Mandatory Data Breach Notification Laws

Westland Insurance Group Ltd.

On November 1, 2018 changes to the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) will take effect. These changes will establish mandatory data breach reporting requirements on organizations to notify affected individuals and the Privacy Commissioner of privacy breaches; and record keeping requirements following the discovery of a breach.

In the event of a *breach of security safeguards*, a written report must be filed with the Privacy Commissioner which must include a description of the circumstances and cause (if known) of the breach; a description of the personal information that was breached; the number of individuals affected by the breach; and details of actions taken or planned to reduce harm and notify affected individuals.

Organizations will also be required to provide Notification to affected individuals describing the circumstances of the breach and the personal information that was breached. Additionally, such organizations will be required to confirm to individuals details of actions taken or planned to reduce harm, as well as steps that affected individuals can take to reduce or mitigate the risk of harm that could result from the breach.

> ***A breach of security safeguards means the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards. (PIPEDA Act)***

Organizations should understand the potential threats and liabilities they face, and adopt policies and procedures to strengthen their data security infrastructure and respond to potential privacy breaches.

10 Tips for Reducing the Likelihood of Privacy Breach:

From the Office of the Privacy Commissioner (OPC)

1. ***Know what personal information you have, where it is, and what you are doing with it.*** Data inventories and process maps will help ensure you know exactly what personal information you need to protect, as well as when and where you need to protect it. When and where do you collect personal information? Where does that information go? Who can access it, and what do they do with it? You must understand your data before you can protect it!
2. ***Know your vulnerabilities.*** Conduct risk and vulnerability assessments and/or penetration tests within your organization to ensure that threats to privacy are identified. Don't just focus on technical vulnerabilities, though. Are third parties collecting personal information on your behalf without appropriate safeguards? Do you use paper-based application forms, which are transferred to a central location (the loss of which means you'll have no way of knowing who the affected individuals are, let alone how to notify them)? When you upgrade your systems, do the old systems and databases remain active, unwatched and unpatched? The OPC has seen each of these scenarios lead to a breach. Identify your organizations' weak points before a breach identifies them for you!
3. ***Know your industry.*** Be aware of breaches in your industry. Attackers will often re-use the same attacks against multiple organizations. Pay attention to alerts and other information from your industry association, or whatever your source of industry news – don't be the next vulnerable target!
4. ***Encrypt laptops, USB keys and other portable media.*** Organizations often focus on privacy breaches caused by hackers, but this ignores some key threats. Perhaps the most common type of preventable breach seen by the OPC occurs due to loss or theft of unencrypted laptops, USB keys, and other portable media. In many of these incidents, the use of sufficiently strong encryption could have turned a headline-grabbing privacy breach into a minor issue!
5. ***Limit the personal information you collect, as well as what you retain.*** You should know not only why you are collecting each piece of personal information, but why you are keeping it. Where possible, don't collect personal information – for example, in most identity authentication cases it is enough to view, but not record, an individual's identification. Also, if personal information is only collected for limited purposes, securely dispose of it after they have been fulfilled. Always keep in mind: you can't lose what you don't have!
6. ***Don't neglect personal information's end-of-life.*** It is important that you protect personal information throughout its lifecycle – including the often overlooked end-of-life. Clearly define your policies and procedures about the secure destruction of personal information, and make sure they are followed. The OPC has seen breaches caused by documents left behind in a move or thrown in the garbage, as well as by information not being properly erased from discarded or recycled electronics. Like an action movie hero, personal information tends to survive and reappear when its destruction isn't seen through to the end!

