

Privacy Breach Risk and Insurance

Vancouver Presentation
10 April 2014



Presented by
Brian Rosenbaum LL.B
National Director
Aon Risk Solutions™
Financial Services Group
Legal and Research Practice
Aon Cyber and Privacy Group

AON

Agenda

- Regulatory/Legislative Landscape
 - Canada Overview
 - Multiple Applicable Laws
 - PIPA v PIPEDA
 - Europe/U.S.
- Privacy Breach Notification Laws
 - Canada
 - Alberta
 - U.S.
- Securities Laws
- D&O Privacy Liability
- Payment Card Industry Standards
- OSFI Memorandum: Cyber Security Guidance/Self Assessment

Agenda

- Key Self-Examination Questions
- Privacy Breach Statistics
 - Causes of Publicly Reported Privacy Breaches
- Cost of a Loss
 - Third Party
 - › *Litigation*
 - › *Regulatory Actions*
 - First Party
- Insurance Under Traditional Policies
- Specialized Insurance
- Hot Button Policy Issues
- Aon Initiatives, Tools and Resources
- Questions

Regulatory/Legislative Landscape | Canada

Private Sector

- Federally
 - Personal Information Protection and Electronic Documents Act (PIPEDA)
- Provincially
 - British Columbia Personal Information Protection Act (PIPA)
 - PIPEDA, Alberta PIPA, Québec PPIPS, Manitoba PIPITPA (when in force)

Public Sector

- Federally
 - Privacy Act
- Provincially
 - BC: Freedom of Information Protection of Privacy Act (FIPPA)
 - Similar acts in other provinces

Health Information

- British Columbia
 - PIPA applies to health care providers in private practice
 - FIPPA applies to health authorities and hospitals
 - E-Health Act applies to designated databases
- Other Provinces
 - Ontario: PHIPA
 - Alberta HIA
 - Manitoba: PHIA
 - Saskatchewan: HIPA
 - New Brunswick: PHIPAA
 - Nova Scotia: PHIA
 - Newfoundland & Labrador: PHIA

Multiple Applicable Laws

- PIPEDA could apply on its own or in tandem with PIPA
- PIPEDA could apply to BC-regulated organizations if they collect or transfer PI across provincial or international borders:
 - Use a national credit reporting bureau based outside of BC to run credit checks
 - Sell a mailing list to another province
 - Send customer data to a loyalty program in another province
- Both PIPA and PIPEDA could apply to BC-regulated organizations if they are:
 - Under contract to another organization that follows a different privacy law and are obligated by that contract to follow the organization's rules (i.e. consulting services to FWUB)
 - Involved in cross-boarder PI flows
- Ensure your organization is complying with the highest standards of any applicable law



Regulatory/Legislative Landscape

PIPA v PIPEDA

- Although PIPA is similar to PIPEDA, there are changes that BC organizations need be aware
- PIPA applies to non-profits even when engaged in non-commercial activities (PIPEDA only applies to NPOs when they engage in commercial activities)
- PIPA applies to employee PI (PIPEDA does not unless FWUB)
- Grandfather provisions under PIPA for PI collected prior to enactment in 2004 (PIPEDA has no such provisions and requires retroactive consent)
- Office of the Information and Privacy Commissioner of BC has power to sanction and impose fines directly of up to \$100,000 for non-compliance (Privacy Commissioner of Canada must go through Federal Court)
- Consent provisions regarding sensitive PI (health and financial) under PIPEDA are “opt-in” where under PIPA there is a conditional form of implied consent
- PIPA has an exemption for the use and disclosure of employee and customer PI in the course of business transaction such as a merger, purchase, lease, amalgamation) without consent (PIPEDA has no such exemption)

Regulatory/Legislative Landscape

Europe

- E.U. Data Protection Directive and Act
 - Over-arching legislation for 25 member states
 - Stricter standards
 - Broad definition of data and data controller
 - Transfer of E.U. personal data to:
 - › *Canada*
 - › *U.S.*
 - Regulatory enforcement examples
 - Global participation of regulators
 - Review and amendments to E.U. data laws may make Canadian laws no longer deemed equivalent

U.S.

