

Cyber Risks and Management: From Policy to Practice

A Presentation to the BC Hotel Association
September 22, 2026

Drew Woytko, Director, Business Development,
Western Financial Group
Mercy Iannicello, Partner & National Chair of Cyber & Privacy Liability
Group
Dolden LLP

National Firm



Canada's Specialty Insurance Law Firm

VANCOUVER | KELOWNA | CALGARY | GUELPH | TORONTO | HALIFAX



BRITISH COLUMBIA
HOTEL ASSOCIATION



Western
FINANCIAL GROUP
Canada's Insurance Broker

Affiliated with

RSS • avocats
Insurance Law Group lawyers

MONTREAL

Dolden's Privacy Team



- 10 lawyers nationally, including 1 licensed to practice in Québec
- Act as breach coach on a variety of claims across Canada, including ransomware, business email compromise, social engineering, theft, etc.
- Report and negotiate with federal and provincial regulators
- Provide cyber coverage advice to insurers
- Defend and act as monitoring counsel on cyber class actions
- Designated Net Diligence Authorized Breach Coach®

Agenda

1. Cyber Policies
 - First and Third Party Coverages
2. Considerations for Third Party Contracts
3. What is a Privacy Breach?
4. BC PIPA requirements
5. Common Risks
6. Ransomware example

Question #1

Do you currently carry a cyber liability insurance policy for your hotel?

- a. Yes
- b. No
- c. Not sure

Question #2

Do you have a written incident response plan if you sustained a breach tomorrow?

- a. Yes
- b. No
- c. What's that mean?

Question #3

What would be a moderate cyber incident response cost a hotel?

- a. \$50,000
- b. \$150,000-\$200,000
- c. Over \$500,000

Cyber Policies

- Designed to address privacy and security breaches
- Expanded to address cyber crime
- Claims Made and Reported Coverage
 - Applies only to claims that are first made and reported (or breaches first discovered) during the policy period

First & Third Party Cyber Coverage

• First Party

Purpose:

- Indemnifies an Insured for its own direct loss arising from a privacy breach or security breach
- Typically covers costs to resolve breach from start to finish

Third Party

Purpose:

- Indemnifies Insured for defence costs & damages insured becomes legally obligated to pay b/c of claim against insured arising from privacy breach, security breach, technology wrongful act, or media liability
- “Open ended” grants of coverage, not limited to specific statutory and common law remedies

Hospitality Insurance Program Coverages

Coverage	Tier 1 Included	Tier 2	Tier 3
Business Interruption	\$250,000	\$1,000,000	\$2,000,000
Digital Asset Destruction	\$250,000	\$1,000,000	\$2,000,000
Incident Response Expense	\$250,000	\$1,000,000	\$2,000,000
Cyber Extortion/Ransomware	\$50,000	\$1,000,000	\$2,000,000
Regulatory Defense and Penalties	\$250,000	\$1,000,000	\$2,000,000
Payment Card Industry Fines and Expenses	\$250,000	\$1,000,000	\$2,000,000
Security and Privacy Liability	\$250,000	\$1,000,000	\$2,000,000
Multimedia Liability	\$250,000	\$1,000,000	\$2,000,000
Aggregate	\$1,000,000	\$2,000,000	\$3,000,000
Social Engineering – NEW	\$10,000	\$10,000	\$10,000
Optional Endorsements Available			
Bricking	Not Available	\$1,000,000	\$2,000,000
Reputational Harm	Not Available	\$1,000,000	\$2,000,000

Third Party Agreements

Things to consider:

1. **Define the data:** Is it PII? Is it confidential information?
2. **Define the purpose** the vendor may use it for
3. Ensure **consent** to use the data for other purposes is obtained
4. Require **security safeguards**
5. **Notification** and **timeline** in the event of a privacy or cyber incident
6. **Data retention and deletion; data control**

What is a Privacy Breach?

- When personal information is collected, retained, used or disclosed in a way that is not in accordance with legislation.
- What is personal information?



Canadian Privacy Legislation

- Federal legislation: PIPEDA
- BC PIPA
- Alberta PIPA
- Quebec also has its own legislation

Federal Breach Notification

When:	• Mandatory if there is a “real risk of significant harm” (low hurdle)
How:	• Direct notification (mail, email, phone) or indirect where direct is not possible
How Soon:	• “as soon as feasible”
To Whom:	• Privacy commissioner(s) • Affected individuals • Authorities and organizations who may assist with mitigating the harm • Professional and other regulatory bodies

Common Cyber and Privacy Risks

- Employee Misconduct & Error
- Business Email Compromise
- Wire Fraud & Social Engineering Fraud
- Ransomware

Role of Breach Coach: “Quarterback” the Response

- Crisis Management
- Coordinate Response
- Investigate the circumstances around the breach
- Provide Legal advice on obligations under legislation
- Report & negotiate with regulators
- Minimize potential harm & liability

What happens when a cyber breach occurs?

Spotlight: Ransomware Example

Hotel X, with an annual revenue of \$25 million, discovers their entire computer systems, including all servers, have had malware installed. Hotel X cannot get back into its systems, and company operations have come to a halt.

The well-known group, Akira, leaves behind a ransom note telling Hotel X that Akira has accessed their network and exfiltrated sensitive data related to their employees, vendors and customers. Akira makes a demand for \$10 million. Payment is required within 48 hours, or Akira has threatened to publish the data on their leak site.

What now?!

- Report the Breach immediately to insurer/broker or hotline
- Get Breach Coach involved immediately
 - Investigate the circumstances around the breach
 - Coordinate Response

Forensics: The What? When? and How?

- Scoping Call
- Ransom Negotiation
- Containment
- Investigation
- Restoration

Notification

Notification and Negotiation:

- BC PIPA is slightly different
- Legal and regulatory compliance, law enforcement, public/client relations
 - Privacy Commissioner(s)
 - Law Enforcement
 - Affected individuals, clients and business partners

Costs and Ransomware Considerations

Average costs to respond to “modest” cyber incident:
\$150k-\$200k+

Forensic Investigation:	\$50,000-\$150,000
Threat Negotiation:	\$10,000
Credit Monitoring & ID Theft Expenses:	\$12/person for 1year
Crisis Management/PR	\$10,000
Breach coach/legal	\$20,000-\$30,000

Any BI loss?

Repair/Restoration/Replacement Costs?

Risk Management Strategies

- Pre-breach Plan
 - Breach Counsel
 - Incident Response Plan
- Security Posture
- Data retention and deletion Policies
- Employee Training

Dolden

Questions?



Canada's Specialty Insurance Law Firm

VANCOUVER | KELOWNA | CALGARY | GUELPH | TORONTO | HALIFAX



BRITISH COLUMBIA
HOTEL ASSOCIATION



Western
FINANCIAL GROUP
Canada's Insurance Broker

Affiliated with

RSS • avocats
lawyers
Insurance Law Group

MONTREAL