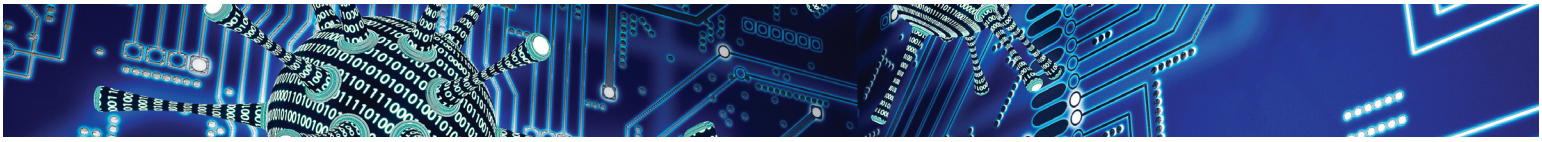

MANDATORY DATA BREACH NOTIFICATION IS COMING: IS YOUR ORGANIZATION READY?

By: Imran Ahmad and Roya Baryole[1]

The *Digital Privacy Act* amends the *Personal Information Protection and Electronic Documents Act ("PIPEDA")* in several key ways. While most of the provisions of the *Digital Privacy Act* came into force in June 2015, those relating to breach reporting, notification and record keeping are anticipated to come into force later this year once the associated Regulations come into force.

We provide below an overview of these changes and what organizations should be doing to ensure they comply.

What Are the Key Changes?

1. Mandatory Data Breach Notification

Imagine a scenario where an employee loses a corporate laptop containing customer information at a trade show. Once the regulations are adopted, the corporation will be required to not only inform the Office of the Privacy Commissioner (the "Commissioner"), but may also be required to inform the customers whose information was lost, potentially increasing the corporation's litigation exposure as a result of the incident.

In cases where an organization reasonably believes that a breach of its security measures creates "a real risk of significant harm to an individual," mandatory data breach notification requirements will be enforced under section 10.1 of *PIPEDA*. This assessment will be based on the sensitivity of the personal information that was compromised; the probability that the personal information has been, is being or will be misused; and "any other prescribed factor." "Significant harm" is defined in a broad manner and includes (among other harms) bodily harm, humiliation, damage to reputation or relationships, financial loss and identity theft.

The notification to affected individuals must be "conspicuous," must be given directly to the individual provided it is feasible to do so, and must be given as soon as feasible. The notification must allow the individual to understand the significance of the breach and to take whatever steps possible to mitigate or reduce the risk of harm.

Also under PIPEDA, where notice is given to affected individuals, the Act will require organizations to notify other organizations, such as government institutions and credit bureaus, as soon as feasible, if the notifying organization believes that the other organization can reduce risks or mitigate harm. These disclosures will not require consent.

2. Security Breach Logs

Another key change will be that organizations will be required to keep records of all security breaches involving personal information. While it is currently unclear what level of materiality will require logging requirements, what is clear is that the Commissioner will have the right to request and review these records at any time.

3. Stiff Penalties for Non-Compliance

In the most extreme cases, fines of up to $100,000 may be imposed for knowingly violating the mandatory breach notification requirements or breach record keeping requirements. Since the Regulations have not yet been finalized, it is unclear at this time whether a violation will include a single incident (e.g. a single failure to notify all individuals) or each incident (e.g. each failure to notify each individual). What is clear is that the Commissioner now has the ability to impose significant fines for non-compliance.

What Does This Mean for Organizations?

Given the imminence of these changes, organizations should conduct a review of and update their existing protocols and policies to ensure that they have the ability to detect, respond and report data breach incidents internally.

Organizations should also assess what type information they hold (e.g., personal information, intellectual property, supplier data, etc.) and how they would respond should that information be compromised. This is why having a data breach incident response plan that includes establishing broad thresholds for notification to the Commissioner and affected individuals is important.

Given that the mandatory data breach notification requirement will result in an increased risk of litigation, organizations should ensure that their insurance coverage is sufficient and that they have a discussion with their legal counsel about when steps can be taken to mitigate their litigation exposure before a breach occurs (e.g., employee training, security audits, identifying cybersecurity vendors of record, etc.).

While the new requirements may appear to be burdensome, the good news is that the applicable standard is one of "reasonableness", not absolute perfection. Accordingly, organizations should take steps to ensure compliance and make sure to document them appropriately.

[1] Imran Ahmad is a Partner at the law firm Miller Thomson LLP and leads the cybersecurity law practice and can be reached at iahmad@millerthomson.com. Roya Baryole is a corporate lawyer with an interest in cybersecurity and can be reached at roya.baryole@gmail.com.

Contact

Imran Ahmad
Partner
416.597.6031
iahmad@millerthomson.com