Edelman

PIPEDA:
THE NEW PRIVACY LANDSCAPE AND WHAT IT MEANS FOR YOUR BUSINESS

KEY PRIVACY LEGISLATION AMENDED

On November 1, 2018, the federal government brought into force key provisions of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). These new regulations will drive increased public awareness around the way companies acquire, process, store, and share consumer data—with significant legal, financial, and reputational risks attached.

THREE KEY CHANGES

Under the new provisions of PIPEDA, Canadian organizations are now legally obligated to:

Report	Record	Notify
• Report a breach of security safeguards to the Privacy Commissioner.	• Keep a comprehensive record of every breach of security safeguards for two years.	• Notify impacted stakeholders when there is a real risk of significant harm.

BY THE NUMBERS

1 IN 5

The number of Canadian businesses that reported a data breach last year

(Source: Statistics Canada)

80%

Percent of global consumers who believe failure to keep customer information secure impacts trust in a company

(Source: Edelman Trust Barometer)

IMPACT FOR BUSINESS

While the updates to PIPEDA provide enhanced protection for consumers, they also generate increased risks for businesses:

Legal
Compliance has become more complicated and expensive. The more stringent guidelines also create greater potential for litigation.

Financial
In addition to compliance costs, failure to comply with the new regulations can trigger fines up to $100,000.

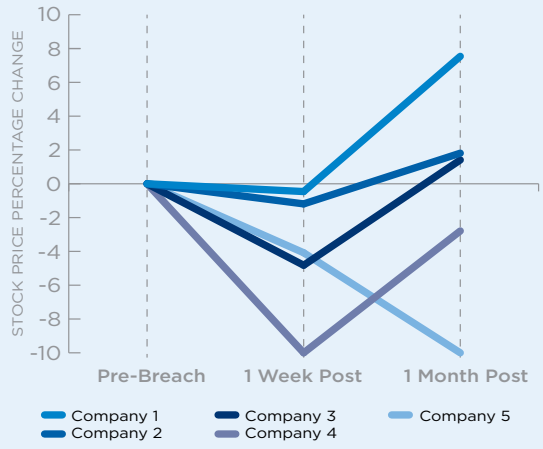
Reputational
The mandatory reporting and notification requirements mean organizations face greater exposure and scrutiny from internal and external stakeholders.

STEPS FOR ORGANIZATIONS TO TAKE

Proactive dialogue around privacy	To inform that dialogue, organizations should develop a core privacy narrative that enables them to frame the conversation, demonstrate good governance, and highlight their commitment to data security best practices.
Plan for a data security incident	Develop a data incident communications response plan that guides communication with key stakeholders, including customers, employees, business partners, government officials, and media.
Practice, practice, practice	The communications response team should simulate a high-risk, high-probability scenario that tests the response plan and bolsters team performance.

COMMUNICATIONS & STOCK PERFORMANCE

In a study of the five largest breaches over the past five years among Fortune 500 companies, Edelman analyzed the relationship between communications strategies and stock price performance, identifying several best practices for responding to a breach:



Companies with the best stock price performance immediately after a breach took the following key steps:

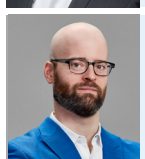
- **Proactive Disclosure**
  Notified relevant stakeholders before a third party.
- **Participated in the Public Conversation**
  Engaged with media to ensure company key messages were captured in coverage.
- **C-Suite Visibility**
  Ensured a member of the C-suite (CEO, CIO, CISO) demonstrated accountability over the breach.
- **Regular Cadence of Communication**
  Provided ongoing and transparent updates to impacted stakeholders.
- **Centralized Information Hub**
  Created a centralized source of information about the breach (e.g. microsite, call centre).

For more information on how changes to PIPEDA may impact your business, please contact Edelman's Crisis and Risk Practice Group.

CALGARY
John Larsen
General Manager, Calgary
Executive Vice President, Crisis & Risk National Lead
C: 403-860-1421 | E: john.larsen@edelman.com

VANCOUVER
Ari Indyk
Vice President, Crisis & Risk
C: 778-223-7067 | E: ari.indyk@edelman.com

TORONTO | OTTAWA
Greg Vanier
Senior Vice President, Crisis & Risk Data Security Lead
C: 647-527-5314 | E: greg.vanier@edelman.com



MONTREAL
Samuel Lessard
Account Director, Crisis & Risk
C: 514-863-5795 | E: samuel.lessard@edelman.com