CYBERSECURITY IN CANADA: WHAT TO EXPECT IN 2017

By: Imran Ahmad, Partner, Miller Thomson LLP

Summary

1. **Mandatory Data Breach Notification Is Coming.**
   It is anticipated that regulations related to mandatory data breach notification, record keeping of breaches and fines of up to $100,000 for non-compliance will come into force later in 2017. This will require organizations to review existing policies or implement new internal processes for identifying and responding to data breaches.
2. **Continued Growth in Cybersecurity and Privacy Litigation.**
   2017 will see continued growth of class action certification of cybersecurity and privacy actions and further reliance on torts such as "inclusion upon seclusion" and "disclosure of private facts". Further, once the mandatory data breach notification requirement comes into force, it is anticipated that litigation in this area will increase.
3. **Boards' Oversight – "Business Judgment Rule" Should Prevail.**
   Boards will increasingly be engaged in cybersecurity oversight by scrutinizing managements' strategy and plans to effectively identify, mitigate and respond to cyber threats. Boards will move from a passive oversight model (i.e., simply being informed about cyber risks) to an active oversight model (i.e., being engaged in an ongoing dialogue with management about cyber risks).
4. **Vendor Management – Beware of the Weakest Link.**
   Recognizing that hackers may use vendors to access and compromise the purchasers' network, organizations will increasingly scrutinize vendors' cybersecurity measures. Formal vendor management programs and robust contractual language related to cybersecurity will continue to be adopted by public and private sector organizations.
5. **Accelerated Adoption of Cyber Insurance.**
   Canadian organizations will increasingly turn to cyber insurance as part of their cyber risk mitigation strategy. However, care will need to be taken that they obtain the appropriate type of coverage based on their particular cyber risk profile.

What to Expect in 2017

2016 saw an alarming number of Canadian organizations (public and private) become victims of malicious cyberattacks and data breaches. Hackers did not discriminate who they targeted – victims included financial institutions, universities, hospitals, government agencies, retailers and manufacturers. The techniques they used were both sophisticated and varied, ranging from ransomware (malware that encrypts data until the victim pays a ransom) to advanced persistent threats (deliberate attempts to break into a particular organization's network). Unfortunately, 2017 is shaping up to be another busy year for hackers who show no signs of slowing down.

The following five key cybersecurity trends in 2017 should be on every general counsel's and risk manager's radar.

1. Mandatory Data Breach Notification is Coming

In June 2015, the Digital Privacy Act was adopted. It introduced several key changes to Canada's federal privacy law, the Personal Information Protection and Electronic Documents Act ("PIPEDA"). Some of the changes that are anticipated to come into force this year include mandatory record keeping for all breaches, mandatory data breach notification, and significant penalties for non-compliance.

The mandatory data breach notification requirement, while not currently in force, will require organizations to give notice to affected individuals and to the Office of the Privacy Commissioner of Canada (the "Commissioner") about data breaches in certain circumstances. Specifically, PIPEDA will require organizations to notify individuals and report to the Commissioner all breaches where it is reasonable to believe that the breach creates a "real risk of significant harm to the individual". These provisions will be brought into force

once the regulations are finalized, which is anticipated to be in the second half of 2017. They are likely to increase an organization's litigation exposure as result of a breach.

The mandatory record keeping of all breaches of safeguards involving personal information under an organization's control will require that organizations review existing processes or implement effective detection, reporting and tracking mechanisms, to ensure compliance.

From an enforcement standpoint, violations of the breach notification or the record keeping requirements (e.g. covering up a breach, failing to notify or failing to keep records) can result in a fine of up to $100,000.

2. Continued Growth in Cybersecurity and Privacy Litigation

Over the past five years Canada has seen an upward trend when it comes to litigation involving data breaches. Confidential personal and corporate information is at risk from a variety of threats, ranging from the exploitation of big data to clerical error, workers' misconduct and criminal hackers. There are a number of common law and statutory tools available for victims to seek compensation in court following a breach.

