NEW

Professional Development Certificate

Cybersecurity & The Law:

Risk Management in the Digital Economy

April 12 - May 7, 2024 | 5 weeks | Part-time | Hybrid | $3,995 + HST

As cyber threats become more sophisticated, the need for corporate leaders and legal professionals well-versed in the intricacies of cybersecurity and AI is paramount. Our new certificate program is your shield against these risks.

You Will:

- Test your capacity to **spot potential exposures to harm** and to **focus on solutions.**
- Learn how to **assess & communicate risks effectively** and to **enact policies that reduce risks**.
- Hear from industry experts about **developing cybersecure business practices.**
- Learn how to **advise various stakeholders when your systems are compromised**.
- Practice skills and **learn to work collaboratively** with tabletop exercises and simulations.

Register today at: **cybersecurityandthelaw.ca**

Toronto Metropolitan University

Lincoln Alexander Law
Professional Development

ROGERS
cybersecure
catalyst

LAW SOCIETY
OF ONTARIO
accredited

You will learn and gain tremendous insight from a faculty of leading privacy and legal experts

Program Chairs

Imran Ahmad

Partner, Head of Technology, Co-Head of Information Governance, Privacy and Cybersecurity, Norton Rose Fulbright Canada LLP

Imran advises clients across all industries on a wide array of technology-related matters, including outsourcing, cloud computing, SaaS, strategic alliances, technology development, system procurement and implementation, technology licensing and transfer, distribution, open source software, and electronic commerce.

As part of his cybersecurity practice, Imran works with clients to develop and implement strategies related to cyber threats. He advises on legal risk assessments, compliance, due diligence, security, and data breach incident preparedness and response.

Imran often acts as "breach counsel" in the event of a cybersecurity incident, and has extensive experience in managing complex cross-border security incidents. He also provides representation in the event of an investigation, enforcement action or litigation.

Imran is the author of Canada's first legal incident preparation and response handbook *Cybersecurity in Canada: A Guide to Best Practices, Planning, and Management, 2nd Edition* (LexisNexis, March 2021).

Noemi Chanda

Partner, Data Protection and Privacy Leader, Cyber Risk, Deloitte LLP

Noemi is a Partner in Deloitte's Data Protection and Privacy practice in Toronto. She provides privacy, data protection, and cyber strategy services for organizations seeking to deliver new and better services for their clients and the community, advising in the areas of regulatory compliance, data protection, information privacy, and risk management.

She specializes in serving technology, healthcare, retail, and public sector clients participating in new initiatives that involve the collection or use of personal information.

Prior to Deloitte, she articled at Borden Ladner Gervais LLP and was a Visiting Researcher at the University of Washington Tech Policy Lab, where she looked at privacy in the context of the Internet of Things, AI, connected and autonomous vehicles, and robotics. Noemi holds a BA from the University of Waterloo, a Master's in Economic Policy from McMaster University, and a law degree from the University of Toronto Faculty of Law. She is licensed to practice law in Ontario.

.

Program Speakers

Imran Ahmad, Partner, Head of Technology, Co-Head of Information Governance, Privacy and Cybersecurity, Norton Rose Fulbright Canada LLP

Jason Ball, Vice President Legal, Rogers Communications

Melissa Carvalho, Vice President Global Cyber Security Strategic Services, RBC

John Comacchio, Senior Vice President and Chief Information Officer, Teknion

Sunny Handa, Partner, Head of Technology, Co-Head of Information Governance, Privacy and Cybersecurity, Blakes

Naveen Hassan, Associate General Counsel & Director, Privacy and Risk Management, The Hospital For Sick Children

Shurouq Hijazi, Director, KeyData Associates

Kevin Magee, CSO, Microsoft

Charles Muggeridge, Author, FleishmanHillard HighRoad

Sarah Muttitt, Vice President and Chief Information Officer, UHN

Iain Paterson, Chief Information Security Officer, WELL Health Technologies

Laurie Pezzente, Senior VP, IT Risk, RBC

Melanie Power, Detective Staff Sergeant, Manager Cyber Crimes Investigations Team, Ontario Provincial Police

Ruth Promislow, Partner, Bennett Jones LLP

Molly Reynolds, Partner, Torys LLP

Sundeep Sandhu, Vice President, Cyber Security & CISO Rogers Bank, Rogers Communications

Jeff Schwartzentruber, Sr. Machine Learning Scientist, eSentire

James Stewart, CEO - Founder, TrojAI

Murali Vigendran, Virtual CISO, Cyber Risk Researcher, Responsible AI SME, Gen AI Implementation, SigmaRed Technologies

Benefits of the Course:

Comprehensive Expertise:
Attending this course equips participants with a deep understanding of the interplay between cybersecurity and legal considerations. Attendees can provide nuanced advice that addresses both technical and legal dimensions.