- Fragmented legislative framework
 - No primary federal statutes (although could change with three new laws proposed in 2014)
 - Variety of federal and state statutes apply
 - Historically pass subject specific laws
- Major statutes federal
 - Over 40 federal statutes with privacy provisions
 - Red flag rules imposed by FTC
 - Fair and Accurate Credit Transaction Act (FACTA)
 - HITECH Act: expands HIPAA data security requirements to business associates doing business with healthcare organizations

Canadian Breach Notification Laws

- PIPEDA NOW
 - When does the obligation to notify arise?
 - Failure to properly notify in timely fashion can lead to civil and regulatory liability
 - Early notification = mitigation
 - Canadian legislation has no mandatory breach notification obligations except for PHIPA (Ontario), Alberta PIPA (new health information acts in NS, NB, NL and MB's new PIPITPA)
 - Guidelines/protocols strongly urge to notify if breach creates a risk of significant harm
 - <http://www.ipc.on.ca/images/resources/priv-breach-e.pdf>
 - Breach notification requirements under BC PIPA are essentially the same as under PIPEDA
- PIPEDA Bill (private member Bill C-475)
 - Discretion left in hands of organization
 - Threshold to report is “a possible risk of significant harm” (lower standard than previous Bill C-12)
 - Reporting window is “as soon as reasonably possible”
 - Report “material breaches” to the privacy commissioner
 - Need to establish proper protocols and procedures
 - In Second Reading and debated in December 2013 before Parliament adjourned for the holidays

U.S. Breach Notification Laws

Clients/Prospects That Collect PI of U.S. Citizens

- 47 states have mandatory breach notification laws
- Each state's laws differ
 - Application
 - Definition of PI
 - Application to encrypted data
 - Electronic data and paper or just electronic data
 - Trigger threshold
 - Method of notification
 - Timing of notification
 - Obligation to notify government agencies
 - Private right of action
 - Regulatory penalties

Key Operation Privacy Issues

CSA Requirements

- Hundreds of organizations victimized by data breaches where valuable PI and corporate information was stolen/accessed with the following negative outcomes:
 - Public confidence erosion
 - Devaluation of IP
 - Loss of competitive advantage
 - Decreased business opportunities
 - Increased expenditures on data security
- Because these data breaches may have an adverse impact on an organization's financial performance failure to disclose such events promptly may lead to regulatory and civil liability
- In Canada, securities laws require the disclosure of events and uncertainties that are reasonably likely to materially affect the issuer's performance

Key Operation Privacy Issues

CSA Requirements

- This could include privacy risks if they are reasonably likely to have an indirect effect on the issuer's financial condition, results or operations that are material to investors
- Issuers that offer online payment services and that collect financial or health information are more likely to be within the subset of business that will have to consider these types of disclosures
- Therefore SEC cyber risk reporting guidelines released in October 2012
- Securities regulators are becoming more aggressive in dealing with cyber disclosure failures (33% of U.S. Fortune 500 companies make inadequate disclosures in filings)
- Target's Ds&Os recently sued (21 January 2014) in derivative class action over recent breach that led to a stock drop (allegations they did nothing to prevent breach when they knew security was inferior)

Key Operational Privacy Issues

Payment Card Industry Data Security Standards (PCI DSS)

- Standards established by contract for all businesses that accept credit card payments online and offline
- Standards are common set of industry tools and measurements to help ensure the safe handling of sensitive information (12 requirements)
- Amount of business volume will determine the specific compliance requirements
- Needs to be updated annually and vulnerabilities need to be addressed
- Credit card companies have compliance initiatives, including financial or operational consequences to certain business that are not PCI compliant
- Tracing the money and the issue of the holdback
- Distinction between damages, fines/penalties, chargebacks and holdbacks under PCI
- Compliance or near compliance is a strong insurance underwriting requirement

Key Operational Privacy Issues

OSFI Memorandum on Cyber Security Guidance/ Self Assessment

- Released 28 October 2013
- OSFI expects senior management of FRFIs to review cyber-risk management policies and practices to ensure that they remain appropriate and effective
- OSFI released a cyber security self-assessment guidance to assist FRFIs in their self-assessment activities
- FRFIs are encouraged to use this assessment tool to assess their current level of preparedness, and to develop and maintain effective cyber security practices
- The assessment tool template sets out the following six groups of desirable properties and characteristics that FRFIs must rank on a scale from 1 to 4 based on maturity:
 - Organization and resources
 - Cyber risk and control assessment
 - Situational awareness
 - Threat and vulnerability risk management
 - Cyber security incident management
 - Cyber security governance

Key Operational Privacy Issues

OSFI Memorandum on Cyber Security Guidance/ Self Assessment

- For each item that has not been fully implemented, the template encourages an FRFI to indicate an action plan and target date for full implementation.
- Although OSFI is not planning to establish specific guidance for the control and management of cyber risk it is a priority for 2013 – 2016 in its plans and priorities
- OSFI may request FRFIs to complete the assessment or otherwise emphasize cyber security practices during future supervisory assessments

Key Self-Examination Questions

What type of PI do you collect/store/use?

