BUSINESSCLASS
KNOWLEDGE ▪ SEMINARS ▪ INSIGHTS

Blakes

Under Cyberattack: How Can Canadian Directors Mitigate Liability?

By Hélène Deschamps Marquis and Joe Abdul-Massih

Several former Yahoo! Inc. executives recently settled a derivative action for US$29-million, following data breaches from 2013 and 2014 that compromised approximately three billion accounts. These data breaches were the biggest known intrusions of a single company's computer network at that time. Given the absence of Canadian case law on director liability in the context of a data breach, prudent directors may gain an advantage by reviewing U.S. case law and adapting their strategy and approach to data privacy and security.

LESSONS LEARNED FROM YAHOO'S DATA BREACH

In February 2017, Yahoo! Inc.'s shareholders filed a shareholder derivative action in the United States District Court for the Northern District of California against Yahoo! Inc.'s board and senior managers for their handling of the 2013 and 2014 data breaches. Allegations consisted of Yahoo! Inc. officials breaching their fiduciary duties by failing to protect Yahoo! Inc.'s data, failing to implement proper safety mechanisms in order to prevent cyberattacks and issuing false statements about Yahoo! Inc.'s knowledge of the data breaches.

After the data breaches were disclosed, Verizon, who had entered into a stock purchase agreement with Yahoo! Inc. for the sale of Yahoo! Inc.'s operating assets (Verizon Transaction) in 2016, quickly amended the purchase price: consideration to be paid by Verizon to Yahoo! Inc. was reduced by US$350-million.

Some say it could be indicative of a new trend where directors and officers of organizations are increasingly held liable for their conduct during a breach. Others attribute the large settlement to Verizon's ability to negotiate a significant reduction of the purchase price. Unlike other derivative lawsuits, damages to the company were easy to quantify.

BOARD RESPONSIBILITIES IN CANADA

The *Canada Business Corporations Act* (CBCA) and comparable corporate law statutes require that every director and officer of a corporation – in exercising their powers and discharging their duties – exercise the care, diligence and skill that a reasonably prudent person would exercise in comparable circumstances. In interpreting compliance with this standard, courts recognize that business decisions will

usually involve some degree of risk and that it would be inappropriate to subsequently apply 20/20 hindsight to past decisions. The CBCA also provides that a director has complied with this duty of care if he or she relied in good faith on a report of a person whose profession lends credibility to a statement made by the professional person.

While preventing all data breaches is a laudable objective, given the complexity of information systems and the ever-evolving ingenuity employed by cybercriminals, such a goal may be impossible or impractical and it is not the standard to which directors of Canadian companies should expect to be held accountable. Consistent with their duty of care, the board should practice prudent cybersecurity risk oversight fundamentals and continuously reassess the changing landscape of standards and risk.

RISK MANAGEMENT: TIPS AND TRICKS

According to a recent study exposing the cost of data breach incidents in 13 regions around the world, the average cost of a data breach in Canada is C$5.78-million, with an average cost of C$255 per lost or stolen record. For more information, please see our July 2017 *Blakes Infographic: Data Breach Disruptions: The Cost of Cybercrime in Canada*.

One factor that reduces the cost of a data breach is board-level involvement in cybersecurity matters. Although there is no need for the board to get into the technical weeds of cybersecurity, such as how to conduct penetration testing or establish effective firewalls, the board does need to understand enterprise-wide cybersecurity risk management and set a tone from the top of commitment to cybersecurity.

Below are a few ways in which the board can leverage its risk analysis and management skills to monitor and advance cybersecurity, reduce liability and ensure compliance with their fiduciary duties:

1. **Establish a privacy management structure** by ensuring that a privacy officer, information security personnel and an incident response team are in place and review existing incident response plans, policies and procedures to identify any cybersecurity and data breach issues.
2. **Conduct data mapping** by reviewing the types of personal information collected by an organization and other data critical to the organization to ensure that data management practices are appropriate.
3. **Assess information systems** by reviewing the security tools in the organization's network and the software applications in place.
4. **Review training practices** to ensure that the organization's key information technology and information security personnel is properly trained on incident response and management.
5. **Conduct regular table top exercises and red team attacks** with the organization's incident response team and other professionals.
6. **Be proactive** by retaining an external legal counsel to serve as breach coach to ensure the organization is prepared.

CONTACT US

Hélène Deschamps Marquis
helene.deschampsmarquis@blakes.com
514-982-4042

Joe Abdul-Massih
joe.abdul-massih@blakes.com
514-982-4297