DATA BREACHES & CYBERSECURITY INCIDENTS:
The Legal Guide to Preparedness and Response

Can't make a live date?
You will have online access to the program for 120 days.

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 intensive course – spread-out over two mornings – 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 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, sign-up for the *Online Primer* **Fundamentals of Data Breaches and Cybersecurity Incidents**. Bundled pricing is available!

> *"It was very good overall. The counsel was excellent and made [the] Scenario."*
>
> **Dimitar Demirevski,** Senior Legal Counsel, Volaris Group

Program Chair

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

Date and Time

November 20 & 27, 2020
9:00 a.m. – 12:30 p.m. &
9:00 a.m. – 1:00 p.m. EST

Online – Live Interactive

Online Replay:
January 21, 2021
9:00 a.m. - 5:00 p.m. EST

Location

Online – includes 120-day access to program archive

Register today at:
osgoodepd.ca/databreaches

LAW SOCIETY OF ONTARIO accredited

APPROVED FOR LAWPRO RISK MANAGEMENT CREDIT

OSGOODE OSGOODE HALL LAW SCHOOL PROFESSIONAL DEVELOPMENT | YORK UNIVERSITÉ UNIVERSITY

Data Breaches & Cybersecurity Incidents:

The Legal Guide to Preparedness and Response

More than ever before, cybersecurity lapses and other data breaches have become a top concern for businesses.

How many organizations had their data breached in the past year? Almost **all of them**, suggests a recent survey. A panoply of companies face difficult **consequences, steep fines, and these actions and penalties are public, often making headline news, and trust is difficult to regain once breached**.

To avoid costly missteps, you must ensure you **know the right questions** to ask, have appropriate **protocols** and **procedures** in place, and the **skills** and **knowledge** you need to competently respond to a security incident or to advise your team and stakeholders.

This essential *OsgoodePD* program provides you with a **practical** overview of how to prepare for and respond to a data breach and cyber incident. The **solutions-focused instruction** draws from **real-world examples** of cybersecurity designs, plans, incident responses, insurance policies and procedures.

Get Important Insights, Including:

- Navigating breach reporting laws in Canada, the US and Europe/UK
- Current trends in data breach and privacy litigation
- Key components and strategies for an effective incident response plan
- The role and composition of the breach response team and tips for best practices
- Legislated breach notification requirements and drafting breach notifications
- Conducting an organizational review to minimize and mitigate data breach risks
- How to ensure that you're properly insured and that your insurance responds

PLUS! Using a sample case scenario, you will get hands-on learning to help you ensure a cyber-resilient organization.

This Intensive Course is Essential For:

- Lawyers practicing in corporate law, privacy law or information technology law
- Business leaders (executive officers, information/privacy officers, technology officers)
- Government and regulatory representatives
- Professionals working in cybersecurity, data breaches, privacy, compliance, risk management and anti-money laundering
- Banking and financial services professionals and executives
- Anyone with a keen interest in cybersecurity, data breaches, and privacy

Agenda

November 20, 2020
9:00 a.m. to 12:30 p.m. EST

MODULE ONE: Understanding Your Legal Obligations

9:00 a.m.

Chair's Welcome & Opening Remarks

9:15 a.m.

Navigating Breach Reporting Laws in Canada, the US & Europe/UK

A timely session on the key similarities and differences in breach reporting laws across Canada, the United States and Europe/UK, including:

- Cross-Canada survey
- Spotlight on notable reforms – anticipated QC legislation and legal reforms coming out of other provinces, including BC
- Comparison with key US and European/UK breach reporting laws
- How to address conflicts, redundancy and other jurisdictional matters

Faculty: Sean Hoar, James Lloyd, Lyndsay Wasser

10:30 a.m.

Health Break

10:45 a.m.

Understanding Your Legal Risks & Damages: An Essential Litigation Update

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 crucial update will provide you with a succinct review of recent incidents in Canada and elsewhere. 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?

Faculty: Catherine Beagan Flood

11:45 a.m.

How to Ensure that Your Insurance is Adequate & Responds

Get tactical guidance to evaluate whether you're properly insured against cyber risks and to ensure that you are adequately covered in the event of an incident, including:

- Review of the principal framework of insurance policies – to what extent do traditional policies apply to data breaches?
- Understanding a "cyber" policy or a data breach insurance policy
- The interplay between insurance and other remedies
- Review of key considerations to determine successful coverage and ensure insurance response (includes checklist)

Faculty: Gregory Eskins, Jennifer Hunter

12:30 p.m.

End of Module One

November 27, 2020
9:00 a.m. to 1:00 p.m. EST

MODULE TWO: Practical Guidance on Security, Privilege & the Incident Response Plan

9:00 a.m.

Chair's Welcome and Opening Remarks

9:15 a.m.

Incident Response Plans: How Can Legal and Security Work Together More Effectively?

- What does a good incident response plan entail?
- Not really a legal document – so what is it? Elements you need to watch out for
- How does the incident response plan impact the issue of privilege?
- How to get security and legal working together? Best practices and "lessons learned"
- Tools and tactics for ensuring a collaborative team effort

Faculty: Ed Dubrovsky, Daniel Glover

10:15 a.m.

