AON

ALIA Universal Cyber Coverage Webinar

ALBERTA LAWYERS INDEMNITY ASSOCIATION

Welcome message

ALBERTA LAWYERS INDEMNITY ASSOCIATION

David Weyant, K.C.

President and CEO

Alberta Lawyers Indemnity Association

AON

An Introduction to the Team

Presented By:

Katie Andruchow, AON,
National Cyber Broking Practice Leader

Alex Juneau, ZURICH,
Cyber Underwriting Specialist

Maud-Julie Audit, ZURICH,
Senior Claims Counsel

Agenda

1

Cyber Threat landscape

- By the Numbers
- Ransomware Trends
- Cyber Insurance Market
- Benefits of the Universal Program

2

ALIA Universal Cyber Program

- Overview of Limits & Coverage
- Loss Examples
- Uncovered Matters

3

Claim Process and Vendor Panel

- How to report a Claim
- When to report a Claim
- Zurich Vendor Panel

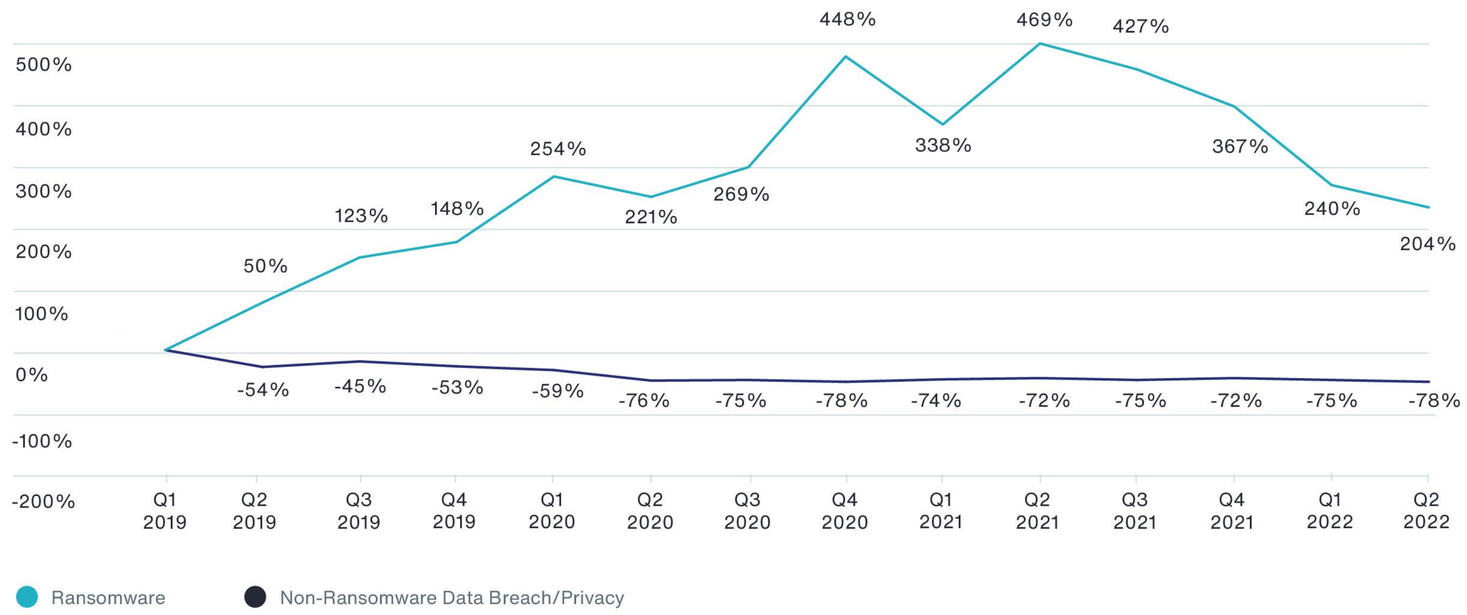
The Cyber Threat Landscape

AON

Loss Trends

Frequency and severity for errors and omissions and media liability claims remained rather constant through the first half of 2022. By contrast, Aon data shows cyber claims frequency declined quarter-over-quarter, driving favorable adjustments loss ratios through the first half of 2022.

Cyber Incident Rates Over the Past Thirteen Quarters



Source: Risk Based Security, analysis by Aon. Data as of July 12, 2022; Ransomware data exfiltration per Coveware Quareterly Ransomware Report as of May 3, 2022.

Key Observations:

- Ransomware activity has continued to **outpaced Non-Ransomware Data Breach/Privacy Event activity.**
- **Ransomware up 204%** from Q1 2019 to Q2 2022
- Compared to Q1 2022:
  - **Ransomware down 10%**
  - **Non-Ransomware Data Breach/Privacy down 13%**
- Similar to Q1, the most commonly impacted industries by Ransomware in Q2 2022 were:
  - Public Sector
  - Manufacturing
  - Healthcare
  - Business & Professional Services
- Data exfiltration occurred in 77% of ransomware cases per Coveware in Q1 2022.