7. ***Train your employees.*** Policies can only be effective when those responsible for implementing and abiding by them are aware of what they contain, why they exist, and the consequences of neglecting their responsibilities. You should have in place ongoing privacy and security training and awareness programs that go far beyond 'box-ticking' exercises. Employees who fully understand their roles and responsibilities in protecting personal information can be one of an organization's best lines of defense against privacy breaches!
8. ***Limit, and monitor, access to personal information.*** Employees' access to personal information should be limited to what they need to know, particularly when this information is sensitive. This can help ensure they don't become the cause of a breach, either accidentally or intentionally. Similarly, monitored access logs can help you identify unusual behaviours, and potentially prevent an incident either before it occurs or in the early stage. Don't burden your employees with more information than they need to do their jobs!
9. ***Maintain up-to-date software and safeguards.*** This is Security 101 – if you don't protect yourself against known vulnerabilities, you greatly increase the likelihood of a breach. Establish systematic, documented processes to ensure security-related patches are applied in a timely manner, and that software that is no longer in use is removed from your system. As well, ensure that the virus and malware definitions associated with your anti-virus and anti-malware software are current by allowing them to perform regular updates. Operate at the speed of your attackers!
10. ***Implement, and monitor, intrusion prevention and detection systems.*** An organization's first goal is to prevent intrusions, and you should have systems in place to do so. However, the reality is that even with the best protections in place, your system may get breached. Measures such as intrusion detection systems, firewalls and audit logs can help you to identify and respond to privacy breaches before they escalate – assuming you're paying attention to them. Ensure that safeguards used to monitor network or system activities and mitigate threats have been properly implemented and are proactively monitored. Don't rely only on the guards you've posted at your gate; know what's happening inside your walls!

Source: https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/02_05_d_60_tips/

What types of threats are out there?

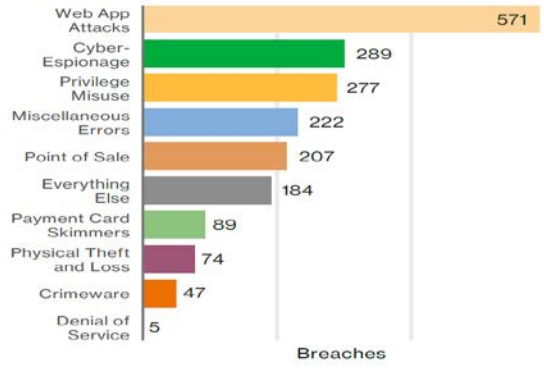

Figure 33: Percentage and count of breaches per pattern (n=1,935)

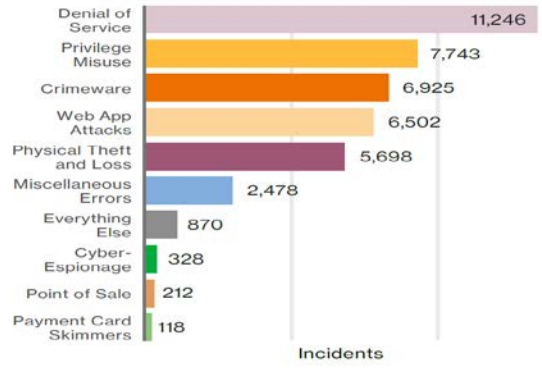

Figure 34: Percentage and count of incidents per pattern (n=42,068)

Is there any such thing as being 100% secure?

Source: Verizon's 2017 Data

Are you Protected?

It is said that there is no such thing as 100% secure. Therefore, changes to PIPEDA increase the need for cyber risks insurance, which can provide insurance protection to cover costs of investigations, notification, liability, legal defense and other expenses associated with responding to data breaches.

An important feature of a Cyber Risks Insurance Policy is the Incident Response coverage included, which serves as the first port of call to third party "Response Partners" who can provide incident investigation and breach response support.

The benefits of Incident Response coverage is that independent legal, forensic and restoration specialists can be deployed to provide crisis support management.

In addition to this, Cyber Risks insurance can provide legal defense cost coverage and pay legal liability and regulatory costs associated with data breaches as well as first party damage costs resulting from Malware, Ransomware, Denial of Service (DOS) or other malicious attacks.

Traditional Property and Casualty Insurance typically exclude Cyber and Data Risks, and this type of coverage can only be provided under a specialized Cyber Risks Insurance Policy.