Road to PIPA Week 17: What happens if there is a breach?

Risk assessment is not only about identifying the privacy risks in your organisation and ensuring that controls are in place to mitigate those risks. It is important for your organisation's Privacy Committee to also consider what happens if those controls fail to protect personal information.

This tool is designed to guide your organisation's Privacy Committee through an exercise to review the risks and harms to both individuals and the organisation. Use the PIA findings and Mitigation Plan to identify common scenarios in your organisation where security might be breached and discuss how that might affect stakeholders.

Read through the scenarios provided below, and consider how the facts might play out in your organization. As you do, consider the following questions:

- What might failure to protect personal information from misuse look like in your organisation?
- Considering the type of personal information you use, what are the potential harms to individuals?
- What are the potential harms to the organisation overall?*

Scenario 1.

An employee of a financial services company forwards an email containing the personal records of 2000 individuals to an unauthorised employee, who should not have been privy to the information.

The employee realizes the error and refers the matter to the organizations' Privacy Officer (PO). Upon review, the PO determines that the personal records comprised of full names, addresses, and bank account details. However, the records were not forwarded any further, and the internal employee was subject to a confidentiality agreement in their job duties. The PO requests the deletion of the records, along with an affirmation of the deletion.

Having considered the facts, the PO defined the matter as a low tier breach, given the determination that it is very unlikely there would be a risk of harm or any adverse effect to the individuals.

Scenario 2.

An employee of a medical insurance company forwards an email containing the personal records of 100 individuals to an unauthorised third-party vendor.

The employee realizes the error and refers the matter to the organisations Privacy Officer (PO). Upon review, the PO determines that the personal records comprised of full names, addresses, patient account numbers, health insurance numbers, and prescription information.

Based on facts, the PO requests that the third-party vendor deletes the records and provide an affirmation of the completion of the request, but does not receive a response. Having considered the adverse effect, the PO defined the matter as a breach due to the risk of harm and directly notified PrivCom and the affected individuals, while meeting all notice requirements under S.14 of PIPA.

**Harms identified may extend beyond PIPA or privacy issues.*