ONE-YEAR ANNIVERSARY OF MANDATORY DATA BREACH REPORTING: LESSONS THE OPC HAS LEARNED AND WHAT BUSINESSES NEED TO KNOW

Posted on November 11, 2019

Categories: Insights, Publications

November 1, 2019 marked a year since reporting data breaches became mandatory under the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**").

Prior to November 1, 2018, cautious organizations reported data breaches to the Office of the Privacy Commissioner of Canada ("**OPC**") on a voluntary basis. Since November 1, 2018, amendments to PIPEDA impose mandatory reporting and notification requirements on organizations subject to PIPEDA. You can read more about these requirements in our November 2018 bulletin.

Since making reporting data breaches mandatory, the OPC has seen a significant increase in the number of reported data breaches. The OPC recently published a blog post sharing keys lessons learned since implementing these changes.

Number and trends of data breaches reported

The OPC received a total of 680 data breach reports in the first 12 months — an increase of six times the volume received during the same period a year earlier. Over 28 million Canadians were reportedly affected by the data breaches.

A majority of the reported data breaches involved unauthorized access to personal information, as shown in the chart below. The main causes of breaches resulting from unauthorized access are employee snooping and social engineering hacks, such as phishing and impersonation.

More than one in five reported data breaches involved cases of accidental disclosure, such as situations where documents with personal information were provided to the wrong person.

The OPC also saw an increase in reports involving data breaches that affected a small number of people. In some instances, the reported breach was a personalized attack on a single individual. The OPC commended this reporting practice, because a data breach can pose a real risk of significant harm even when it affects only

one individual.

-

Type of Incident	Total Breach Reports
Accidental Disclosure	147
Loss	82
Theft	54
Unauthorized Access	397
Grand Total	**680**

Reducing the risk of data breaches

The increase in reported data breaches is a reminder for businesses to think carefully about the safeguards they have in place to protect individuals' personal information.

The OPC shared the following tips to help businesses reduce the risk of data breaches:

- **Understanding the data before protecting it**

  Businesses should know the type of personal information they have, where it is stored and what they are doing with it. It is also important to understand when and how personal information is gathered, where it comes from, where it goes, and who has access to it.

- **Awareness of vulnerabilities**

  Businesses should carry out risk and vulnerability assessments to identify threats to privacy. The OPC advises businesses to not only focus on technical vulnerabilities, but also to determine whether employees are aware of their privacy responsibilities and the risks involved, and whether third parties collecting personal information on the business' behalf have sufficient protections.

- **Awareness of breaches in your industry**

  Hackers typically employ similar methods to attack businesses in the same industry. It is important for businesses to stay alert and informed of attacks in their industry to avoid being the next victim.

In addition to the above, organizations should carefully review the breach reporting and notification requirements with relevant stakeholders, including senior leadership. Employees should continue to receive training, with emphasis on the need to identify and escalate any breaches to the appropriate person(s) within the organization as soon as possible. Consider hosting a "lunch and learn" to work through the new obligations, and discuss how they may affect employees in their daily roles.

The need to establish a breach or incident response team and plan is more critical than ever, given the time-sensitive nature of the reporting and notification requirements. In the event of a suspected breach, organizations must make a number of decisions very quickly, including engaging in a particularly nuanced analysis of whether a given situation triggers the mandatory reporting and notice requirements. Organizations should take the opportunity to think through and assign roles and responsibilities prior to any potential breach, when the circumstances are significantly less rushed and stressful.

Organizations that experience a suspected or actual breach of their security safeguards are encouraged to immediately contact privacy professionals to determine whether reporting and notification is required, and to avoid incurring significant penalties for non-compliance.

by Mitch Koczeginski and Chiedza Museredza

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.