LESSONS LEARNED FROM ALBERTA'S OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER (OIPC) 11-YEAR REPORT

Posted on September 21, 2022

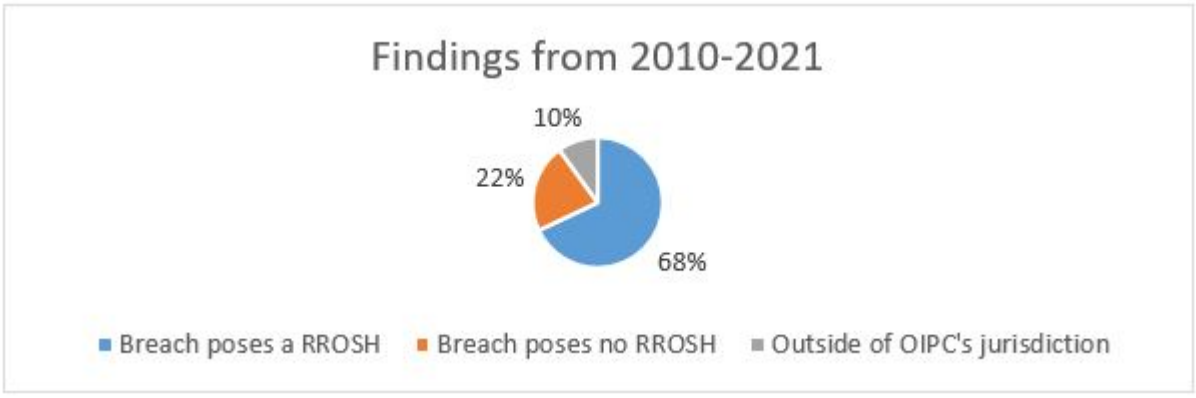
Categories: Insights, Publications

On May 1, 2010, Alberta became one of the first North American jurisdictions to require organizations to notify individuals affected by privacy breaches and to report those incidents to Alberta's OIPC. This was legislated under section 34.1 of Alberta's *Personal Information Protection Act*[1] ("**PIPA**"), which requires organizations to notify the OIPC of any privacy breach "involving the loss of or unauthorized access to or disclosure of" personal information where there exists "a real risk of significant harm" ("**RROSH**") to an individual. After receiving a breach report, section 37.1 of PIPA grants the OIPC the authority to require an organization to notify individuals for whom there is a RROSH as a result of the breach. This requirement to notify is set out in section 19.1 of the associated *Personal Information Protection Act Regulation*[2] (the "**PIPA Regulation**").

The OIPC has reflected back on this 11 year history by issuing the PIPA Breach Report 2022[3] (the "**Report**"), which summarizes the nearly 2,000 privacy breach reports reported to the OIPC between April 1, 2010 and March 31, 2021.

The OIPC Report

As outlined in the Report, OIPC received 1,977 breach reports during the 11 year period, and of these breach reports, the following determinations were made:



These breaches have led to organizations sending millions of notifications to affected individuals in the past 11 years, including 1,951,180 notifications required under PIPA between April 1, 2020 and March 31, 2021 alone.

In determining the risk a breach poses to an individual, the OIPC considers the intent or cause of the breach, the type of personal information involved, whether the data was encrypted, and the length of time the data was exposed.

The OIPC Report notes that almost all of the reported RROSH breaches involved some basic contact information of the affected individuals, such as telephone numbers or mailing addresses. However, most of the breaches involved identity, financial, and employment information, leading to the threat of identity theft, fraud, or financial loss. The Report also indicates a decrease in compromised medical information and an increase in compromised transaction information, such as purchase history, which can lead to increased vulnerability to identity theft and fraud.

The OIPC Report indicates that the industries most commonly affected by RROSH breaches are the finance, retail trade, and insurance industries, while the most commonly affected individuals are an organization's customers or clients, followed by its employees. For more information on employee breaches, see our bulletin "Stop Snooping: Alberta Privacy Commissioner Finds Employee Snooping Results in Real Risk of Harm".

Causes

The most common cause of the reported RROSH breaches were compromised electronic information systems through the installation of malware or ransomware, or through the exploitation of system vulnerabilities. The theft of physical documents, devices, or storage mediums was the second leading cause, and transmission errors through misdirected mail, emails, or faxes was the third most common.