Network Security & Privacy – State of the Market 2021-22

Claims and losses

Claims data is being analyzed as more breaches are being reported and remediated.

- Complexity of breaches has driven an increase in incident response expenses incurred by insureds.
- Increasingly punitive legal and regulatory environment.
- There has been a significant increase in frequency and severity of ransomware claims with some carriers reporting nearly 500% increase in ransomware claims. Currently this is the number one cause of the hardening of the cyber market.
- A recent vulnerability discovered relating to SolarWinds Orion Platform software has potential to be a systemic loss significantly impacting the global cyber insurance market.

Coverage

Insurers are evolving their policy wordings in light of claims experience to protect cyber portfolio profitability

- Coverage is starting to decrease as carriers being to implement sublimits to reduce amounts paid out following a ransomware incident. Coinsurance is also being imposed by some carriers all in an effort to help manage their exposure to ransomware loss.
- Exclusionary language to protect carriers from the impact of SolarWinds is also being explored.
- Insurers are differentiating their offering with prebreach risk management services and online information portals.
- Emphasis on pre-arranged claims response vendors, with some insurers stipulating use of their own vendors in order to control cost.

Capacity

Insurers are reviewing their capacity deployed, new entrants and exits common.

- Capacity is available globally: domestic, London, and Bermuda.
- Decreases in capacity may be seen where insured risk control metrics are subpar or insured participates in a high-risk industry sector.
- The impact of work from home and enhancements made by insurers to improve/elevate insured's cybersecurity measures are being reviewed and may affect deployment of capacity.
- Maximum capacity for primary placements is now capped at 5M. Excess capacity is required to access additional limits.

Retentions

Retentions are being reviewed.

- Retention can vary greatly based on industry class, size and unique exposures.
- Insurers are using retentions as a tool to manage claims experience and portfolio profitability.
- Minimum retentions are being set by insurers on a portfolio basis that are dependent on revenue bands and industry classes.
- Generally speaking, retentions tend to be increasing.

Pricing

The cyber market is hardening. We expect rates to continue to increase into the foreseeable future.

- Insurer's profitability has been materially impacted by the uptick in frequency and severity of ransomware incidents, as well as the recent SolarWinds vulnerability.
- Premiums are increasing, degree depends on industry, claims history and cyber risk posture.
- Required rate on lines continue to increase for excess layers.

Note: This is a general summary and could vary based on client industry and size.

AON

Key Areas of Underwriting Focus, Aon's Recommendations

Key Areas of Underwriting Focus

Multi-Factor Authentication (MFA)	Endpoint Protection and Response (EDR)	Phishing Exercise/Cyber Awareness Training
Patch Management	Secure RDP/VPN	Incident Response Plan
Previous Incidents and Containment	Disaster Recovery/ Backups	Email Filtering

Aon's List of Critical Network Security Controls

1. Multi-factor authentication (MFA) for:
   Email, privileged accounts, all remote access
2. Security & phishing awareness training
3. Regularly Conducted Assessments
4. Properly configured URL filtering and email attachment sandboxing
5. Advanced endpoint detection and response (EDR) solution
6. 24/7 Managed SOC (Security Operations Centre)
7. Advanced malware detection tool that inspects network traffic
8. 16+ character service account and domain admin passwords
9. Lateral Movement Detection Tools
10. Properly configured security information and event management (SIEM) platform
11. Continuous security monitoring function
12. Business Resilience
13. Disabling accessibility of remote desktop directly from Internet

AON

© 2022 Aon Reed Stenhouse Inc.

ALIA Universal Cyber Program

- Coverage is available to all Subscribers and firms regardless of control profile and loss history
- Broad terms and conditions on a market competitive wording, coverage is inclusive of ransomware loss events
- Tried and tested claims response and vendor panel for all to access

AON

ALIA Cyber Program Coverage Overview

AON

ALIA Universal Cyber Program Overview

Liability Claim Costs

	Deductible
$250,000 each Claim / $250,000 Aggregate each Law Firm **For Coverage 1. Security Liability Coverage**	$5,000
$250,000 each Claim / $250,000 Aggregate each Law Firm **For Coverage 2. Privacy Liability Coverage**	$5,000
$250,000 each Claim / $250,000 Aggregate each Law Firm **For Coverage 4. Regulatory Proceedings**	$5,000

ALIA Universal Cyber Program Overview

First Party Response Costs

	Deductible
$35,000 each Claim / $35,000 Aggregate each Law Firm **For Coverage B Breach Cost coverages, Cyber Extortion Coverage**	$5,000