- Data elements (different definitions of PI in various statutes)
- Employee personal information (provincially protected only in BC/AB/QC/MB)
- Customer/client information (PIPEDA, PIPAs, PIPITPA or Québec Act)
- Personal health information (Governed in whole or in part by a specific act)

What type of organization do you have?

- Federally or provincially regulated (FWUB such as transportation, banking subject to PIPEDA)
- Commercial activity (PIPA only applies to NPOs engaged in commercial activities)
- Government/municipal (FOIP Act)

Key Self-Examination Questions

Where are you located and how does your PI flow?

- Within or outside of province, country (trans-border application of laws, Principle 4.3 compliance)

Does your privacy adequately deal with compliance in all the jurisdictions you operate and does it align with your actual management practices?

- Prudent to compare aspects of all legislation to determine most stringent provisions

Do you do any of the following?

- Encrypt your data (partially, if not fully)
- Allow your employees to work remotely (i.e. at home, on mobile devices on business trips)
- Create, implement and enforce remote working policies and BYOD policies
- Utilize BYOD software
- Provide onboard and ongoing employee training
- Audit and assess privacy policy/procedure against own policies and peers
- Stress test and vulnerability scan IT security
- Employ sanitization software to cleanse equipment in sale and end-of-lease situations

Key Self-Examination Questions

Do you outsource any part of computer network operations to third parties and or contractors to manage your data in any way?

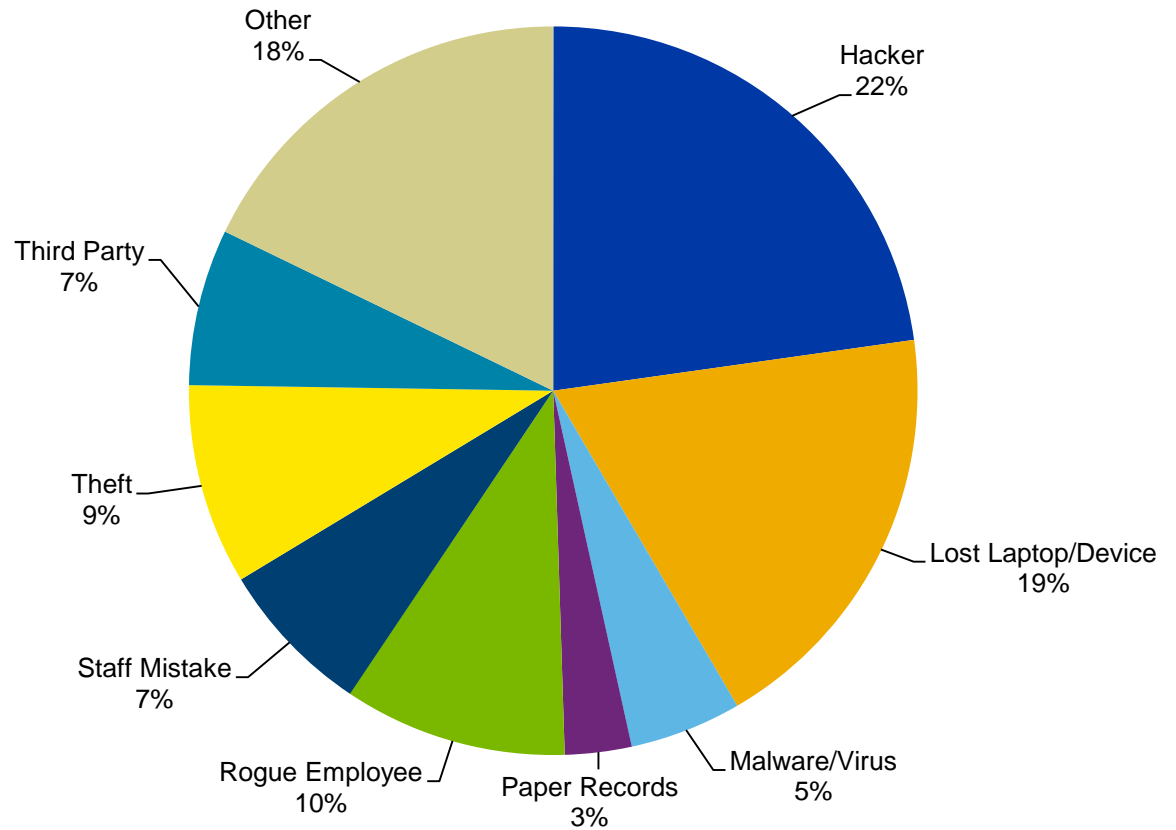
- Your security is only as good as theirs (audit their practices)
- You are still responsible for your customers/employees data
- PIPEDA contractual protections
- U.S. service providers/Patriot Act
- Check their insurance

