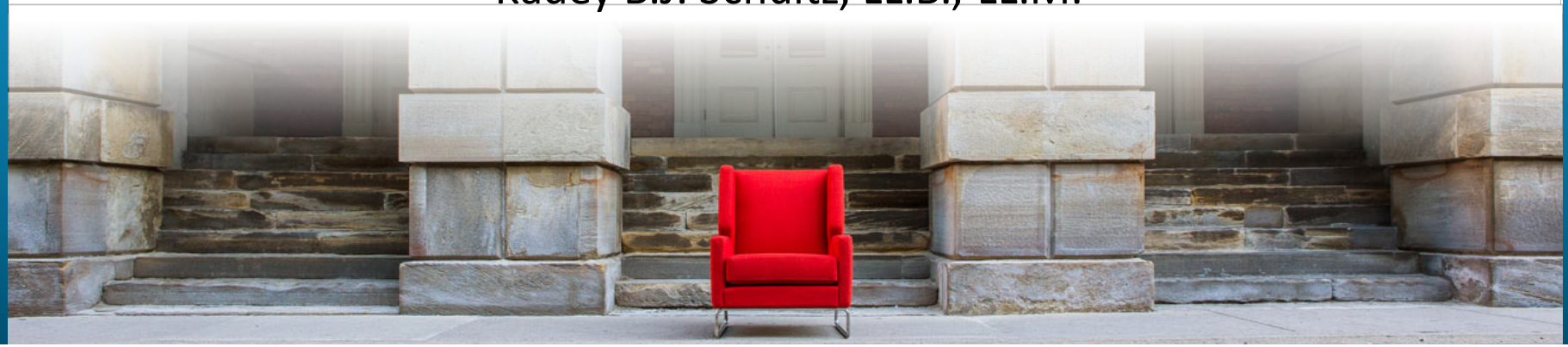
Cyber Risk in Canada: What to Watch Out for and How to Be Prepared

Twenty Toronto Street Conferences and Events, OBA Institute

February 2, 2016

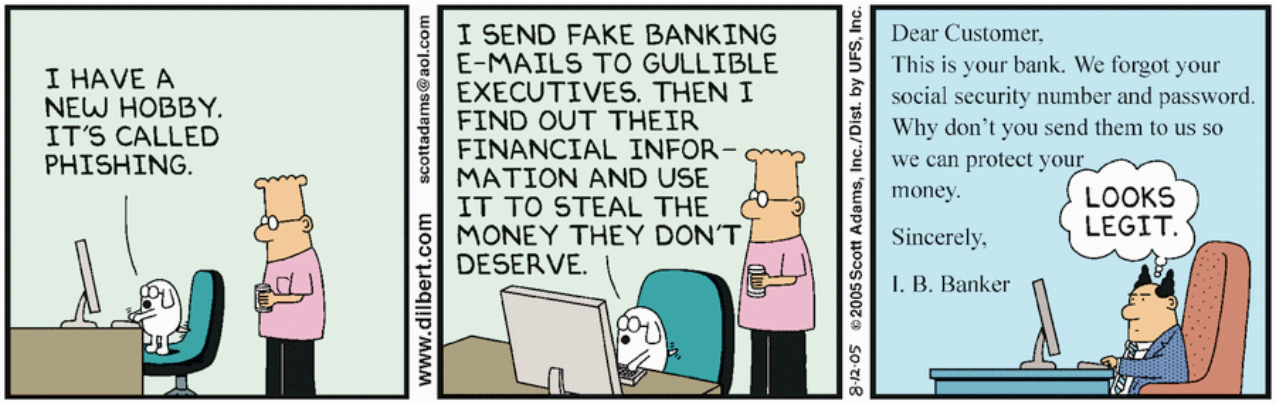
Kadey B.J. Schultz, LL.B., LL.M.



Cyber Risk in Canada: What to Watch Out for and How to Be Prepared

1. What is Cyber Risk?
2. What's all the Buzz about Cyber Risk?
3. Privacy Law – The Current State of Affairs
4. The New IIROC Best Practices Guide: Takeaways
5. Five Must-Dos for Law Firm Security in 2016
6. Up Next: Cyber Risk and the "Internet of Things"

What is Cyber Risk?



What is Cyber Risk?