Regulatory Mastery:
Through in-depth modules, participants gain the knowledge to navigate complex regulatory landscapes. This enables the alignment of data practices with legal requirements, ensuring clients' cybersecurity measures remain compliant and robust.

Crisis Preparedness:
Practical exercises and discussions enhance participants' crisis management skills. They learn to provide effective support to clients during critical incidents and offer forward-looking guidance in ever-evolving tech environments.

Strategic Insights:
The program fosters the ability to assess cybersecurity postures, identify vulnerabilities, and offer tailored advice. This ensures that clients receive advice that is both legally sound and strategically aligned, enhancing overall cybersecurity effectiveness.

LAW SOCIETY
OF ONTARIO
accredited

The Lincoln Alexander School of Law is an accredited provider with the Law Society of Ontario.

This program contains:

Substantive Content - **32 h 45 m**
Professionalism Content - **2 h**
EDI (Equality, Diversity and Inclusion) Professionalism Content - **1 h**

TOTAL: 35 h 45 m

Who should attend:

- **Senior Leaders and Managers:** Learn how to define business requirements, identify technology assets, and engage with stakeholders while implementing policy.
- **Technology Team Leads:** Enhance tech solutions with a strong grasp of legal compliance.
- **In-house / Corporate Counsel:** Strengthen expertise in cybersecurity and AI law, and provide more effective legal guidance and risk management within organizations.

Agenda

WEEK 1

Module 1: Understanding Technology in Contemporary Business*

Explore the evolving landscape of technology in today's business world, with a focus on client-based cybersecurity needs and risk assessment.

Course Introduction and Administration: Introduction to the program, assessment requirements, and participant introductions.

Defining the Client's Business Context: Understanding organizational missions, governance structures, and threat and risk assessments.

Exercise - Perspectives on Cybersecurity and Legal Advice: Q&A with guest speakers to define the client's business context.

Establishing How the Client Uses Digital Technologies: Overview of digital infrastructure, data types, and cybersecurity considerations.

Technology in Contemporary Business: A deeper look at the role of technology in today's business environment.

Exercise- Business Technology Mapping: Groups analyze technology maps to identify purposes and potential vulnerabilities.

Assessing Client's General Cybersecurity Posture: Analyzing client contexts and potential cyber issues requiring legal insights.

WEEK 2

Module 2: Assessing Legal Risks in Cybersecurity

Dive into the legal implications of client cybersecurity risks, including case law, regulatory landscapes, and providing relevant legal advice in the cybersecurity context.

Identify Legal Implications Related to Client Cybersecurity Risk: Understanding the legal impacts of cybersecurity risks, case law, and regulatory contexts.

Define the Information/Data Regulatory Landscape: Exploration of privacy laws, data protection, and international regulations.

Providing Situated and Relevant Advice on Legal or Regulatory Issues: Sources of expertise and resources for legal counsel in cybersecurity.

Providing Advice Based on Organizational Context: Evaluating the client's cybersecurity posture, in-house and outsourced capabilities, and legal implications.

Ensuring a Common Understanding of Threats and Risks: Establish a consistent interpretation of threat and risk across an organization - communicating cyber to different audiences.

Exercise - Identify Threats and Vectors: Identifying primary threats and attack vectors based on a scenario.

Providing Legal Advice in Cybersecurity: Balancing risks and trade-offs when providing legal advice.

WEEK 3

Module 3: Privacy, Data, and Information Protection in the Digital Economy

Delve into data use, transmission, and storage requirements relative to regulatory mandates, examining types of data and protection mechanisms.

Examine Client's Data Use and Protection Requirements: Overview of data types and the importance of data protection.

Exercise - Advising on Compliance in Support of Client Security Requirements Definition: Identifying the client's regulatory environment and legal responsibilities for data protection.

Challenges in Data Security and Legal Implications: Exploring data security challenges and their legal ramifications.

Exercise - Oversee a Privacy Impact Assessment (PIA): Walk-through and completion of a PIA template based on a case.

Determine Level of Compliance and Organizational Risk: Ethical decision-making, due diligence, and tangible and intangible impacts of non-compliance.