Maximum amount claimable per firm in a policy period is $285,000

ALIA Universal Cyber Coverages Overview

| Privacy and Network Security Risk

Risk

Overview

- **Privacy and Network Security Liability**
  - **Privacy Liability:** Liability coverage for certain defence costs and damages suffered by others for any failure to protect personally identifiable or confidential third-party corporate information, whether or not due to a failure of network security. Coverage may include: unintentional violations of the insured's privacy policy, actions of rogue employees, and alleged wrongful collection of confidential information.
  - **Security Liability:** Liability coverage for certain defence costs and damages suffered by others resulting from a failure of computer security, including liability caused by theft or disclosure of confidential information, unauthorized access, unauthorized use, denial of service attack or transmission of a computer virus.

- **Regulatory Proceedings -** Liability coverage for certain defence costs for proceedings brought by a governmental agency in connection with a failure to protect private information and/or a failure of network security. Coverage includes certain fines and penalties where insurable by law. Compensatory damages, i.e. amounts the insured is required by a regulator to deposit into a consumer redress fund, may be covered

All descriptions, summaries or highlights of coverage are for general informational purposes only and do not amend, alter or modify the actual terms or conditions of any insurance policy. Coverage is governed only by the terms and conditions of the relevant policy.

AON

Liability Loss Examples

Description of Loss - Ransomware

The Insured was the victim of a cyber attack involving internal data. Insured was the victim of a ransomware attack from a Russian group, encrypting multiple servers and workstation.

The ransom was paid, a receipt was received detailing the data that was at risk and the encryption key. The data at risk included hundreds of records of insured employees and ex-employee personal information.

The law firm retained an IT forensic firm (a cyber security firm)

The consequences of the breach included a class action involving the employees suing the insured.

Coverage applicable under the ALIA Program:

250,000 liability limit after $5,000 retention is eroded

35,000 first party limits

AON

ALIA Universal Cyber Coverages Overview

| First Party Exposure

Risk

Overview

- **Breach Event Expenses -** Reimbursement coverage for certain of the insured's costs to respond to a data privacy or security incident. **Covered expenses include certain computer forensics expenses, legal expenses, costs for a public relations firm and related advertising to restore your reputation, consumer notification, call centers, and consumer credit monitoring services**

- **Cyber Extortion** - Reimbursement coverage for the insured for expenses incurred in the investigation of a threat and any extortion payments made to prevent or resolve the threat.

All descriptions, summaries or highlights of coverage are for general informational purposes only and do not amend, alter or modify the actual terms or conditions of any insurance policy. Coverage is governed only by the terms and conditions of the relevant policy.

AON

First Party Loss Examples

Description of Loss - Insider Threat

After a nursing home employee resigned, the home discovered that she had emailed herself patient records. The nursing home reported the event to their insurer who put them in touch with privacy counsel.

Upon investigation and interviewing the former employee, counsel helped the home determine that notification was not necessary as the files were never used and had been deleted.

Coverage applicable under the ALIA Program:

$35,000 first party limit after $5,000 retention is eroded

AON

First Party Loss Examples

Description of Loss - Insider Threat

A hospital employee was stealing patient information and selling to a local crime ring to file fraudulent tax returns. The hospital was advised of this by law enforcement and began an investigation.

115,000 patient records were affected, containing SIN, DOB, address and treatment information. The hospital used forensics, legal, main and call center, credit monitoring and crisis management services under their insurance policy.

Coverage applicable under the ALIA Program:

$35,000 first party limit after $5,000 retention is eroded

AON

First Party Loss Examples

Description of Loss - Stolen Device

An incident at a company arose when a laptop was stolen from a vehicle being used by the insured's HR manager. The laptop was unencrypted and held files containing employee information, such as name, address, SIN and salary information for all the insured's employees from 2004-08.

Forensics and privacy counsel were engaged and determined the insured was obligated to notify and provide credit monitoring to 36,000 individuals

Coverage applicable under the ALIA Program:

$35,000 first party limit after $5,000 retention is eroded

AON

First Party Loss Examples

Description of Loss - Stolen Devices

Thirty server hard drives and 10 desktop computers were stolen overnight from a law firm. Data included information regarding law firm employees and clients. Medical records regarding clients may have also been compromised as well as thousands of pages of other documents stored on the devices.

The insurer assisted and connected the firm to privacy counsel and forensics. With their guidance the insured ultimately notified 150 employees whose data was compromised and 25 external clients. The affected individuals were also offered credit monitoring as their social security numbers were involved.

Coverage applicable under the ALIA Program:

$35,000 first party limit after $5,000 retention is eroded

AON

First Party Loss Examples

Description of Loss - Ransomware

The insured reported two separate cyber-attack events, both dates of each event were documented, within two months of each other.

