



Cyber Security and Privacy

Chad Sullivan – *Fredericton, NB*

Koren Thomson – *St. John's, NL*

Sarah Dever Letson – *Saint John, NB*



Causes of Action

Intrusion upon Seclusion

Jones v. Tsige, 2012 ONCA 32

- Requires:
 - (a) intentional conduct (includes reckless conduct);
 - (b) an invasion of a person's private affairs or concerns without lawful justification;
 - (c) that a reasonable person would regard as highly offensive, causing distress, humiliation or anguish.

Class Actions

- Lost or misplaced information
 - *Condon v. Canada*
- Employee snooping
 - *Moore & Shinold v. Capital District Health Authority*
- Employee stealing information for third parties
 - *Evans v. Bank of Nova Scotia*
- Third party hacking
 - *Lozanski v. The Home Depot Inc.*

Vicarious Liability for Cybersecurity Matters

- Vicarious liability is imposed when the act is authorized by the company or the act is so connected with authorized acts that they are regarded as a mode of doing an unauthorized act.

Statutory Invasion of Privacy

- Requires:
 - a) A violation of an individual's privacy;
 - b) That it is done willfully; and
 - c) Without a claim of right.

Other Sources of Civil Liability

- Claims by Financial Institutions
- Claims by Shareholders



Mitigate the Risk: Insurance

Potential Applicable Policies

- Commercial general liability
- Errors and omissions
- Director & officer liability

Cyber Security Insurance

- Policies for losses resulting from cyber security incidents.
- Very little standardization.
- What may not be covered:
 - Social engineering losses
 - New hardware

- Software upgrades
- Third-party errors
- Third-party contract claims
 - *P.F. Chang's China Bistro Inc v. Federal Insurance Company*, 2016 WL 3055111
- Intellectual property theft and reputation damage

So What is Covered?

- First party coverage
 - Notification costs
 - Forensic investigation costs
 - Crisis management costs
 - Cyber Extortion costs
- Third party coverage
 - Network security costs
 - Privacy liability



What is Effective Cybersecurity Governance?

- Increased cost of Cybersecurity attacks is resulting from detection and response times being too slow.
- Deficiencies in planning for incident response leaves organizations vulnerable if there is a breach.
- Directors of Canadian companies, consistent with their fiduciary duty and duty of care, need to exercise oversight over Cybersecurity risk.

- Liability can arise not from a cybersecurity breach itself, but from a failure to demonstrate that the board properly assessed and considered the risk.
- The bottom line is – the development of appropriate policies and procedures to manage and address Cybersecurity risk can demonstrate board care and diligence.

Components of a Cybersecurity plan:



Source: IIROC
Cybersecurity Best
Practices Guide

Components of a Cybersecurity plan:

- Security safeguards/defensive plan
- Breach detection/monitoring
- Breach response
- Breach recovery
- Regular review

Organization and Board Buy-in:

- Responsibility
- Budget
- Education
- Training
- Regular reporting to the Board



These materials are intended to provide brief informational summaries only of legal developments and topics of general interest.

These materials should not be relied upon as a substitute for consultation with a lawyer with respect to the reader's specific circumstances. Each legal or regulatory situation is different and requires review of the relevant facts and applicable law.

If you have specific questions related to these materials or their application to you, you are encouraged to consult a member of our Firm to discuss your needs for specific legal advice relating to the particular circumstances of your situation.

Due to the rapidly changing nature of the law, Stewart McKelvey is not responsible for informing you of future legal developments.