Do you partner with entities and does this alliance involve the sharing/handling of their data?

- You may be liable for a future breach affecting your business partners

Types of Privacy Breaches

Cause of Publicly Reported Breaches



Cost of a Loss

Third Party Liability

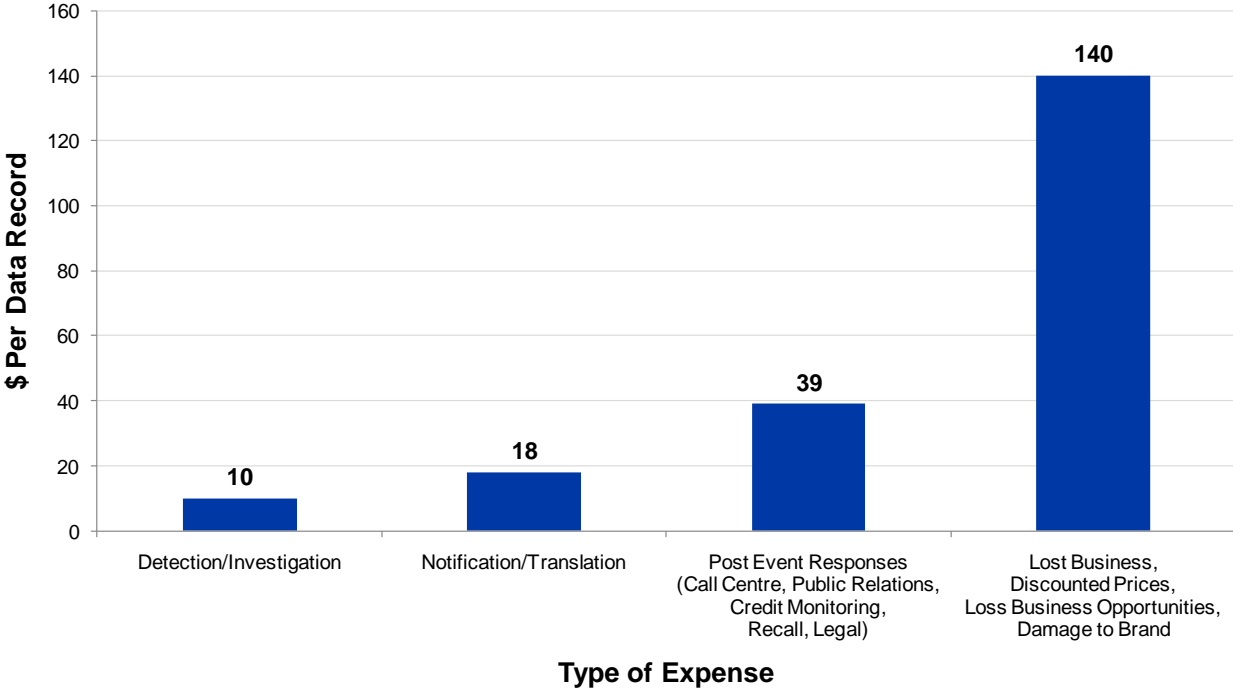
- Civil suits
 - From business partners (i.e. financial institutions for credit card notification and recall expenses)
 - Class actions (list on slide 27)
 - From the general public for identity theft (Jones case)
 - From employees
 - Compensatory damages
 - Legal fees
- Regulatory investigations and proceedings
 - From privacy commissioners
 - Fines, penalties and civil awards
 - Costs to comply with orders

