

CPE Credits
11 Hours

Technology and Cybersecurity Risk Management

Comprehensive and Practical Information for Organizational
Management of Technology Risks and Threats

December 13 - 14, 2017 • Toronto

Technology and Cybersecurity Risk Management leads you through the essential elements required to manage and mitigate the operational impact of these looming, and seemingly inevitable, risks including:

- IT/Cybersecurity Risks In The Enterprise Risk Management Plan
- Identifying Sources of IT Risk and Tactics to Manage/Reduce Risk
- Cybersecurity and Risk Mitigation – Not “If” But “When” and Dealing with “Cyber-Fatigue”
- Personal Data Management and Protection
- Third Party Risk Management – IT and Cybersecurity
- Risk-Based Risk Management – Why Controls/Audit Are Not Enough
- Monitoring and Detecting Threats Including the Use of Analytics
- Quantifying Cyber Risk in Economic Terms
- Case Study: Examining a Breach and Recovery – What a Recovery Plan Looks Like
- Cybersecurity/IT Insurance Coverage – Ins and Outs of Risk Mitigation
- Current Cybersecurity Legal Risks and Requirements
- SOX, Certification, Financial Reporting and Disclosure

Who Will Be Presenting

- Deloitte LLP
- Ernst & Young LLP
- Fasken Martineau DuMoulin LLP
- KPMG LLP
- Mandiant, a FireEye Company
- Marsh McLennan
- Meyers Norris Penny LLP
- PricewaterhouseCoopers LLP
- Risk Lens

Who Should Attend:

- Chief Financial Officers
- Chief Risk Officers
- Chief Accountants
- Chief Compliance Officers
- VPs, Directors and Managers
 - Risk Management/Reporting
 - Finance
 - Technology and Data Security
 - Compliance
 - Accounting
 - Financial Reporting
 - Regulatory Accounting
- Controllers
- Internal Auditors
- Risk Managers
- Audit Committee Members
- Corporate Counsel
- Audit and Assurance Professionals
- Industry Regulators and Standard Setters
- Financial Analysts

FREE

Digital Copy of
Conference Proceedings

All final materials delivered at the conference will be made available to delegates after the conference in electronic format in addition to the conference manual.

Program - December 13**9:00 a.m. – 9:05 a.m.****Opening Remarks from the Chair***Eugene Atangan, A.V.P. Operational Risk Management,
TD Bank Group***9:05 a.m. – 10:00 a.m.****IT/Cybersecurity Risks In The Enterprise Risk Management Plan***Paul Hanley, Partner, Deloitte LLP*

- An overview of new & emerging cybersecurity risks
- Understanding IT risks in your organization
 - identifying external threats
 - internal sources of risk - personnel, contractors, third party vendors
- Implications of IT/cybersecurity risks - financial, reputational, regulatory
- Breaking down silos – integrating IT/IT risk management with broader organization
- How Boards are reacting to security breaches and IT risks – concerns and expectations
- Dealing with IT and cybersecurity risks as business risks – leveraging your ERM plan
- IT risk management's missing link – connecting IT frameworks (COBIT, ISASCA) to the broader enterprise risk management framework to achieve corporate goals
- Developing a risk appetite statement for IT risk
- Understanding the limits of a controls-based framework to manage risk – when is there a need for a risk-based approach to ITRM
- Quantifying IT risk management expenses and the cost of losses from hacks/theft – tackling the security budgeting challenge
- Creating your IT risk dashboard including key risk indicators (KRIs) and key performance indicators (KPIs)
- Practical examples and insights from working experiences

10:00 a.m. – 11:00 a.m.**Identifying Sources of IT Risk and Tactics to Manage/Reduce Risk***Yassir Bellout, Partner, Cyber Security, KPMG LLP*

- Highlighting risks from established IT/communications technology
- Considerations for risks arising from more recent and emerging technologies
 - cloud computing
 - payment technologies
 - mobile/connected devices
 - blockchain
 - artificial intelligence
- Ensuring your risk appetite documentation anticipates and enables new technology adoption
- Issues in developing risk management strategies for new and unfamiliar applications
- Methodologies to consider for the introduction of technology to the organization from a risk management perspective

11:00 a.m. – 11:15 a.m. Morning Networking Break**11:15 a.m. – 12:15 p.m.****Cybersecurity and Risk Mitigation – Not “If” But “When” and Dealing with “Cyber-Fatigue”***Marcus Troiano, Principal Consultant, Strategic Cybersecurity Services, Mandiant – A FireEye Company*

- Overview of today's cybersecurity threat landscape
 - who are the attackers?
 - what are their objectives?
 - understanding their targets and why they were chosen
 - effects of attacks on business organizations
 - insights on attacks the media do not cover
- Examples of attacks and what was learned from them
- What role have “insiders” played in cybersecurity attacks?
- Attacks resulting in physical damage to IT infrastructure/loss of assets
- Establishing defences and mitigation tools to counter an unseen, dynamic threat
- Examination of best practices and leading mitigation tools