- Risk that affects organizations that...
  - Host, store, share or transmit proprietary and confidential data
  - Produce or disseminate electronic content
  - Transact business and generate revenue through online services

What is Cyber Risk?

- Risk that affects organizations that...
  - Have exposures to handling personal identifiable information
  - Have business operations that would be impacted by disruptions in service
  - Outsource storage, processing or sharing of confidential information with third party service providers

THAT’S ME!!!

What is Cyber Risk?

- The advent of an increasingly connected world means businesses need to adapt to survive
- Businesses need to consider recovery plans, new corporate governance issues related to technology and privacy and how they deal with private information and data breaches
- Must now consider adding cyber coverage to traditional insurance policies

An Insurer's Perspective

- Underwriters for insurance companies will consider a variety of factors in assessing your business
- Does your business have a cyber attack response and recovery plan?
- Do your employees have adequate training to deal with sensitive information?

An Insurer's Perspective

- Do you understand the different kinds of data your business deals with and how to properly safe guard them?

- Will your business be able to afford the various costs associated with handling a breach?

An Insurer's Perspective

- Traditional insurance policies may or may not respond to data breach situations
  - General liability
  - Business interruption
  - Fidelity (Crime)
  - Directors' and officers' liability
  - Professional liability

An Insurer's Perspective: Forms of Cyber Liability

- Third Party Liability: Insurance policies used to pay damages caused to third parties by the insured

- First Party Expenses: claims made by an insured to their own insurance company

An Insurer's Perspective: Third Party Liability

- Privacy Liability: Loss arising out of a failure to protect sensitive personal or corporate information

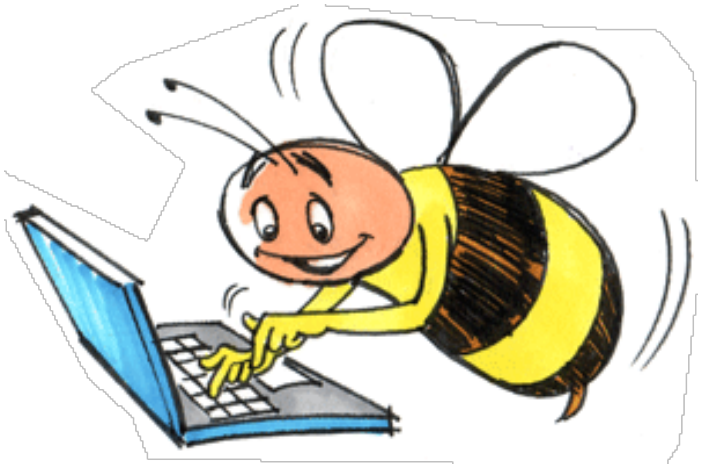
- Network Security Liability: Loss arising out of a failure of network security leading to the disclosure or theft of personal or corporate information

An Insurer's Perspective: First Party Expenses

Cyber Risk insurance covering the costs of…

- Notifying those whose information was exposed
- Managing public relations following a breach
- Providing credit monitoring services to clients
- Conducting forensic studies to determine the scope of a breach
- Paying hackers to relinquish control of a computer system

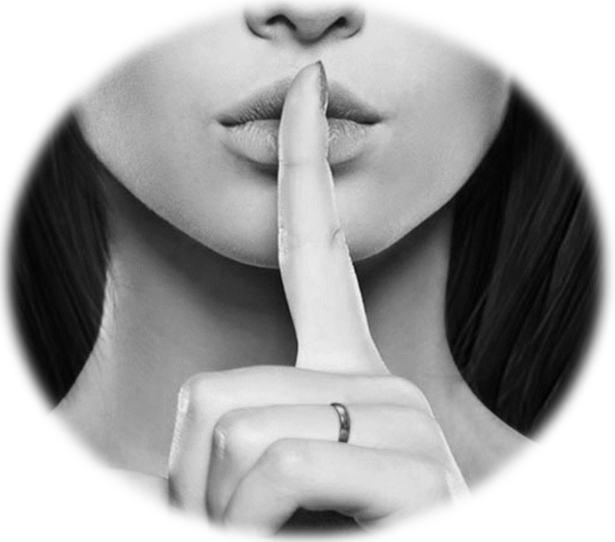
What's all the Buzz about Cyber Risk?



