Case In Point

Federal Privacy Commissioner Uses Ashley Madison Incident to Promote Good Information Governance

Date: August 25, 2016

Organizations subject to Canadian privacy law should be aware that the Office of the Privacy Commissioner of Canada (together with the Australian Information Commissioner) recently issued a report on the 2015 breach of the Ashley Madison website – a breach that affected nearly 35 million individuals who had used the online dating site for adults seeking discreet affairs.

The OPC used its investigation to articulate some very broadly-applicable information governance requirements. Specifically, it said that the company that operates Ashley Madison breached the safeguarding requirement in PIPEDA by failing to:

- develop and maintain a *documented* information security framework
- develop, maintain and administer an “explicit” risk management process that featured periodic and proactive assessments of security threats
- administer adequate role-based data security training for *all staff*.

Formality clearly matters to the OPC. It noted that the company employed numerous security controls, but adopted them “without due consideration of the risks faced” and without a coherent framework to assure their proper management.

The OPC also found a breach of the safeguarding requirement by failing to prevent the following two “security weaknesses”:

- use of single factor authentication for VPN remote access
- poor key and password management practices (which led to the storage of keys and passwords in plain text).

While the OPC’s conclusion is based, in part, on the “highly sensitive” personal information with which the company was entrusted, the identification of these weakness is nonetheless notable. The OPC also identified intrusion detection as another security weakness, though it did not rely on it in concluding the company was in breach.

The report addresses other narrower issues including record retention, the charging of fees for deletion of records, the collection and authentication of user e-mail addresses and transparency and openness. Organizations should also note the aspects of the Ashley Madison matter with which the OPC did *not* take issue – the company’s incident response and breach remediation efforts, for example. These efforts are briefly summarized in the report.