12:15 p.m. – 1:15 p.m. Luncheon**1:15 p.m. – 2:15 p.m.****Personal Data Management and Protection***Jordan Prokopy, Director and Privacy Practice Leader,
PricewaterhouseCoopers LLP*

- Personal data protection landscape and trends in Canada and globally
- Regulatory requirements for personal data management and protection
 - breach notification
 - retention/destruction
 - personal data inventorying and mapping
 - individual access/correction/erasure rights
 - data protection impact assessments and privacy by design
- Technology's role in data protection

2:15 p.m. – 3:15 p.m.**Third Party Risk Management – IT and Cybersecurity***Gus Leite, Director Risk Assurance, PricewaterhouseCoopers LLP*

- Identifying third parties creating risk exposure
 - contractors
 - vendors
 - outsourced IT management
 - IT and communications service providers
 - cloud computing services
- Tackling the challenge of third parties providing services to your third parties – how to control the supply chain
- Steps to take prior to entering into outsourcing agreements
- How to monitor risks associated with third parties
- How cyber attacks use third parties to gain access to primary targets
- What to do beyond contract requirements
- Can using analytics assist in managing third party risks?
- Regulatory requirements for third party risk management
- Frameworks and processes available to utilize

3:15 p.m. – 3:30 p.m. Afternoon Networking Break

3:30 p.m. – 4:30 p.m.

Risk-Based Risk Management – Why Controls/Audit Are Not Enough

Jason Murray, Senior Manager, MNP LLP

- Clarifying the objectives and limitations of internal control
- Why internal audit cannot do it all
- How a risk-based management process moves from reaction and complacency to risk anticipation and response
- Everything starts with realistic risk assessment – what does “low tolerance” really mean to an organization?
- Evaluation of cybersecurity risks using similar methodology to other risks
- Basing decisions on knowing acceptable risks and quantifying potential loss
- ISO 27001 and NIST – best practices frameworks

Program - December 14

9:00 a.m. – 9:05 a.m.

Opening Remarks from the Chair

Eugene Atangan, A.V.P. Operational Risk Management, TD Bank Group

9:05 a.m. – 9:50 a.m.

High Definition Threat Detection – How to Enhance Cyber Hunting with Analytics

Naveed Islam, Manager, KPMG LLP

- Cybersecurity landscape – evolving threat capabilities and monitoring/detection tactics
- Security relevant data sources (internal and external)
- The traditional security monitoring model and use case development
- The model that works
- What are analytics in the cybersecurity context?
- The right place for analytics in security operations
- How to assess maturity of your cybersecurity operations

9:50 a.m. – 10:45 a.m.

Quantifying Cyber Risk in Economic Terms

Jack Jones, Co-Founder and E.V.P. Research and Development, Risk Lens

- How and why current risk measurement methods fail
- Common misperceptions regarding cyber risk quantification and why they're wrong
- The two models required for solid cyber risk quantification
- Distinguishing direct losses from broader and sometimes more subtle fallout
- The hard part of risk quantification (and it isn't data)
- The real differences between qualitative and quantitative risk measurement
- How to lay the foundation for effective risk measurement in your organization

10:45 a.m. – 11:00 a.m. – Morning Networking Break

11:00 a.m. – 12:00 p.m.

Case Study: Examining a Breach and Recovery – What a Recovery Plan Looks Like

Seyed Hejazi, Manager, Ernst & Young LLP

- Dissecting a cyber attack – planning a response
- Identifying the essential matters to address and considering priority
- Key communications issues
- Do regulators need to be notified? External stakeholders?
- Examples of incidents and how the fallout was handled – what has been learned?
- What should be built into a recovery plan and allocating responsibilities
- Getting the recovery plan off paper – how to ensure timely, effective response
- Post-recovery considerations and modifying a pre-attack recovery plan

12:00 p.m. – 1:00 p.m. Luncheon

1:00 p.m. – 2:00 p.m.

Cyber Insurance 101 – Ins and Outs of Risk Mitigation

Catherine Evans, Vice President, Marsh McLennan

- How to think about and quantify cyber risk
- Traditional insurance coverages and cyber risk
- What do cyber policies cover and what's not covered?
- Key coverage considerations
- Underwriting process and the information required
- Sample loss scenarios and claims concerns
- Market trends

2:00 p.m. – 3:00 p.m.