The Ashley Madison Hack

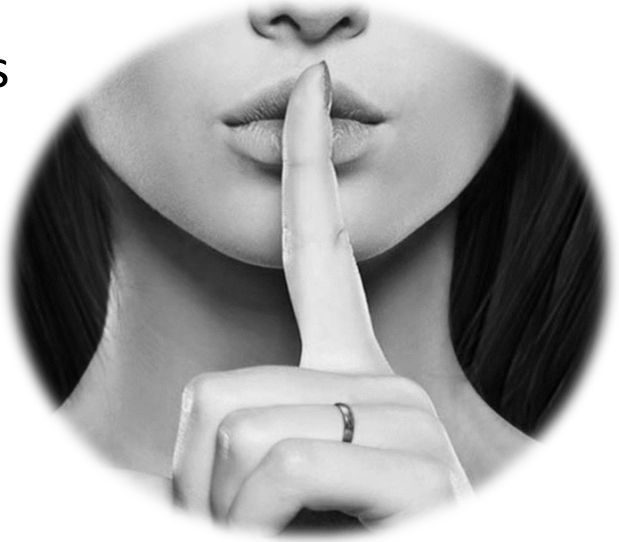
- Ashley Madison is a dating site owned by Avid Life Media, which encouraged its users to engage in extramarital affairs

- They claimed to have a highly secure system and offered a $20 Paid Delete option which allowed users to fully remove their private data



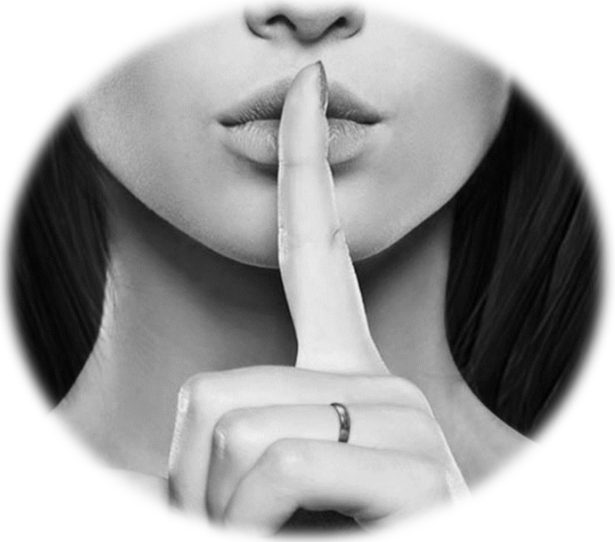
The Ashley Madison Hack

- On July 15, 2015, the website's data base was infiltrated by a group called the Impact Team
- They claimed to have accessed user accounts containing credit card numbers and financial records, sexual preferences, names, addresses and emails
- They revealed that the Paid Delete option was not always honoured



The Ashley Madison Hack

- Bad news followed for Avid Life Media including reports of extortion attempts, three suicides and a disgraced state prosecutor
- Two Class Action lawsuits were initiated in Canada and four federal suits in the United States
- Users of Ashley Madison are still reporting instances of blackmail in 2016



IIROC Case Studies

- On December 21, 2015, the Investment Industry Regulatory Organization of Canada (IIROC) released a Cybersecurity Best Practices Guide

- The Guide was released in recognition of the importance of proactive management of cyber risk to ensuring the stability of their member firms and the Canadian capital markets

- Features case studies exhibiting how simple or complex a data breach can be

IIROC Case Studies

Business Email Compromise – February 2015

- The CFO of Infront Consulting Group Inc. received an email that appeared to come from the company's CEO to process a payment of $169,705.00 USD to an investment brokerage in Naples, Florida
- The scheme failed only because the CFO called the CEO while reviewing the request
- The CEO said he knew nothing about the request

