lost (12 per cent) or stolen (8 per cent).

Key Takeaways for Businesses

The OPC reaffirms that being proactive about privacy concerns and data breach management plans can help minimize the risk that an eventual breach will lead to significant harm, both to individuals and to the organization. As such, we continue to encourage all organizations to incorporate privacy and data protection considerations and safeguards into every step of their processes and procedures so that they are properly prepared to manage and respond to any eventual data breach that occurs. This can include various measures, such as:

- Breach Response. Establish a written breach response and recordkeeping procedure that includes designating who will be making and documenting decisions about reporting breach incidents to the OPC, notifying affected individuals and making timely disclosures to other interested persons (*i.e.* investors). A detailed breach record can help an organization determine if it has any particular vulnerabilities or systemic issues that could be better addressed;
- Internal accountability. Designate individuals within the organization to be responsible for data protection initiatives and incorporate privacy considerations into all policies and practices, and regularly review these to ensure that they reflect the latest guidance;
- Privacy training. Conduct regular privacy training and regularly update privacy training modules to ensure these reflect the latest guidance. This can allow an organization to ensure that employees are aware of how to properly handle personal information, what constitutes a breach and what the process is for reporting a breach internally;
- External accountability. Include data protection obligations and commitments in outsourcing agreements with third party service providers and, where useful, audit rights with respect to the practices and safeguards employed by those third parties. For instance, in a recent report of findings, the Commissioner noted that an organization had fulfilled its accountability requirements when transferring personal information to a service provider for processing by using a security addendum that was deemed "sufficient to ensure a level of protection that was comparable to that which would be required under [PIPEDA]." The security addendum included a list of specific safeguard requirements, such as: "(i) implementing measures to protect against compromise of its systems, networks and data files; (ii) encryption of personal information in transit and at rest; (iii) maintaining technical safeguards through patches, etc.; (iv) logging and alerts to monitor systems access; (v) limiting access to those who need it ; (vi) training and supervision of employees to ensure compliance with security requirements; [and] (vii) detailed incident response and notification requirements" (See PIPEDA Report of Findings #2019-003).

For more details about best practices for complying with PIPEDA's mandatory breach reporting obligations, see our previous bulletins, "Privacy Commissioner's Guidance for Compliance with PIPEDA's Breach of Security Safeguards Obligations" and "Canadian Personal Information Security Breach Obligations – Preparing for Compliance".

By: Lauren Phizicky

Services: Cybersecurity, Privacy & Data Protection