Cost of a Loss

First Party Costs

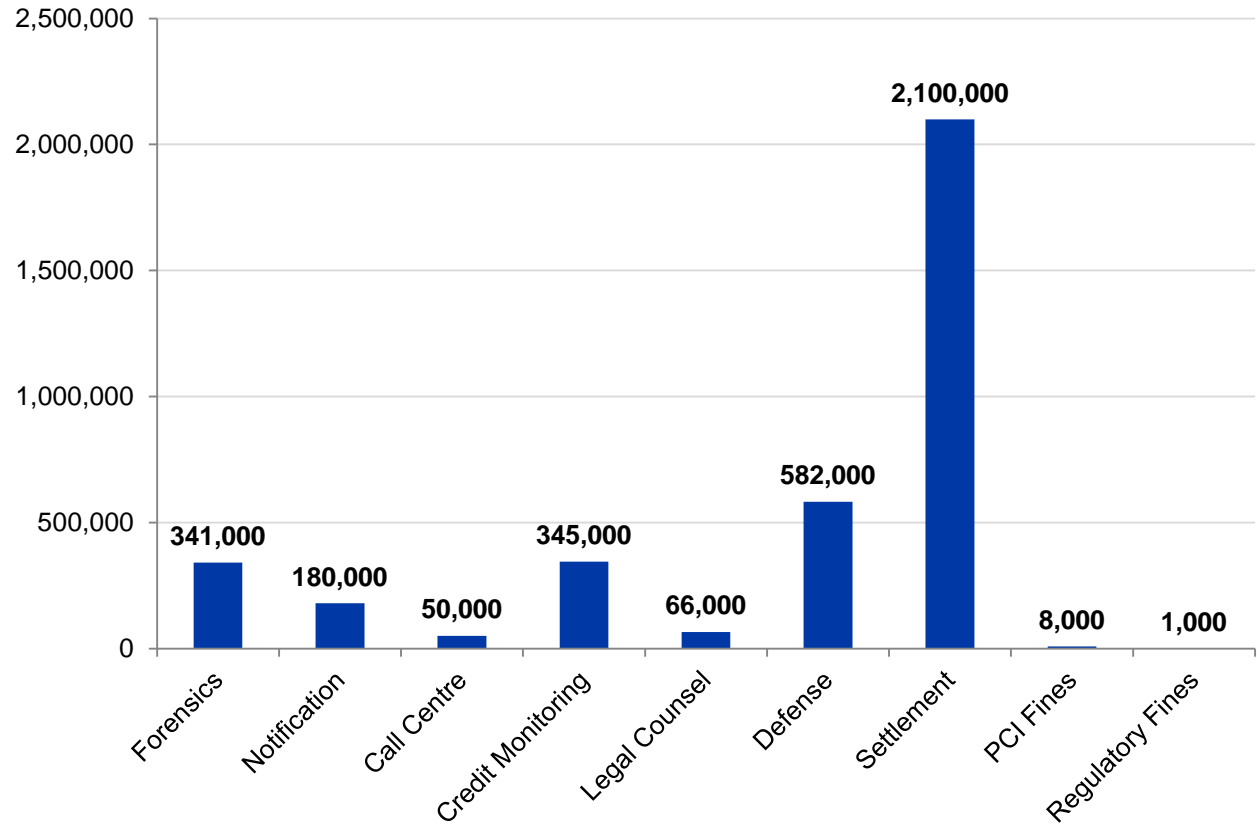
- Organization's out-of-pocket costs
 - Damage to data and property
 - Recovery and restoration expenses
 - Loss of intellectual property
 - Business interruption
 - Internal investigation
 - Lost employee productivity
 - Notification expenses
 - Interaction with regulators
 - Call centre expenses
 - Website maintenance
 - Credit monitoring
 - Public relations
- Damage to reputation
 - Bad press
 - Loss of confidence
 - Damage to brand
 - Loss of business opportunity
 - Future revenues due to lost customers/clients
 - Damaged business relationships

Costs of a Data Breach Per Data Record



Overall Average Cost per Breach

First/Third Party Liability



Recent Canadian Class Action Lawsuits

- Sony (certification pending)
 - Database stolen
 - 77 million PI records compromised
 - Combined \$1B class action in multiple countries including Canada
- IIROC (certification pending)
 - Unencrypted mobile device lost
 - 52,000 brokerage industry clients' records at risk
 - \$52M class action
- Minister of Human Resources and Skills Development (certification pending)
 - Lost portable unencrypted hard drive
 - Data on 583,000 student loans at risk
 - Amounts to be determined
- Google (certification pending)
 - Interception and illegal use of customer PI
 - All Google users affected
 - \$500 per email claims as damages (could be billions)