Current Cybersecurity Legal Risks and Requirements

Alex Cameron, Partner, Fasken Martineau DuMoulin LLP

- PIPEDA (Personal Information and Protection and Electronic Documents Act) and Digital Privacy Act
 - when to notify individuals and report to the Commissioner
 - requirement to notify related third party organizations to mitigate risk
 - mandatory record-keeping for breaches
 - enforcement and penalties
 - provincial regulations mirroring PIPEDA
- Canadian Security Administrators – CSA Staff Notice 11-332
- OSFI and cybersecurity
- Litigation and class action risks arising from cybersecurity breaches
 - summary and update of the latest cases and trends
 - potential liability for privacy breaches
 - lessons learned from how plaintiffs frame their claims
 - the importance of effective incident response
 - effective legal risk management

Technology and Cybersecurity Risk Management

FAX THIS REGISTRATION FORM NOW TO (416) 504-6978

264

Yes! Register me for: Technology and Cybersecurity Risk Management

Photocopy this form for additional delegates.

I cannot attend but please keep me informed of future events

Mr./Ms./Mrs. _____

Title _____

Company _____

Address _____

City _____ Province _____ Postal Code _____

Telephone () _____ Extension _____ Fax () _____

E-mail Address _____

Company's main line of business _____

Number of employees on site

1-25 26-50 51-100 101-250 250 - 500 501+

Please send me a **FREE Toronto and Area Visitor's Information Package**

Please do not remove or obscure address below.

Acumen Information Services
Suite 1100, 151 Yonge Street
Toronto, Ontario M5C 2W7
HST No. R862562543



Sponsorship and Exhibition Opportunities Limited

Sponsorship and exhibition options are available for this event. For more information or to check availability, please contact us by phone at (416) 504-6952 or by e-mail at info@acumeninformation.com.

REGISTER NOW - HERE'S HOW!

1. Fax: (416) 504-6978
2. Mail:
Acumen Information Services
Suite 1100, 151 Yonge Street
Toronto, ON, M5C 2W7
3. E-mail:
info@acumeninformation.com
4. On Line:
<http://www.acumeninformation.com>
5. Phone: (416) 504-6952

Register Me For:

Registration Options	Before November 1, 2017	Before November 15, 2017	After November 15, 2017
IT/Cybersecurity Risk	\$1,999.00 + HST	\$2,099.00 + HST	\$2,199.00 + HST

Please register me with the **early-bird discount** (ends November 15, 2017)

Payment Method

Please Charge to my VISA MASTERCARD

Card Number: _____ Expiry Date: _____

Signature: _____ Security No. _____

Cheque enclosed, payable to **Acumen Information Services**

Please invoice me

Early Bird Special

Register prior to **November 15, 2017** and you will obtain the following savings:

Second delegate: \$100 Discount
Third delegate: \$150 Discount
Fourth delegate: **FREE**

GROUP DISCOUNT

Fourth Delegate Free!

If three individuals from one organization register at the same time, a fourth person may also be registered to attend free of charge. The free registration must be of equal or lesser value than the paid registrations. Please contact us to arrange for attendance of larger groups.

Location and Accommodation

The conference will be held at a convenient location in downtown Toronto. Venue information and special conference accommodation pricing details will be provided upon confirmation of the venue.

Delegates can register at the Acumen service desk beginning at 8:00 a.m. on the morning of the first day of the conference. Registration fees do not include hotel accommodation.

Group Discount: Fourth Delegate FREE!

If three individuals from one organization register at the same time, a fourth person may also be registered to attend free of charge. The free registration must be of equal or lesser value than the paid registrations. Please contact us to arrange for attendance of larger groups.

Your Registration Includes

Registration fees include all conference materials, continental breakfast, lunch and refreshments. Parking and accommodation are not included.

Cancellation Policy

Substitutions may be made at any time. If you are unable to attend, please make cancellations in writing and fax to (416) 504-6978 prior to 5:00 p.m. on November 30, 2017. A credit voucher will be issued to you for the full amount, redeemable against any other Acumen conference. If you prefer, you may request for a refund of fees paid less \$250.00 administration fee. Registrants who cancel after above date will not be eligible to receive any credits or refunds and are liable for the entire registration fees.

Confirmed delegates who do not cancel before November 30, 2017, and fail to attend will be liable for the entire registration fees.

Duplicate Mailings or Incorrect Information

Please advise us if you receive a duplicate mailing of this brochure or if you would like us to change any of the mailing information shown on the brochure. Please fax us a copy of the registration form with the changes you would like us to make. Please pass the additional copy on to a colleague.

The Acumen Guarantee

If you find that this event does not meet the high quality standards you expect from this event, we will issue you a letter of credit equal to the value of the event. The individual delegate or any member of his or her company may use this letter of credit for two years from date of issue. Write us a letter describing why you were dissatisfied and direct it to the General Manager. Acumen Information Services reserves the right to change the date, location and content for the event(s) offered herein without further notice and assumes no liability for such changes.