* The program schedule is available on the website: **cybersecurityandthelaw.ca**

Agenda

WEEK 4

Module 4: Supporting a Client in Crisis: Advising in Cybersecurity Incident Response

Prepare for crisis management and learn to deliver legal advice during cybersecurity incidents, including tools, techniques, and post-incident analysis.

Advise Clients in Crisis: Understanding crisis management and communication during cybersecurity incidents.

Advising Clients in Crisis – Tools and Techniques: Practical tools and techniques for advising clients during crises.

Identify Legal Issues Throughout the Incident Response Process: Exploring legal considerations in the incident response phases.

Exercise - Basic Breach Scenario: Simulated exercise to understand cybersecurity incident response.

Guide Post-Incident Activities Through a Legal Lens: Addressing legal fallouts, lessons learned, and reporting post-incidents.

Legal Issues – Post-Incident Analysis: Discussing legal issues arising in post-incident analysis and activities.

WEEK 5

Module 5: Legal and Ethical Challenges and Opportunities of AI in Cybersecurity - Symposium & Synthesizing Exercise

Program concludes with a symposium on AI as an emergent technology and the changes it is driving in both the legal and cybersecurity landscapes with an emphasis on ethical adoption. Certificate participants will lead a synthesizing exercise.

Understanding the Legal Landscape: AI as a Cybersecurity Threat and Solution: Dissecting the impact of artificial intelligence on cybersecurity and considered legal responses.

Managing Ethical AI in Cybersecurity: Exploring the role organizations play in the acquisition, deployment & implementation of AI cybersecurity solutions & the potential ethical implications.

Exercise - Lead the Discussion: Using learning concepts & frameworks gained throughout the program, Certificate participants will lead small group discussions among symposium attendees to surface opportunities & challenges, identify stakeholders, & suggest guardrails on organisational uses of AI in cybersecurity. Exercise will conclude with a group presentation to the plenary session.

Fireside Chat: Cybersecurity and AI – Who loses? The case for more inclusive engagement: A broad discussion of the inclusivity issues posed by AI and cybersecurity, including an examination of the digital divide and the potential for AI to improve or worsen existing inequities. The conversation will highlight the need to consider a broad range of populations and use cases when integrating technology advancements.

> *“With new legislation, the rapid adoption of AI technology, and increased costs in cybersecurity insurance, in-house counsel are facing new challenges in keeping up with data security.*
>
> *…Organizations that incorporate privacy into their systems are at a competitive advantage with consumers and in recruiting employees.”*
>
> - Canadian Lawyer,
> May 30, 2023

About Us

Certificate in Cybersecurity & The Law is a collaboration between the **Lincoln Alexander School of Law** and **Rogers Cybersecure Catalyst** at Toronto Metropolitan University.

Toronto Metropolitan University

Lincoln Alexander Law Professional Development

The Lincoln Alexander School of Law at Toronto Metropolitan University is reimagining legal education. Its mission is to equip lawyers with the contemporary skills and experience required to expand the reach of justice and to respond to the evolving challenges that face Canadian society.

The law school is launching a new professional development program designed to serve practicing lawyers and business professionals in Ontario and beyond. The Cybersecurity & The Law certificate is one of several offerings in an upcoming series of accredited professional development certificates.

ROGERS cybersecure catalyst

Rogers Cybersecure Catalyst is Toronto Metropolitan University's national centre for training, innovation and collaboration in cybersecurity. Headquartered in Brampton, Ontario, and offering programs and services across Canada, the Catalyst empowers individuals and organizations to seize the opportunities and tackle the challenges of cybersecurity.

Together with its partners and collaborators, the Catalyst works to realize a vision of healthy democracies and thriving societies, powered by safe and secure digital technologies.

Registration Details

Pricing

Price: $3,995 + HST.

Group Discounts

Group discounts are available. Organizations sending 2-10 attendees are entitled to a 10% discount. For larger groups please get in touch for available discounts. If you wish to receive an invoice or to register as a group, please contact Bernard Sandler at bsandler@torontomu.ca.

Cancellation and Refund Policy

A full refund is available up to three weeks before the program start date. After that, a refund minus a $300 processing fee is available until the start date. No refunds are available once the program has begun. Attendee substitutions can be accommodated.

Certificate of Program Completion

Attendees will receive a certificate upon completion of this program. Participants must attend all program modules and participate in small group and online activities to receive a certificate.

Register Today at: **cybersecurityandthelaw.ca**

For Further Program-Related Information, Please Contact:

Bernard Sandler
Professional Legal Education Program Manager, Lincoln Alexander School of Law
bsandler@torontomu.ca