IIROC Case Studies

Ransomware – June 2015

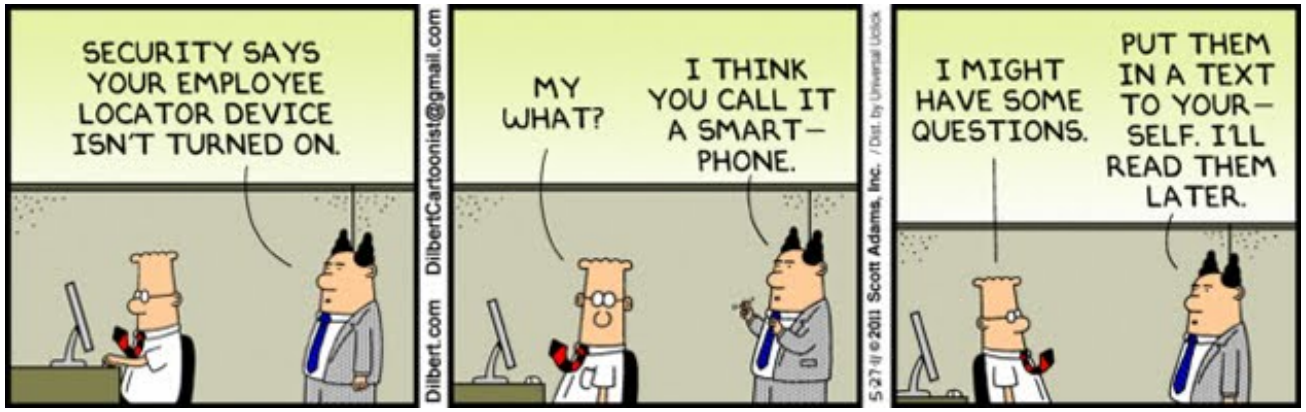
- Municipal computers in Mahone Bay and Bridgewater were infected by the CryptoLocker virus which encrypted and locked off access to files
- The infection came with a ransom letter asking each user for $900 in return for unlocking the files
- The US Justice Department estimated that CryptoLocker caused a total of $27 million in damages in its first two months of operation

IIROC Case Studies

Social Engineering Fraud – April 2015

- Mega Metals Inc. was defrauded when the email account of an Italian third party broker was compromised
- Mega Metals wired $100,000 to a German vendor, who then complained that no payment was received
- An investigation revealed that the third party broker's computer systems were infected with password collecting software allowing criminals to falsify wire-transfer instructions on purchases

Privacy Law – The Current State of Affairs



Privacy Law – The Current State of Affairs

- Canada has been slow to innovate legislatively on the issue of cybersecurity
- Until recently, the only legislation related to this problem was *The Personal Information Protection and Electronic Documents Act* (PIPEDA)
- On June 18, 2015, *The Digital Privacy Act* (DPA), designed to expand the obligations of corporations under PIPEDA, was given royal assent

Privacy Law – The Current State of Affairs

The Personal Information Protection and Electronic Documents Act

- Purpose is to "establish rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information"

- Simultaneously, it aims to help facilitate the collection, use and disclosure of such information for reasonable purposes

Privacy Law – The Current State of Affairs

The Personal Information Protection and Electronic Documents Act

- PIPEDA applies to all organizations in Canada engaged in business practices

- It also sets out principles of fair information practices, which aim to promote accountability, transparency and accuracy while limiting the indiscriminate collection of data

Privacy Law – The Current State of Affairs

The Personal Information Protection and Electronic Documents Act

- PIPEDA allows individuals to file written complaints with the Privacy Commissioner against an organization for contravening any part of Division 1 of the statute

- If the Commissioner finds it appropriate, an investigation is conducted, following which the complainant may seek a Court hearing

Privacy Law – The Current State of Affairs

The Digital Privacy Act

- The DPA introduced a mandatory data breach notification requirement under PIPEDA
- An organization that experiences a data breach involving personal information under its control must report to the Commissioner and the individual affected if it is believed that the breach creates a real risk of significant harm
- Significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on a credit record and damage to or loss of property

Privacy Law – The Current State of Affairs

The Digital Privacy Act

- The DPA also created an enforcement provision (less aggressive than the European Union's) which deems anyone in contravention of the rules to be guilty of an offence punishable on summary conviction and liable to a fine not exceeding $10,000 or an indictable offence with a fine of $100,000

NOT SO FAST!

