BEARDWINTER LLP
The Defender
Vol.12 | Issue 2
April, 2018

Mandatory breach reporting in Canada: What it means for cyber insurers

Cary Schneider is a partner at Beard Winter LLP specializing in insurance and civil litigation matters including the growing area of cyber and privacy law. He is a member of the International Association of Privacy Professionals (IAPP), is in the process of being certified as a Certified Information Privacy Professional/Canada (CIPP/C), and studies cyber security at Harvard University. Cary advises insurers on breach and coverage situations, as well as assists businesses in preparing pre-breach data plans and post breach responses.

Your comments are appreciated and if there are any commercial or insurance related topics that you would be interested in reading about, please feel free to email us and we will certainly explore the possibility of writing an article. Contact: defender@beardwinter.com

There is nothing like a deadline that motivates people to take action. In Canada, the due date for organizations to have their privacy compliance protocols in place, or risk severe consequences, has just been announced to be November 1, 2018. As of that date, it will be mandatory for organizations to disclose to both their customers and the privacy commissioner when they have suffered a data breach that results in the possibility of a "real risk of significant harm". It has now become much more perilous to practice the "sweep under the rug" approach to addressing data breaches. As business technology systems have continued to grow at an exponential pace, breaches of privacy, ransomware, and cyber-attacks have now entered our day-to-day lexicon. Companies are on high alert that they need to protect their consumers' privacy. Having a data breach plan that includes a consideration of cyber insurance is one of the pivotal means of addressing this risk. Now is the time for cyber insurers to explain how their product assists companies in advance of this pending deadline.

Mandatory Breach Notification To Consumers

Determining the types of data breaches that must be disclosed to consumers, the means of notification, and when to do it are far from clear. Under the data breach notification regulations, a company must evaluate whether a breach poses a "real risk of significant harm". The guidelines to determine a risk of significant

harm includes: "risk of bodily harm, humiliation, damage to reputation or relationships, loss of employment or professional opportunities, financial loss, identity theft, negative effects on credit record or damage to or loss of property". Examples include credit card numbers, compromising photographs, and health information.

The question of when a company is to notify its consumers of the breach is another tricky proposition. The law provides that organizations must notify consumers "as soon as feasible after an organization determines that a breach has occurred". What

"feasible" means will certainly be subject to interpretation and undoubtedly litigation. The longer the delay in notifying about the breach, the more chance a person's private data is subject to compromise without recourse to mitigation. Similarly, the greater the likelihood of possible harm to the individual the more likely the possibility of a claim/class action lawsuit. On the other hand, a rush to notification for a minor breach that does not meet the "real risk of significant harm" threshold can have an unnecessary detrimental impact on one's business reputation.

Specific provisions (which have not been formalized yet) set out what must be included in the notice. The affected individuals are to be notified by email, mail, telephone, or in person, except if the cost of doing so would be prohibitive and then other provisions would apply. Companies and insurers should take special care concerning the content of the notice as this often forms the foundation for a lawsuit against the company. The specific provisions include:

- a description of the circumstances of the breach;
- the day on which, or period during which, the breach occurred;
- a description of the personal information that is subject of the breach;
- a description of the steps that the organization has taken to reduce the risk of harm to the affected individual resulting from the breach or to mitigate that harm;
- a description of the steps that the affected individual could take to reduce the risk of harm resulting from the breach or to mitigate that harm;
- a toll-free number or email address that the affected individual can use to obtain further information about the breach; and
- information about the organization's internal complaint process and about the affected individual's right, under the Act, to file a complaint with the Commissioner.

Cyber insurers can educate potential insureds on how various coverages for notification expenses, data recovery, breach coaches, ransomware, third party liability, and business interruption helps address their concerns.

Mandatory breach notification to the Office of the Privacy Commissioner of Canada (OPC)

In addition to the regulations regarding notifying consumers of the breach, organizations must also notify the privacy commissioner as of November 1, 2018. Many cyber policies provide coverage for legal expenses during an investigation by the OPC and some even for certain regulatory fines. This is important for potential insureds to appreciate, as such investigations could become costly, are imposing, and may result in significant adverse consequences.

The provisions provide that an organization must give notification of the breach to the OPC in writing, a description of the breach, cause of the breach (if known), an estimate of the number of people at risk of significant harm by the breach, what personal information was compromised, a description of what the company is doing to resolve the breach and reduce the risk of harm, plans for how it plans to reach each of the affected individuals, and a contact person who can answer further questions from the privacy commissioner about the breach.

