Human Resources Legislative Update

Mandatory Breach Notification Comes to Canada: What To Do About It

Date: April 12, 2018

It's been a long time coming, but we finally know that mandatory breach notification is coming to Canada.

Beginning November 1, 2018, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) will require notification to affected individuals and the federal Privacy Commissioner when a security incident involving personal information results in a "real risk of significant harm."

Of all the things that this significant change might lead you to do, your priority should be to revisit your incident response policy (IRP) to align it with the change and otherwise ensure it is reflective of good practice. A good IRP will set you up for excellent incident response. Done right, it is less a "policy" than it is a handbook or guide – centralizing authority to make key decisions, defining key decision points and providing **practical guidance** to structure your incident response.

The following are some of the incident response practice points that we have been recommending to our clients. Now is a good time to consider building them into your IRP:

- **Facilitate internal reporting.** Does your policy define what an "incident" is? Does it require all incidents to be reported to a "SPOC" – a single point of contact? Does it forbid those who become aware of an incident from communicating with affected individuals before reporting internally?
- **Give the SPOC adequate authority to contain.** Does your policy, for example, specify that the SPOC can (where reasonable and necessary) temporarily suspend certain IT services.
- **Set the terms for investigation.** Does your policy indicate that your objective is to take "all reasonable steps" to investigate cause and exposure? It should. Does your policy identify common assumptions and challenge decision-makers to question them? It should.
- **Enable a quick response.** Does your policy include an appendix with key numbers? Does it incorporate a contingency plan for communicating when your regular communications services are down? Does it list pre-approved vendors?
- **Control communications.** Does your policy include a protocol for reporting to regulators and notifying individuals? Does it do enough to ensure the incident response team keeps its dealings confidential? Does it contemplate the involvement of counsel and set out how communication should occur with a view to future privilege claims?
- **Notification.** Does your policy set out when you will provide for credit monitoring? Does it encourage you to communicate a meaningful remedial plan without platitudes that signal you don't care?

Organizations should measure their policies against these practice points and the new PIPEDA requirements. If you would like our assistance with this, please contact us or another member of the firm.