CapriCMW

CUSTOM INSURANCE SOLUTIONS

PIPEDA Mandatory Breach Reporting Requirements

What It Means for Canadian Businesses

Did you know?

As of November 1, 2018, organizations hit by a privacy breach (that meets certain conditions) will be required to notify affected individuals and the Office of the Privacy Commissioner.

By failing to report, organization could be subject to a $100,000 fine for each individual not notified.

Canadians have long been anticipating the implementation of federal privacy breach reporting requirements. Originally passed on June 18, 2015, Bill S-4 - the Digital Privacy Act, included amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA). Most of the amendments are already in force with the exception of those pertaining to privacy breach reporting.

As of November 1, 2018, organizations hit by a privacy breach (that meets certain conditions) will be required to notify affected individuals and the Office of the Privacy Commissioner.

According to the Act, organizations must report any breach where there is a "real risk of significant harm to the individual." The term "significant harm" is defined as "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on (one's) credit record and damage to or loss of property."

How do you determine if there is a risk of significant harm?

1. Did the breach involve sensitive information?
2. Is there a strong probability that this information could be misused?
3. Could there be any financial, reputational, psychological or physical harm done?

Currently, it's up to the organization that suffers a breach to handle as they see hit (except where the provincial authority specifies requirements i.e. Office of the Information and Privacy Commissioner of Alberta). Effective November 1, 2018, it will be the responsibility of organizations to handle breaches as per the below. Few organizations have robust, written breach response plans in order to comply efficiently and effectively.

New Handling Requirements

SCENARIO 1

Incident occurs with no loss of personal data.

Action Required:

Organization to keep an internal record.

SCENARIO 2

Breach occurs with loss of personal data but it is determined that it does not pose a real risk of significant harm.

Action Required:

Organization to keep an internal record.

SCENARIO 3

Breach with loss of personal data occurs and it is determined that a real risk of significant harm exists.

Action Required:

Organization notifies the individuals affected and the Privacy Commissioner of Canada "as soon as feasible."

SCENARIO 4

A breach occurs a with loss of personal data and a real risk of significant harm and the organization **does not** provide notification as required.

The organization could be subject to a $100,000 fine for each individual not notified.

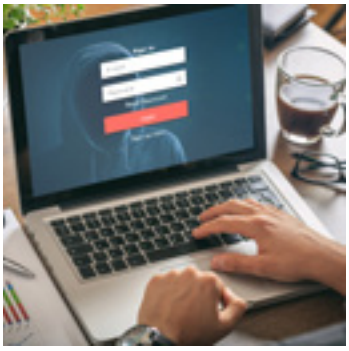
Did you know?

According to a survey commissioned by the Privacy Commissioner of Canada, only 4 in 10 businesses have policies or procedures in place in the event of a breach involving customer personal information.

The Federal Government's Perspective and Actions on Cybersecurity

On March 9, 2017, the Statistics Canada server was attacked, forcing the website to go offline for hours. Although no personal data was reportedly exposed, it served as a stark reminder that even the best protected and most secured systems and organizations can be breached. With 32 of Canada's 38 million population on the internet, and the most common password being "password," the potential harm done is astronomical.

Recently, the Government of Canada announced a $500 million investment over 5 years in cybersecurity, including the establishment of the Canadian Centre for Cyber Security. Serving as a resource centre for individuals and businesses, it will also operate a voluntary certification program for small and mid-sized businesses, covering best practices to help businesses understand and respond to cyber attacks.



Risk Analysis

- What are your organization's "crown jewels" (the information assets of most value that would hurt the business most if compromised)?
- Where are they kept?
- What losses could occur?
    - Financial (phishing, ransomware)
    - Reputational (i.e. Equifax, University of Calgary)
    - Operational (stress of interruption with financial ramifications)
- What is the current plan? Has it been tested?
- Are the C-Suite and Board engaged?

Best Practices

- Require dual authentication for fund transfers to counter phishing attacks.
- Segregate critical data and assets. This is a basic risk management technique traditionally applied to physical assets key to a business.
- Regularly test business continuity and disaster recovery plans.
- Conduct regular "red team" exercises (realistic simulations of cyber attacks to test your team's ability to respond and minimize the impact)
- Ensure proper, ongoing "cyber hygiene" – up to date patches, anti-virus, anti-malware, etc.
- Consider the motives of those that may attack your organization (financial, operational disruption, etc.). Who would attack? Why would they attack?

Develop an Action Plan

Establish a clear and well-defined communication strategy along with a thorough, written incident response plan. Your response plan should outline all the steps to be taken by teams following the discovery of a breach, including a designated response team and their individual responsibilities, as well as the procedure to be followed by different departments (management, legal, IT, HR, PR). Like a fire drill, it is important to frequently test your plan and ensure every member of your team is familiar.

For further information and resources on protecting your business and developing an action plan, please contact a CapriCMW Risk Advisor.