Depending on the circumstances of the breach and the action/inaction taken by the organization to address the problem, the OPC may conduct an investigation. While the OPC does not currently have the power to order an organization to take any specific action, it can make recommendations for a company to follow. The OPC may even go one step further and begin a legal action in the Federal Court of Canada to compel an organization to follow its recommendations. The OPC does have the power to level fines of up to $100,000 for a privacy violation and an organization may suffer significant reputational harm as a result.

As of November 1, 2018, organizations are also mandated by law to maintain a record of every privacy breach for a period of two years. Organizations that fail to do so may fall afoul of the OPC.

Conclusion

Canada has been a laggard in terms of strong mandatory breach requirements, when compared to other western democracies. The recent introduction of the General Data Protection Regulation (GDPR) privacy legislation in the European Union is probably the most comprehensive in the world. Forty-eight states in the US have laws requiring companies to notify regulators and individuals of a data breach. Make no mistake about it, the new provisions coming into effect November 1, 2018 are long overdue and here to stay.

The mandatory breach notification start date of November 1, 2018 provides both a great opportunity and increased risk to cyber insurers. The opportunity arises as more organizations

are coming to realize that their traditional CGL policies are no longer sufficient. Privacy breaches involving Equifax, Bell, Target, Under Armour, and Uber are front page news items. No matter how formidable the company, hackers are finding a way to burrow through their defences. The disclosure of the data scandal involving Facebook and Cambridge Analytics is reminding us of the importance of our privacy. Companies are realizing that significant exposure from a data breach can include business reputation, business interruption, first party expenses, and third party claims. Mandatory breach notification requires a company to publicly address a privacy problem and cyber insurance is a tool to help soften the blow.

At the same time, there is an increased risk to cyber insurers. The fact that companies are now required to take action to disclose these breaches has the resulting impact of more claims being made. Significant coverage questions will need to be investigated including whether the breach occurred within the policy period, compliance with terms of the contract, existence of a data breach plan, and careful review of the exclusions. Educating the insured on their obligations to comply with the regulations and providing guidance could reduce or eliminate third party claims. Assisting the insured at the outset of choosing a knowledgeable breach coach, and explaining the importance of solicitor-client privilege, will help facilitate a more effective response and likely a less expensive claim.

The November 1, 2018 mandatory breach notification start date should serve as a wake-up call about the consequences of not protecting an individual's privacy. In this day and age, where criminal hackers seem to be one step ahead of cyber defences, it is negligent for a company not to foresee the risk of harm and have a breach response plan in place. Cyber insurance often serves as a vital component of such a plan. The famous idiom of the 19th century UK Prime Minister Benjamin Disraeli still rings true today: "I am prepared for the worst, but hope for the best".

Contact us at: defender@beardwinter.com

The Beard Winter Defender Past Issues

Cyber Hacking and Security: Consequences For Canadian Companies And Insurers

The prevalence of cyber-predators unleashing new and comprehensive hacks that infiltrate a company's network grows seemingly unabated. The question is not "if" a company will be subject to a cyber-attack but rather "when".

Liability In Motor Vehicle Accident Cases: Left-Hand Turns, Pedestrian Knock-Downs, and Rear-End Collisions.

The analysis and investigation of liability in a motor vehicle accident case are crucial to the evaluation of every claim. Any percentage of liability that can be attributed to the plaintiff or co-defendant results in a direct financial saving to your particular claim.

The Examination Under Oath: Underutilized and Under-Appreciated (Updated and Revised)

The evaluation of any personal injury claim primarily revolves around a question of credibility. The impact of the injuries suffered by one claimant is often significantly different compared to the same injuries suffered by another claimant. There is no scientific-medical diagnostic tool that can predict to what extent one person's injuries will result in a long term disability while as someone else will suffer a temporary health setback.

A Year In Review: How The LAT Has Interpreted The MIG

The Licensing Appeal Tribunal ("LAT") has been in existence for one year and decisions are being rendered at a fast and furious pace over the past few months. As we know, this is a new system and very much different from what we are accustomed too in many key respects. It is difficult to predict what an Adjudicator will consider important to their decision making in terms of the influence of past law and evidence. For these reasons, it is important to closely review the decisions of the Adjudicators to analyze any trends and thought processes.