Privacy Law – The Current State of Affairs

The Digital Privacy Act

- The Act will not be in effect until the government issues further regulations

- At this point there is no timeline for that change

Privacy Law – The Current State of Affairs

Case Law:

1. *Jones v. Tsige, 2012 ONCA 32*
2. *Chitrakar v. Bell, 2013 FC 1103*
3. *Evans v. The Bank of Nova Scotia, 2014 ONSC 2135*
4. *Condon v. Canada, 2014 FC 250*
5. *Albayate v. Bank of Montreal, 2015 BCSC 695*

Privacy Law – The Current State of Affairs

Jones v. Tsige, 2012 ONCA 32

- Confirmed the existence of the tort of **intrusion upon seclusion** (breach of privacy) as an independent cause of action in Ontario

- Case involved two employees of the Bank of Montreal, one of whom used her work computer to surreptitiously access the other's personal bank accounts at least 174 times over the course of a year

Privacy Law – The Current State of Affairs

Jones v. Tsige, 2012 ONCA 32

- Set out a number of factors:
  - A defendant's conduct must be intentional or reckless
  - A defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns
  - A reasonable person would regard the invasion as highly offensive and causing distress, humiliation or anguish

Privacy Law – The Current State of Affairs

Chitrakar v. Bell, 2013 FC 1103

- Bell Canada conducted credit checks without Chitrakar's consent
- This was found to be contrary to section 3.1 of PIPEDA
- The Court noted that while assessing damages was difficult absent a "direct loss", PIPEDA permits a court to award damages for "humiliation" pursuant to subsection 169(c)

Privacy Law – The Current State of Affairs

Evans v. The Bank of Nova Scotia, 2014 ONSC 2135

- The first class action suit arising out of a privacy breach to certified in Ontario

- A bank employee improperly transferred confidential client information to his girlfriend who then released the information to third parties, resulting in identity theft

Privacy Law – The Current State of Affairs

Evans v. The Bank of Nova Scotia, 2014 ONSC 2135

- The cause of action against the bank asserts negligence as well as intrusion upon seclusion

- The certification of this case demonstrates that organizations that fail to properly monitor employees who have access to highly confidential information may be in danger of vicarious liability for both compensatory and nominal damages

Privacy Law – The Current State of Affairs

Condon v. Canada, 2014 FC 250

- Involved the loss of a government-owned hard drive containing the personal information of approximately 583,000 individuals who had applied for student loans
- The Court noted that the hard drive was not encrypted, nor stored in a location that was locked all the time
- Further to *Jones*, the Court stated that the breach of privacy need only to carry the potential for distress, humiliation or anguish

Privacy Law – The Current State of Affairs

Albayate v. Bank of Montreal, 2015 BCSC 695

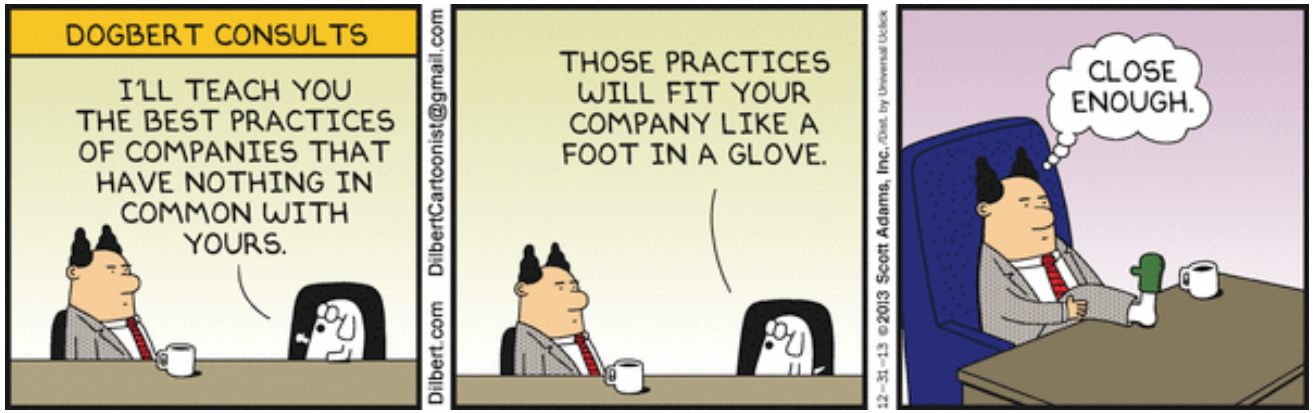
- BMO changed the Plaintiff's address without her consent
- Consequently, her ex-husband received her banking details in the mail (he promised he never looked!)
- Her address was also inaccurately reported to two credit reporting agencies

Privacy Law – The Current State of Affairs

Albayate v. Bank of Montreal, 2015 BCSC 695

- The Court found a breach of her privacy rights under British Columbia's *Privacy Act* and a breach of BMO's contractual obligations to her
- The Plaintiff was unable to prove any actual damages but, in line with the factors set out in *Jones*, she received nominal damages of $2,000
- This was a privacy *leak* rather than a breach – but the rules are the same

