Upcoming PIPEDA Changes

What is changing and what to do about it

UZADO

Get UZED to IT

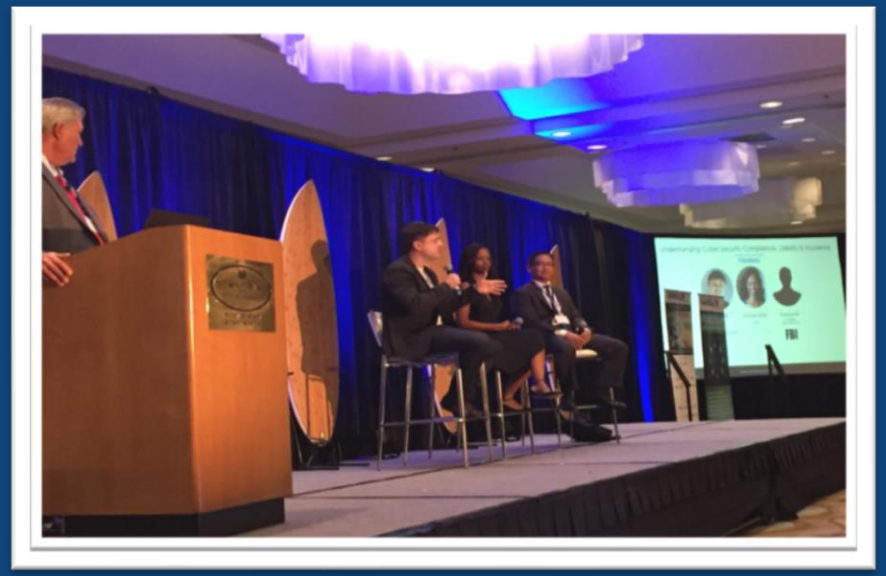
Danny Pehar

Global Television Cyber Security Expert

Danny Pehar

Working with the FBI

Cyber Task Force



Why is this industry so challenging and what does it mean to you?

The human factor

The way we do business keeps changing

The government is involved

The evolution of crime

The skills gap

PIPEDA Overview

The ***Personal Information Protection and Electronic Documents Act*** **(PIPEDA)** - January 1, 2004

PIPEDA was "enacted to alleviate consumer concerns about privacy and to allow Canada's business community to compete in the global digital economy.

PIPEDA is a Canadian law relating to data privacy. It governs how private sector organizations collect, use, and disclose personal information in the course of commercial business.

Any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

On June 18, 2015, Canada passed into law Bill S-4 - The Digital Privacy Act, which made a number of important amendments to PIPEDA.

Provisions of the law relating to mandatory breach reporting and record-keeping – November 1st 2018

Are you ready for November 1, 2018 ?

Breach readiness in Canada is going to take on a whole new meaning:

Federal regulations regarding **mandatory notification, reporting and record keeping of privacy breaches** under Canada's federal data protection law, the **Personal Information Protection and Electronic Documents Act (PIPEDA)**, will come into effect on **November 1, 2018**

In addition to details on record keeping in relation to breaches, the new regulations will detail:

- ✓ **Who** needs to be notified of the breach
- ✓ **What** breaches require notification
- ✓ **When** notification needs to happen
- ✓ **How** the notification needs to be delivered

These changes will present new risks, costs, and challenges for organizations including: **incident response, compliance, legal risk management and additional liability and regulatory exposures**

PIPEDA - Who to notify?

- PIPEDA will include a mandatory requirement for organizations to give notice to affected individuals and to the Commissioner about privacy breaches in certain circumstances

- The current Commissioner is **Daniel Therrien**, who was appointed on June 5, 2014. The Privacy Commissioner of Canada reports to the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

PIPEDA – What to notify on?

- Section 10.1 of PIPEDA will require organizations to notify individuals, and report to the Commissioner, all breaches where it is reasonable to believe that the breach creates a "real risk of significant harm to the individual"

- PIPEDA defines "significant harm" as including, among other harms, humiliation, damage to reputation or relationships and identity theft

- A "real risk" requires consideration of the sensitivity of the information, the probability of misuse, and any other prescribed factor

- No additional factors have been prescribed in the proposed regulations, although the Commissioner will be publishing guidance in respect of this issue

PIPEDA – **When** to notify?

The notice to individuals and the report to the Commissioner must be given in the prescribed form "as soon as feasible" after it is determined that a breach occurred.

PIPEDA – **How** to notify the Commissioner?

A report to the Commissioner must be made in writing and contain the following information:

- The circumstances of the breach and, if known, the cause
- The date or period during which the breach occurred
- The personal information that is the subject of the breach
- An estimate of the number of individuals at a real risk of significant harm
- The steps that the organization has taken to reduce risk or mitigate harm to individuals
- The steps that the organization has taken or intends to take to notify affected individuals
- The name and contact information of a person who can answer, on behalf of the organization, the Commissioner's questions about the breach

PIPEDA – **How** to notify: **Direct** Notification to Affected Individuals

Direct notification to individuals must be given in one of the following 4 ways:

- By email or any other secure form of communication if the affected individual has consented to receiving information from the organization in that manner
- By letter delivered to the last known home address of the affected individual
- By telephone
- In person

PIPEDA – **How** to notify: **Indirect** Notification to Affected Individuals

- The giving of direct notification would cause further harm to the affected individual
- The cost of giving direct notification is prohibitive for the organization
- The organization does not have contact information for the affected individual or the information that it has is out of date
- Indirect notification may be given only by either a conspicuous message, posted on the organization's website for at least 90 days
- By means of an advertisement that is likely to reach the affected individuals

PIPEDA – Record Keeping

- Organizations must maintain a record of every breach of security safeguards for a minimum of 24 months after the day on which the organization determines that the breach has occurred
- Upon request, organizations must provide the Commissioner with such records. The Commissioner may publish information from such records if it would be in the public interest
- The Commissioner may also launch an investigation or audit based on the information in the breach file
- The record must contain any information pertaining to the breach that enables the Commissioner to verify compliance with the breach notification and reporting provisions
- The Commissioner must be able to validate whether the organization notified and reported breaches as required in each case

PIPEDA – Record Keeping

- The purpose of the record-keeping obligation is "to provide the Commissioner with an ability to determine whether or not organizations are tracking all breaches and complying with the requirements to report significant breaches and notify affected individuals."

- It is a good idea to include in breach records of the information which led the organization to conclude that there was no real risk of significant harm, and that it was therefore not required notify individuals

- Organizations subject to PIPEDA should brace for the potential that their breach files will be requested by the Commissioner

- There is no threshold associated with the record-keeping obligation
- A record of all breaches must be kept, irrespective of whether they give rise to a real risk of significant harm
- Nor is there any threshold before an organization would be required to provide its 'breach file' to the Commissioner

What Does It Mean?

Organizations must now, more than ever, ensure that they have in place internal safeguards, policies and procedures to adequately detect, escalate and respond to privacy incidents.

How To Prepare?

Information Gathering - include asset lists, network diagrams, systems information, etc. The more insight into the structure of your organization, the more you prepare

Response Processes - Review the current response process and tailor it as needed. If there is no response process in place, provide a net new protocol

Familiarization - Review various types of breaches that the organization may experience and ensure that the management and the response team feel comfortable that they have:
(a) sufficient information should they need to call for outside assistance;
(b) a better understanding of what a breach might look like, so that they know when to engage outside assistance

Response and Escalation Processes - Build out initial notification and escalation processes

Thank you!

www.Uzado.com