All Canadian organizations will soon be mandated by law to report cyber data breaches that cause significant harm to affected parties and regulators. What do they need to know to prepare?

**Big Changes, Big Mandate**
Canadian organizations should expect some major changes to current data breach notification requirements. Industry privacy and security expectations are continually increasing. Industry best practices are also evolving, requiring organizations to constantly improve data privacy and protection controls.

With the number of breach litigation cases before the courts on the rise, Canada is no longer “immune” to data privacy and security requirements. Organizations are discovering the hard way that affected parties will hold you accountable. The US bill for handling Personally Identifiable Information (PII) is being adopted as an industry standard. Many Canadian organizations are following suit. While there is currently no specific legislative or regulatory requirement to do so, should sensitive information such as healthcare and financial data be exposed in a data breach, Canadian organizations would be compelled to notify affected individuals. Additionally, other forms of sensitive data, such as loyalty rewards points, social media accounts and passwords, are also viewed by the industry as sensitive and organizations are disclosing breaches involving this data, despite not having formal requirements to do so. Keeping pace with increased breach notification in Canada is a rise in litigation stemming from these breaches.

**What to Expect**
As of June 2015, Bill S-4, the Digital Privacy Act, introduced some major amendments to the Canadian privacy act PIPEDA. Those changes pertaining to security breaches are pending regulations and federal government approvals. As per the new mandate, any organizations that experience a data breach are expected to:

- **Determine a “real risk of significant harm”** to anyone whose personal information was involved;
- **Notify individuals** “as soon as feasible” if they face any “real risk of significant harm” to allow organizations to address containment and urgent issues;
- **Report a breach** with any “real risk of significant harm” to the Privacy Commissioner, as soon as feasible;
- **Notify any third party** that the organization experiencing the breach believes is in a position to mitigate the risk of harm; and
- **Maintain a record** of the data breach and make these records available to the Privacy Commissioner.

**What you need to determine now**
- What the new notification and reporting obligations are
- How you will fulfil these obligations
- What is required to keep the necessary detailed records
- Who is accountable for keeping these records

**Federal Requirements**
Introduced in 2014, The Directive on Privacy Practices requires all federal government institutions to report designated breaches of personal information to the Treasury Board Secretariat, the Office of the Privacy Commission of Canada (OPC), and to notify those parties affected. This will mean a commensurate increase in costs with the effort to track down those individuals affected.

Guidelines issued by the Canadian Securities Administrators (CSA) stipulate that organizations should report cyber security incidents to stockholders, even if the company may only be at risk of an incident.

In the US, there are instances of regulators suing organizations due to perceived cyber security gaps that result in an unfair business practice, such as making statements about data security/privacy that are not viewed as true. Although there are no documented Canadian cases, this precedent is expected to be followed in Canada some time in the future.

**Voluntary Requirements**
Breach requirements are ultimately driven by legal, regulatory and contract requirements. With a few exceptions, the current existing data breach reporting program in Canada established by the OPC, came into effect in 2007 and is voluntary. Many organizations who are subject to PIPEDA participate as a matter of best practice.

Organizations can report “material” data breaches to the OPC and notify affected parties, customers, and employees where the breach poses a risk of harm. What must be included varies by province, according to their mandatory data breach frameworks. Recommendations for what may be sent in a notification to affected individuals include: information about the incident and its timing; a description of the personal information involved; what the organization will do to assist individuals; what steps individuals should take to avoid or reduce their harm; sources of information that are designed to assist individuals; contact person and information.
Provincial Requirements
Alberta is the only province in Canada to have mandatory data breach reporting requirements for all private sector organizations. These are laid out under Alberta’s Personal Information Protection Act (PIPA), which states a notification must include: a description of the circumstances of the breach; the date (or time period) of the breach; a description of the information involved in the breach; measures taken by the organization to reduce the risk of harm; and contact information for a representative who can answer questions.

Various requirements exist for 11 of the 13 provinces and territories on reporting public, private and health data breaches and notifying affected individuals. Newfoundland recently legislated mandatory reporting. Only BC, Saskatchewan and Quebec do not currently have mandatory breach reporting requirements in place.

How data breach notification impacts the costs of a data breach.
The reality of data breaches is not “if” but “when”. Is your organization prepared to deal with a breach? According to research on Canada by the Ponemon Institute, the average cost for a breach is $5.4 million. Regulatory fines and data breach-related litigation are two material factors in this cost. Both can be influenced not only by an organization’s ability to protect sensitive information prior to the breach, but also on their ability to notify affected individuals within appropriate timeframes. Failure to comply with breach requirements and industry practices may result in financial loss and irreparable damage to the reputation of your organization.

Why choose KPMG’s cyber team?
Understanding your unique legislative, regulatory and contract data breach notification requirements is a core part of developing your organization’s cyber defensible position. KPMG’s cyber team can provide greater insight into Canadian data breach notification requirements and help define your organization’s cyber defensible position.

Our global cyber team leverages the skills, experience and capabilities of 2,700 accredited practitioners to deliver security and forensic services spanning multiple geographies. Using the same tools and techniques that professional hackers use for ethical hacking and offensive security, we have tested the layers of security for a large number of clients and organizations across multiple industries. To complete our team, we include not only advisors to local, regional and federal law enforcement agencies across North America, but cyber thought leaders and authors of multiple security and forensics books that are shaping the industry.

We believe cyber security should be about what you can do – not what you can’t.

Award winning
KPMG International has been named a Leader in the Forrester Research Inc. report, The Forrester Wave™: Information Security Consulting Services, Q1 2016 achieving the highest score for current offering and strategy.

Trusted
KPMG member firms have a long list of certifications and permits to work on engagements for many of the world’s leading organizations.

KPMG’s Cyber Forensic Leader, Kevvie Fowler is a recognized leader in Data Breach Response recently publishing his latest book, Data Breach Preparation and Response: Breaches are certain, Impact is Not.

Collaborative
We facilitate and work with collaborative forums to bring together many of the best minds in the industry to collectively solve shared challenges and emerging threats.

KPMG’s I-4 forum brings together over 50 of the world’s leading organizations to talk about how to effectively deal with Cyber challenges.

Independent
Our recommendations and technical strategies are based solely on what is fit and appropriate for your business.

KPMG in Canada is not tied to any technology or software vendor.

Global, Local
KPMG is a global network of member firms with over 174,000 professionals in 155 countries with over 2,700 security practitioners globally. KPMG’s regional practices can service your local needs from information security strategy and change programs, to low level technical assessments, forensic investigations, incident response, training and ISO27001 certification.

KPMG’s Cyber Team works with organizations to help prevent, detect and respond to cyber threats.
We can help your organization be cyber resilient in the face of challenging conditions.

Contact us
Francis Beaudoin
National Technology Risk Consulting Leader
T: 514 840 2247
E: fbeaudoin@kpmg.ca

Please contact our 24/7 Cyber response hotline
1-844-KPMG-911
1 (844) 576-4911

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2018 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International.