The New IIROC Best Practices Guide: Takeaways



The New IIROC Best Practices Guide: Takeaways

- Governance: an organization's leadership is responsible for directing the implementation of a comprehensive cybersecurity program and regularly overseeing its effectiveness

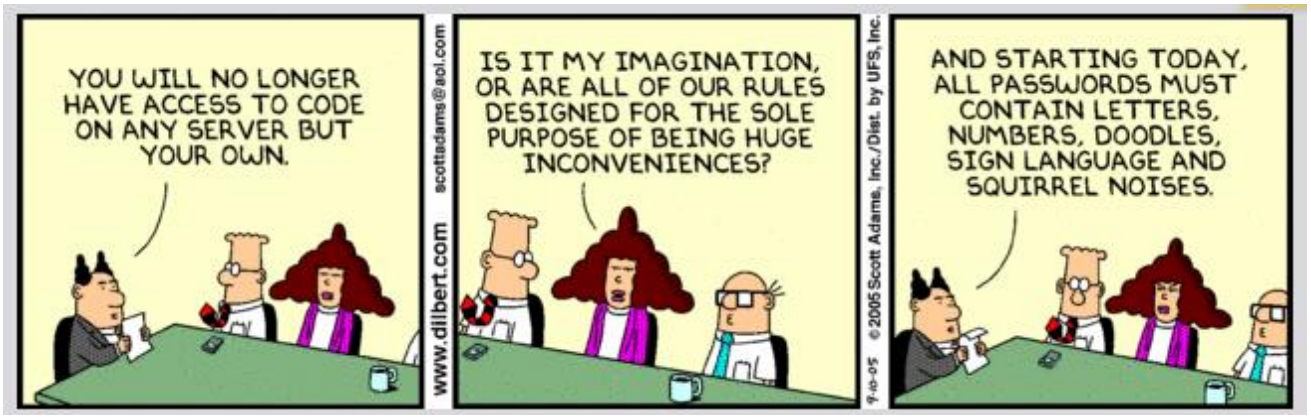
- Training: Training should focus on fostering a culture of procedural compliance, a questioning attitude and having a depth of knowledge to identify potential threats to the organization

The New IIROC Best Practices Guide: Takeaways

- Implementation: The best practices can serve a benchmarking function allowing smaller dealers to situate their efforts relative to industry standards

- Third Party Vendors: Given the rise in the number of security incidents attributed to third party vendors, it is recommended that dealers exercise strong due diligence and develop clear vendor performance policies

Five Must-Do's for Law Firm Security in 2016



Five Must-Dos for Law Firm Security in 2016

1. Get insured!
2. Encrypt your emails and personal data
3. Implement mobile security measures
4. Implement two-step verification measures for employees
5. Be prepared to comply with the increasing frequency of demands under PIPEDA

Up Next: Evolving Issues for Motor Vehicle Litigation

- With the advent of an increasingly connected world there is growing interest in the Internet of Things
- The Internet of Things encompasses all connected devices, from smart phones, to phone applications to self-driving vehicles
- Canada has been slow to deal with this pressing issue, and has yet to have engaged in any substantive discussion of the matter
- Please join Susane Sviergula of Cavanagh LLP for an exciting discussion on this topic and its relation to the changing world of Motor Vehicle Litigation!

Up Next: Evolving Issues for Motor Vehicle Litigation

- Please join Susane Sviergula of Cavanagh LLP for an exciting discussion on this topic and its relation to the changing world of Motor Vehicle Litigation!

schultz frost LLP

KADEY B.J. SCHULTZ, L.L.B., L.L.M.

E. kschultz@schultzfrost.com

T. 416.969.3434

F. 416.969.3435

Over 15 years of insurance defence litigation with significant arbitration, trial and appeal experience at the FSCO, Superior Court, Divisional Court and Court of Appeal.

Specializing in civil litigation, focusing on the defence of Statutory Accident Benefits ("SABS") disputes, including first party claims for benefits, private arbitrations of priority and loss transfer disputes, the interaction between SABS and WSIB, anti-fraud for tort, AB and property, as well as personal injury claims, general negligence and solicitors' negligence.