Recent Canadian Class Action Lawsuits

- Apple (certification pending)
 - Violation of users' rights by allowing apps to transmit private data to advertisers
 - Apple customers
 - Multiple heads of damage including punitive, injunction and compensatory
- Durham Region of Health
 - Loss of unencrypted USB key
 - 83,500 individual health records concerning H1N1 immunization
 - \$40M class action
 - Case settled \$500K legal costs, but amounts to claimants is still outstanding
- Peoples Trust (certification pending)
 - Online application database containing PI was compromised by hack from China
 - 12,000 – 13,000 individuals potentially affected
 - Notification costs already substantial
 - \$13M sought in class action
- Health Canada (certification pending)
 - 40,000 letters went out labeled "Medical Marihuana Program" as the return address



Insurance Under Traditional Policies

- **Commercial general liability policy**
 - Bodily injury/property damage trigger limits applicability
 - Advertising and personal injury provisions may not apply to lost data
- **Property policy**
 - Coverage limited to damage to tangible property
- **Professional and media liability policy**
 - Coverage limited to economic damage arising from negligence in providing professional services
 - Media liability coverage must be very broad to account for privacy breach exposures
- **Commercial crime/fidelity policy**
 - Limited to employee theft of tangible property and computer fraud
 - No third party liability coverage
- **Kidnap, ransom and extortion policy**
 - Limited to extortion threats with ransom demands
- **Directors' and officers' policy**
 - Limited to wrongful acts of directors/officers
 - Bodily injury and property damage, intentional acts excluded

Specialized Insurance

- **State of the market**
 - Many new market entrants and forms
 - Competition is increasing
 - Forms can be very different in structure and approach which makes comparisons challenging
- **Carriers**
 - Chubb
 - AIG
 - ACE
 - Zurich
 - Liberty
 - Travelers
 - London markets
 - Ironshore
 - Everest
- **Capacity and limits**
 - Primary limits available in the \$1M – \$10M range
 - Multi-layer programs can be written
 - Limited loss history and diverse underwriting variables makes benchmarking challenging

Hot Button Policy Issues

- Coverage trigger
- Scope of data
- Breach notification trigger
- Insider acts coverage
- Employee claims
- Off-site breaches/BYOD
- Cloud computing
- Regulatory proceedings coverage
- Fines and penalties
- PCI fines, charges and holdbacks
- Independent contractors' coverage
- Event management coverage
- Business interruption coverage including contingent BI
- Loss of corporate information
- State-sponsored attack coverage





Aon Policy Initiatives


- Chartis Specialty Risk Protector Aon Amendatory Endorsement
- Chubb Cyber Security Aon Amendatory Endorsement
- ACE Privacy Protection (negotiating Aon Amendatory Endorsement)
- Zurich Security and Privacy Protection (negotiating Aon Amendatory Endorsement)
- Travelers CyberRisk (negotiating Aon Amendatory Endorsement)
- Liberty Cyber Suite (will be negotiating Aon Amendatory Endorsement)

Aon Tools and Resources

- Aon's Cyber and Privacy Practice (ACAPP)
 - Coverage audits and customization of policy wordings
- Resources available in addition to insurance transfer
 - Aon's Online Cyber Risk Diagnostic Tool (free ask your Aon representative for details)
 - CERQ
 - CGI

 / Cyber Risk Diagnostic Tool






Aon has created this simple-to-use, interactive tool to help you identify and consider the key internal and external factors that may affect your levels of cyber risks. The tool will provide you with meaningful insight into the most important key cyber risk topics and includes practical guidance on the related governance framework that should be in place as part of an effective cyber risk management strategy. For specific tailored advice and/or product recommendation, please reach out to your local Aon office.

The results of this tool

- ✓ You will receive a report highlighting key cyber risk issues in your company as well as insight into best practices
- ✓ The report includes a visual indication and high level rating for your identified cyber risks

[Start your diagnosis ▶](#)

10 minutes to complete



Questions?



Brian Rosenbaum LL.B
National Director
Aon Risk Solutions™
Financial Services Group
Legal and Research Practice
Tel: 416.868.2411
Email: brian.rosenbaum@aon.ca

AON