

DATA BREACHES & CYBERSECURITY INCIDENTS: THE LEGAL GUIDE TO PREPAREDNESS AND RESPONSE

Do you have the tools you need to avoid, prepare for and respond to an organizational data breach or cybersecurity incident?

If you're a legal professional or executive whose work involves the protection of information, this program is essential. Designed to help you better understand and respond to a data breach incident, this program focuses on **practical, real world scenarios with hands-on learning**. Get expert advice on:

- Data loss and breach prevention strategies, tools and tips
- Strategies for cybersecurity preparedness: incident management plans, data breach response strategies and reputation management
- Best practices and tactics for acclimating to the new breach notification requirements
- Overview and insights of current trends in data breach & privacy litigation

PLUS! For those new to the area, or in need of a refresher, registration includes access to the *Online Primer Data Breaches and Cybersecurity Law 101*.

Note: The Optional Online Primer will become available on October 15, 2019.

Register today at:

osgoodepd.ca/databreaches

Program Chair

Timothy Banks
nNovation LLP,
author of the *Guide to Personal Information Protection and Electronic Documents Act*
(Lexis Nexis Canada)

Date and Time

November 1, 2019
8:30 a.m. – 5:00 p.m. EDT
In Person or Webcast

Online Replay:
December 17, 2019

Location

Osgoode Professional Development
1 Dundas St. West, 26th Floor
Toronto, ON

Data Breaches & Cybersecurity Incidents: The Legal Guide to Preparedness and Response

How many organizations had their data breached in the past year? Almost **all of them**, suggests a recent survey. A panoply of companies face very steep fines. Equifax is set to pay up to \$700M USD in the largest data breach settlement in history, British Airways faces a fine of close to \$230M USD and Marriott Hotels faces a fine of \$123M USD for their late-2018 cyber incident.

Cybersecurity lapses and other data breaches have become a top concern for businesses. To avoid costly missteps, you must ensure you have appropriate protocols and procedures in place and the requisite skills and knowledge to respond to a security incident.

This *OsgoodePD* program provides you with an in-depth overview of how to prepare for and respond to a data breach and cyber incident. You will also learn the questions you need to ask to ensure appropriate prevention measures are in place.

The instruction draws from examples of cybersecurity designs, plans, incident responses, insurance policies and procedures. **Using sample case scenarios, you will get hands-on learning to help you ensure a cyber-resilient organization.**

In-person registration is limited to enhance discussion and time for questions. Register now to secure your place: osgoodepd.ca/databreaches

Get important insights, including:

- Current trends in data breach and privacy litigation
- Key components and best practices for an effective data breach incident response plan
- Privacy law accountability obligations and liabilities
- The role and composition of the breach response team
- Legislated breach notification requirements and drafting breach notifications
- Conducting and organizational review to minimize and mitigate data breach risks

This intensive course is essential for:

- Lawyers practicing in corporate law, privacy law and information technology law
- Business leaders (executive officers, information/privacy officers, technology officers)
- Professionals working in cybersecurity, data breaches, privacy, compliance, risk management and anti-money laundering
- Government and regulatory representatives
- Banking and Financial Services Professionals/Executives

Agenda

8:30 a.m.

Registration opens

9:00 a.m.

Welcome & Overview from Program Chair – Timothy Banks, nNovation LLP

9:10 a.m.

The Regulator Speaks! New Reporting Requirements and Their Implications

David Goodis, Assistant Commissioner, The Information and Privacy Commissioner of Ontario

Sue Lajoie, Executive Director, Compliance, Intake and Resolution Directorate, Office of the Privacy Commissioner of Canada

The regulatory framework for reporting of breaches of security safeguards has changed. Hear directly from the regulators on the latest, including clarification on your new obligations and reporting obligations.

- Understanding the new requirements – are organizations over-reporting or underreporting?
- What are the common mistakes organizations make when reporting?
- What happens when the regulator begins an investigation? How should you respond?

10:15 a.m.

Refreshment Break

10:30 a.m.

Data Breaches and Cyber Incidents in Review: Understanding the Legal Risks and Damages

Catherine Beagan Flood, Partner, Blake, Cassels & Graydon LLP

Recent fines, settlements and awards have sent a strong message to companies who **MUST** take appropriate steps to protect information or face costly consequences. This session will provide you with a comprehensive review of incidents that have taken place over the last

18 months, in Canada and abroad. You will get up-to-the minute insights, including the latest on:

- Current trends in data breach and privacy litigation
 - What are plaintiff's class action lawyers looking for?
 - What activities and breaches have given rise to claims?
 - How have claims been framed?
 - How are defendants responding to such claims?
- Damage awards
 - What can be claimed?
 - What has been successful in Canada, the USA and abroad?

11:30 a.m.

Cyber & Data Breach Insurance: Critical Update

Matthew Davies, VP – E&O/Cyber Canada, Chubb Insurance

Patrick Bourk, Principal – National Cyber Practice Leader, Hub International

- The evolving market for data breach insurance in Canada
- To what extent do traditional policies apply to data breaches?
- What amounts are covered under a 'cyber' policy?
- What is required to obtain data breach insurance?
- Insurance issues regarding outsourcing and service providers

12:00 p.m.

Networking Luncheon

1:00 p.m.

