Happy Anniversary! Privacy Commissioner releases observations and findings after one year of mandatory data breach reporting

November 8, 2019

By Amanda Branch

It has been one full year of mandatory data breach reporting under the *Personal Information Protection and Electronics Documents Act* (PIPEDA). The Office of the Privacy Commissioner of Canada (the OPC) has written a blog post, setting out observations of what it has learned over the past year and what businesses need to know.

Mandatory breach notification under PIPEDA came in to force on November 1, 2018. Before that time, breach reporting to the OPC was done on a voluntary basis. Since November 2018, organizations subject to PIPEDA who suffer a breach of security safeguards that gives rise to a "real risk of significant harm" are required to (i) report the incident to the Office of the Privacy Commissioner of Canada; (ii) notify affected individuals; and (iii) notify any other third party that is in a position to mitigate the risk of harm to affected individuals. While organizations are not required to report a breach that does not give rise to a real risk of significant harm, they are required to keep a record of all breaches for a minimum of two years – and the OPC has the authority to proactively inspect those records.

Looking at the numbers

Here are some key statistics:

- Since November 1, 2018, the OPC has received 680 breach reports;
- According to those reports, the number of Canadians affected by a data breach is well over 28 million; and
- The majority of breaches are due to unauthorized access (58%) and accidental disclosure (roughly 22%), with loss of a computer, storage drive or paper files accounting for about 12% of breach reports, and theft of documents or devices accounting for 8% of breach reports.

Employee snooping and social engineering hacks are the key factors behind breaches resulting from unauthorized access. “Accidental disclosure” occurred in instances where documents containing personal information were provided to the wrong individual or were left behind accidentally.

Tips from the OPC – preventing and responding to a breach.

The OPC has provided some helpful tips for organizations to keep in mind.

First, help reduce privacy breaches at your organization:

- **Know your data**. Know what personal information you have, where it is, what you are doing with it and who has access to it.
- **Know your vulnerabilities**. Conduct risk assessments and penetration tests within your organization, but go beyond technical vulnerabilities to assess whether third parties or employees could be weak spots.
- **Know your industry**. Be aware of other breaches in your industry as attackers often use the same attacks against multiple organizations. The OPC notes a trend in the telecommunication industry is fraud through impersonation where bad actors have convinced customer service agents that they are an account holder. Once a company addresses the issue, the attackers move on to a different telecommunications provider.

If your organization does suffer a data breach, the OPC has the following tips on how to respond:

- **Contain it**. Stop the unauthorized access and shut down the system that was breached.
- **Conduct an initial breach investigation**. Designate an individual with the authority and knowledge to conduct the investigation and make initial recommendations.
- **Involve others as appropriate**. Determine who needs to be made aware of the incident internally (and externally, if necessary).
- **Exercise caution with evidence** to ensure you do not accidentally destroy evidence that may be valuable in determining the cause of the breach or which may allow you to take appropriate corrective action.

Please see here for our article on the OPC's mandatory breach reporting guidance for organizations.