Health Break

10:30 a.m.

Interactive Practical Exercise: The Incident Response Plan (IRP)

Using a mock Incident Response Plan (IRP), you will engage in a live, online interactive fact scenario that exposes key weaknesses in an organization's preparedness and benefit from a valuable debrief.

You will learn the key components of an IRP, weak links in a crisis, how to make timely decisions and better understand how breach reporting and individual notifications work in practice.

This exercise will give you hands-on experience in responding to a data breach. You will emerge with a better understanding of how test and evaluate your organization's own data governance program, including your IRP.
Topics discussed will be drawn from:

- The roles and responsibilities of key stakeholders, including: legal counsel, public relations, forensics and notification providers
- Tactics for effective communication plans
- Due diligence requirements when selecting vendors and sub-contractors
- Contractual terms regarding privacy and security, and audit rights
- Negotiating obligations and indemnities
- Escalation protocols for breaches, and drafting breach notifications
- Testing and monitoring incident response protocols
- Direct vs. indirect notification – includes who and when to notify/report, quarterly reports and public filings
- Credit monitoring and other harm mitigation steps
- Strategic remediation solutions to mitigate reputational risk & maintain brand credibility

Faculty: Imran Ahmad, Timothy Banks, Lynn Larson

11:45 a.m.

Crucial Regulatory Updates

The regulatory framework for reporting of breaches of security safeguards is rapidly changing. Hear from major regulators on the latest, including clarification on your new legal and reporting obligations.

- Summary of crucial updates and new requirements
- Understanding the new requirements – are organizations over-reporting or underreporting?
- What are the common mistakes organizations make when reporting and how to address them?
- What happens when the regulator begins an investigation? How should you respond?

Faculty: Sonja Hanisch, David Goodis

1:00 p.m.

End of Module Two; Program Concludes

ONLINE PRIMER *(Optional)*: Fundamentals of Data Breaches & Cybersecurity Incidents

For those new to the area or looking for a refresher, this module was designed to provide you with a succinct overview of the broad principles in cybersecurity law and data breaches and reporting requirements. Recorded in short segments, you will get a practical overview of legal and regulatory regimes, and an introduction to key technical concepts and terms, explained in a simple and easy to follow manner.

- General Framework of Reporting (approx. 37 mins)
- Reporting to the Office of the Privacy Commissioner of Canada (approx. 25 mins)
- Notification to Individuals (approx. 38 mins)
- Record Keeping (approx. 24 mins)

Faculty: Timothy Banks, Karen Burke, Lindsay Wasser

(Approx. 2 hours total, 4 segments, available on-demand)

Register today at:

osgoodepd.ca/databreaches

Chair

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

Faculty

Imran Ahmad
Partner, Blake, Cassels & Graydon LLP

Catherine Beagan Flood
Partner, Blake, Cassels & Graydon LLP

Karen Burke
Data Protection and Innovation Consultant, Burke Consulting

Ed Dubrovsky
Managing Partner & Managing Director, Cyber Breach Response, Cytelligence Inc.

Gregory Eskins
Canada FINPRO Practice Leader | Managing Director, Marsh & McLennan Companies

Daniel Glover
Partner, McCarthy Tétrault LLP

David Goodis
Assistant Commissioner, Office of the Information and Privacy Commissioner of Ontario (IPC)

Sonja Hanisch
Manager, Breach Response Unit, Compliance, Intake, and Resolution Directorate, Office of the Privacy Commissioner of Canada (OPC)

Sean Hoar
CISSP, CIPP/US, Partner, Lewis Brisbois Bisgaard & Smith LLP, Portland, OR, USA

Jennifer Hunter
Partner, Lerners LLP

Lynn Larson
Senior Counsel, Bell Canada

James Lloyd
Partner, Orrick Herrington & Sutcliffe LLP, London, England, UK

Lyndsay Wasser
CIPP/Canada, Co-Chair, Privacy & Data Protection, & Co-Chair, Cybersecurity, McMillan LLP

"It was a great program [and] I learned a lot. [T]he scenarios were excellent, [and] the role play scenarios were great for practical learning. [D]iscussion about actual breach scenarios was enlightening."

Saleema Kassam, Legal Counsel, CAPREIT

Data Breaches & Cybersecurity Incidents:

The Legal Guide to Preparedness and Response

Registration Details

Fee per Delegate
Program (two half-days): $695 plus HST
Online Primer: $295 plus HST
Bundle Online Primer + Program: $795 plus HST (save $200)
Newly Licensed (2017 – 2020): 50% off regular rate

Fees include attendance, electronic program materials, and 120-day access to the program archive. Group discounts and financial assistance available. Visit www.osgoodepd.ca/group-discounts for details.

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 14 days prior to the program date. If a cancellation request is made with less than 14 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 Hours
Online Primer – LSO (ON): 2h CPD (1h 15m Substantive; 45m Professionalism)
Program – LSO (ON): 7h CPD (6h Substantive; 1h 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.

osgoodepd.ca
416.597.9724
@OsgoodePD

Osgoode Professional Development
1 Dundas Street West, Suite 2600
Toronto, ON Canada M5G 1Z3

Register today at:
osgoodepd.ca/databreaches