SCENARIO #1 Testing an Effective Incident Response Plan

Imran Ahmad, Partner, Blake, Cassels & Graydon LLP

Greg Wolfond, CEO, SecureKey Technologies

Using a mock Incident Response Plan (IRP), you will engage in an interactive role-play that exposes key weaknesses in an

organization's preparedness. You will learn the key components of an IRP and what weak links may hold you back in a crisis, including:

- The roles responsibilities of key stakeholders, including: legal counsel, public relations, forensics and notification providers
- Tactics for clear and coherent communication plans

You will also learn about:

- Due diligence requirements when selecting vendors and sub-contractors
- Contractual terms regarding privacy and security
- Contractual audit rights and conducting audits
- Negotiating obligations and indemnities
- Escalation protocols for breaches
- Testing and monitoring incident response protocols

You will come away with a better understanding of how test and evaluate your organization's own data governance program, including your Incident Response Plan.

2:30 p.m.

Refreshment Break

2:45 p.m.

SCENARIO #2 Breach Notification & Harm Mitigation: Developing an Incident Response Plan & Team – Role Play

Lynn Larson, Senior Counsel, Bell

Timothy Walsh, Senior Director, Breach Services, TransUnion

Engaging in a second role-play, you will 'learn-by-doing' and experience a data breach involving Canadian, U.S. and E.U. residents. You will make real-time decisions, with a focus on better understanding how breach reporting and individual notification works in practice, including:

- Legislated breach reporting and notifications requirements

- Direct vs. indirect notification
- Who to report/notify and when?
- Drafting breach notifications
- Reporting requirements in quarterly reports and public filings
- Credit monitoring and other best practices for harm mitigation
- Strategic remediation solutions to mitigate reputational risk and maintain brand credibility

4:15 p.m.

Group Debrief and Lessons Learned

Timothy Banks, nNovation LLP, author of the *Guide to Personal Information Protection and Electronic Documents Act* (Lexis Nexis Canada)

As a group, you will reflect on the afternoon workshops and brainstorm on effective strategies and approaches you learned. This will be an engaging session that will reinforce key concepts and provide opportunity for questions.

5:00 p.m.

Program Concludes

Online Primer: Data Breaches and Cybersecurity 101

Note: The Optional Online Primer will become available on October 15, 2019.

For those new to the area or looking for a refresher, this online primer was designed to help lawyers and non-technical executives get an overview of the broad principles pertaining to cyber security law and data breaches.

Recorded in short, segmented modules, you will get a comprehensive overview of legal and regulatory regimes, including a general, but tailored introduction, to key technical concepts. Critical terms – that are complex and often overwhelming – will be broken down and explained in a simple and easy to follow manner.

Chairs

Timothy Banks

nNovation LLP, author of the *Guide to Personal Information Protection and Electronic Documents Act* (Lexis Nexis Canada)

Faculty Includes

Imran Ahmad

Partner, Blake, Cassels & Graydon LLP

Catherine Beagan Flood

Partner, Blake, Cassels & Graydon LLP

Patrick Bourk

Principal – National
Cyber Practice Leader,
Hub International

Karen Burke

Data Protection and Innovation
Consultant, Burke Consulting

Matthew Davies

VP – E&O/Cyber Canada,
Chubb Insurance

David Goodis

Assistant Commissioner,
The Information and Privacy
Commissioner of Ontario

Sue Lajoie

Executive Director, Compliance,
Intake and Resolution;
Directorate, Office of the Privacy
Commissioner of Canada

Lynn Larson

Senior Counsel, Bell

Timothy Walsh

Senior Director, Breach Services,
TransUnion

Lyndsay Wasser

McMillan LLP

Greg Wolfond

CEO, SecureKey Technologies

Registration Details

Fee per Delegate

Program Only: \$695 plus HST

Primer Only: \$295 plus HST

Program + Primer: \$795 plus HST

Newly Licensed (2016 – 2019): \$397.50 plus HST

Fees include attendance, program materials, lunch and break refreshments. Visit www.osgoodepd.ca/financial-assistance for details about financial assistance.

Program Changes

We will make every effort to present the program as advertised, but it may be necessary to change the date, location, speakers or content with little or no notice. In the event of program cancellation, York University's and Osgoode Hall Law School's liability is limited to reimbursement of paid fees.

Cancellations and Substitutions

Substitution of registrants is permitted at any time. If you are unable to find a substitute, a full refund is available if a cancellation request is received in writing 21 days prior to the program date. If a cancellation request is made with less than 21 days notice, a \$75 administration fee will apply. No other refund is available.



OsgoodePD has been approved as an Accredited Provider of Professionalism Content by the LSO.

Eligible CPD/MCLE Hours: LSO (ON): 6h 50m CPD (4h 50m Substantive; 2h Professionalism)



OsgoodePD programs may be eligible for CPD/MCLE credits in other Canadian and US jurisdictions. To inquire about credit eligibility, please contact cpd@osgoode.yorku.ca.



This program is approved for LAWPRO Risk Management Credit.

What participants from other OsgoodePD programs in data breaches and cybersecurity said:

“Good content. Eye opening!

Lots to think about, will go back to the office with great ideas to improve.

Highlights all the potential risks and ways to protect.

Very, very informative.

Great takeaway resources.

I thought it was great, all in all. Good materials and very good presenters. Worthwhile to attend.”



osgoodepd.ca

Osgoode Professional Development



416.597.9724

1 Dundas Street West, Suite 2600



@OsgoodePD

Toronto, ON Canada M5G 1Z3



Data Breaches & Cybersecurity Incidents: The Legal Guide to Preparedness and Response

Register today at:

osgoodepd.ca/databreaches