While social engineering and phishing was the fourth leading cause of the RROSH breaches through the past decade, this vulnerability has recently become the second most common cause. As these attacks continue to

become more prevalent, companies need to be cautious about divulging sensitive information to malicious actors posing as someone else, and also ensure that their own employees are not collecting such information from customers and co-workers (unless such information is required as part of their job function or for business operations). For this reason, clear privacy policies and practices are essential.

The remaining causes of the reported breaches consist of misconfigured networks, unencrypted storage mediums, the accidental publication of personal information, and rogue employees.

Detection and Reporting

The Report indicates that organizations are taking an increasing number of days to detect and report RROSH breaches. The average overall timeline has been 90 days to detect a breach and 43 days to report it to the OIPC. The increasing timeline may be due to the insidious nature of compromised electronic information systems, the rising popularity of retaining specialized third parties to assist with breach responses, and the increasing number of other jurisdictions requiring a breach report within a specified timeframe. By comparison, PIPA does not stipulate any strict reporting timeframe.

Section 19 of the PIPA Regulation states the report to the OIPC must be in writing and include the following information:

- A description of the circumstances of the breach;
- The date on which or time-period during which the breach occurred;
- A description of the personal information involved in the breach;
- An assessment of the risk of harm to individuals because of the breach;
- An estimate of the number of individuals to whom there is a RROSH because of the breach;
- A description of any steps the organization has taken to reduce the risk of harm to individuals;
- A description of any steps the organization has taken to notify individuals of the breach; and
- The name and contact information for a person who can answer, on behalf of the organization, the OIPC's questions about the breach.

While PIPA does not provide any criteria in defining a RROSH, the OIPC has provided several helpful resources for organizations, including key steps to take in responding to a breach and information on how to report a privacy breach.

Notification

Overall, according to the OIPC, it took on average 43 days for organizations to notify affected individuals of a RROSH breach. In almost all of the RROSH breaches, organizations notified affected individuals directly through in-person meetings, telephone, mail, or email. The OIPC authorized an indirect notification in 4% of

these breaches, most commonly delivered using website postings, social media, or traditional media when the organization did not have current contact information for some of the affected individuals.

Section 37.1(7) of PIPA states than an organization is not restricted from notifying individuals on its own initiative. Further, section 19.1 of the PIPA Regulation states that notice must be given directly to the individual and include:

- A description of the circumstances of the breach;
- The date on which or time-period during which the breach occurred;
- A description of the personal information involved in the breach;
- A description of any steps the organization has taken to reduce the risk of harm; and
- The name and contact information for a person who can answer, on behalf of the organization, questions about the breach.

Looking Forward

As the number of data breaches that pose a RROSH rise each year, organizations need to be aware of the requirement to report certain breaches to the OIPC and promptly notify affected individuals. Timely notifications are imperative in mitigating the potentially devastating impacts of compromised personal information.

It is important for companies to be prepared for a breach prior to one occurring so that they are ready to take immediate action upon learning of a breach. The OIPC echoes this warning by noting that the proactive implementation of safeguards is the most effective way to protect individuals from the potential harm of privacy breaches. The Report recommends that organizations:

- Implement regular and/or immediate security patching on networks, servers, and devices;
- Sign up for and review updates from cybersecurity agencies and other professionals to keep updated on new threats and possible solutions to protect the organization's information technology infrastructure;
- Train employees regularly on detecting phishing or social engineering attempts; and
- Train employees regularly on protecting personal information contained in laptops or paper documents.

If your organization has any questions about the Report or how you can evaluate, develop, and implement appropriate privacy and data protection policies and procedures to comply with applicable privacy laws and PIPA's current requirements, a member of our Privacy & Data Protection Group would be pleased to assist.

by Julia Loney, Gordana Ivanovic, Kristen Shaw, & Stephen Johnson (Summer Law Student)

[1] *Personal Information Protection Act*, c. P-6.5 2003.

[2] Personal Information Protection Act Regulation, AB Reg 366/2003.
[3] Available online: PIPA-Breach-Report-2022.pdf (oipc.ab.ca).

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.