At common law, Canadian courts, recognizing the rapid pace at which technology is evolving, have been receptive to recognizing new torts advanced resulting in cybersecurity and privacy breaches (e.g., intrusion upon seclusion, disclosure of private facts, etc.) that are being advanced by plaintiffs' counsel. We anticipate this trend to continue and to see the existing torts being further tested by the courts.

In parallel, 2016 saw courts certify and approve settlements for a number of cybersecurity class actions (e.g., R. v. John Doe, Drew v. Walmart Canada Inc. and Lazanski v. The Home Depot). We anticipate this trend to increase given the upcoming breach notification requirements.

3. Board's Oversight – "Business Judgment Rule" Should Prevail

In managing and directing corporate affairs, Boards have an obligation to protect corporate assets (e.g., proprietary information, customer data, goodwill and reputation). This includes overseeing the systems that management has implemented to identify, mitigate and respond to risks, including cyber risks.

As a general rule, Boards should focus on the following:

- High-level understanding of the cyber risks facing the organization, which can vary based on the industry and operations of the organization.
- Potential impact on the organization (e.g., litigation, reputational harm, business interruption, etc.) and mandating management to implement measures to mitigate and effectively respond to these threats.
- Understanding and overseeing the systems (i.e., people, policies and controls) that the organization has implemented to identify, mitigate and respond to risks related to cybersecurity, in particular with respect to incident response.

When it comes to cybersecurity, detailed technological understanding is not required by the Board. Directors are entitled to rely on management and external cybersecurity experts. Ultimately, the "business judgment rule" should apply to decisions regarding issues related to cybersecurity oversight, so long as they abide by the core standards of care, loyalty and good faith that apply to Board decisions more generally.

4. Vendor Management – Beware of the Weakest Link

More often than not, hackers will gain access to an organization's network by targeting a network-connected vendor who has weaker cybersecurity measures in place. Some of the largest data breaches were the direct result of hackers targeting vendors.

The most effective way to address this type of risk is by having an effective vendor management program ("VMP") based on the following four key steps: (i) identify key vendors who have access to the organization's network or data; (ii) identify an individual within the organization to liaise and oversee the relationship with the vendor (including compliance with cybersecurity requirements); (iii) establish guidelines and controls for vendor oversight; and (iv) exercise audit rights and/or verify maintenance of cybersecurity compliance certifications.

The most important part of vendor management is to ensure that the contract governing the relationship with the vendor clearly spells out cybersecurity expectations and specific obligations in this regard by the vendor (including the vendor's obligations in the case of a breach). Moreover, organizations should not hesitate to regularly exercise audit rights or to verify the vendor's compliance with any applicable cybersecurity standards (e.g., ISO 27001 or NIST).

5. Accelerated Adoption of Cyber Insurance

Globally, cyber insurance coverage has seen significant growth. In Canada, while the adoption rate has been slower, we anticipate the cadence to accelerate as organizations turn to insurance as part of their overall cyber risk mitigation strategy.

Broadly speaking, coverage under policies is typically divided into first party (i.e., expenses incurred in the immediate aftermath of a security breach) and third party (i.e., losses or damages caused to customers as a result of the incident).

That said, not all cyber insurance policies are equal and an organization should first assess its cyber risk profile and exposure. A clear understanding of where it stands on the cyber risk spectrum is critical in ensuring that an organization gets the right cyber liability coverage. This exercise will inform organizations when negotiating premiums about the services that should be included in the cyber policy.

While standard commercial general liability ("CGL"), errors and omissions ("E&O"), and directors and officers ("D&O") policies may already provide some of these coverages, if an organization is not careful, there may be cyber-breach exclusions in those policies that may limit the type of assistance required to effectively deal with a cyber incident.

Contact

Imran Ahmad
Partner
416.597.6031
iahmad@millerthomson.com

MILLERTHOMSON.COM

MILLER THOMSON
AVOCATS | LAWYERS