The first attack targeted the insured's production software. Insured conducted an investigation through its IT company, according to the IT company, the hackers would have infiltrated through an email link. The insured did not pay the initial ransom of $50k and believed the problem had been solved.

The second attack occurred overnight. This attack targeted the director's computer. Another ransom request for $50k was received from the same hackers. A cyber-security firm was then retained to investigate and remediate the breach.

Total Cost of Loss:

$72,113 for IT forensics and termination costs

Coverage applicable under the ALIA Program:

$35,000 first party limit after $5,000 retention is eroded

AON

First Party Loss Examples

Description of Loss - Ransomware

The insured was notified from an internal source that an application hosted in cloud platform was not running. An employee logged in, discovering data on the server was encrypted, an HTML ransom note was left.

After high-level assessment following the breach, all servers were shut down, all admin passwords reset, and non-essential service accounts disabled. Relevant parties were notified of the breach, and no evidence that the attack extended into the insured's main network.

The server that was impacted contained records of personal information. The investigative company concluded in their report: no evidence of confidential data access, nor data exfiltration were found. The insured was invoiced for the work of the investigative company.

Total Cost of Loss:

$83,734.88 cost of loss to date

Coverage applicable under the ALIA Program:

$35,000 first party limit after $5,000 retention is eroded

AON

Cyber Coverage OUTSIDE Scope of the ALIA Program

| Miscellaneous Cyber Insurance Coverages

Coverage

Overview

- **Digital Asset Restoration -** Reimbursement coverage for the insured for costs incurred to restore, recollect, or recreate intangible, non-physical assets (software or data) that are corrupted, destroyed or deleted due to a network security failure.
- **Network Business Interruption -** Reimbursement coverage for the insured for lost net income caused by a network security failure, as well as associated extra expense. Retention and waiting periods apply prior to loss reimbursement.
- **Dependent Business Interruption -** Reimbursement coverage for the insured for lost income caused by a network security failure of a business on which the insured is dependent, as well as associated extra expense. Retention and waiting periods apply prior to loss reimbursement.

All descriptions, summaries or highlights of coverage are for general informational purposes only and do not amend, alter or modify the actual terms or conditions of any insurance policy. Coverage is governed only by the terms and conditions of the relevant policy.

AON

The Claim Process & Zurich Vendor Panel

AON

How to Report a Claim

Urgent crisis management and/or reporting of a claim/ circumstance

If urgent crisis management or legal advice is needed following a cyber attack: Please contact the designated incident response breach coach: **Designated Breach coach** **Imran Ahmad** 1-866 -BREACHX / 1-866-273-2249 nrfc.breach@nortonrosefulbright.com This contact information is toll-free and available to access 24 hours 7 days a week.	To provide formal notice of a claim or a circumstance to the insurer: Send claim details to: **Notification Email**: Claims@zurich.com Phone: 1-866-345-3454; Fax: 1-877-977-8077 Zurich Insurance Company Ltd First Canadian Place, 100 King Street West Suite 5500, P.O. Box 290 Toronto, ON M5X 1C9

Zurich Vendor Panel & Benefits

Zurich has a list of preferred vendors, which includes:

- IT Forensics firms
- Ransom negotiators
- Public relations firms
- Credit monitoring firms/call centers
- Defence counsels

Benefits include:

- Vendors are all experts in their fields
- Access to better rates

Cyber Claims Process

STEP 1: NOTIFY ZURICH

STEP 2: FIRST CONTACT

STEP 3: DETERMINE WHO NEEDS TO GET INVOLVED

STEP 4: ONGOING COMMUNICATION

STEP 5: SUBMIT THE PROOF OF LOSS

STEP 6: FINALIZATION

AON

Questions and FAQ

[Cyber Coverage FAQs – ALIA's webpage on the Law Society of Alberta Website]

[ALIACyber@aon.ca]

FAQ

What if a Subscriber and their Law Firm has a cyber policy?

- The Universal Cyber Policy will be EXCESS with regards to any standalone Cyber policy placed for a firm

- The Universal Cyber Policy is intended to provide a baseline level of coverage and provide a linkage to breach response vendors for all firms. There may be firms who wish to pursue additional coverage over and above this offering, or have custom needs as it relates to cyber they wish to address

- The Universal Cyber Policy is intended to be PRIMARY with regards to:
  - Property and Casualty policies and any cyber extensions that might be found under these programs

AON

FAQ

In a loss scenario can I utilize my own vendor for incident response?

- All incident response work should be done by firms on the vendor panel established by Zurich

- If there are conflicts of interest or unique needs to procure work outside the panel, this will be assessed on a case-by-case basis either during the claim consultation process or in advance of a loss by contacting ALIAcyber@aon.ca

AON

Thank You!