clia
[CANADIAN LAWYERS INSURANCE ASSOCIATION]

Understanding Your Insurance Coverage

Dave Jackson - CEO

Agenda

- What is CLIA
- Mandatory Errors & Omissions Coverage
- Excess Insurance
- Cyber Insurance
- Claims-based vs. Occurrence-based
- Insurance Coverage for Retirees
- Cyber Insurance
- Reporting a Claim

What is CLIA

CLIA:

- Is an insurance reciprocal created by the legal profession in Canada in 1988 to ensure access to stable insurance
- Is a not-for-profit organization that provides insurance products to nine **volunteer members** made up of six provinces and three territories
- Assists Law Societies fulfill their public protection mandate
- Administers the insurance reciprocal and assists with the management of claims
- Markets and manages excess insurance layer
- Develops insurance programs for CLIA Subscribers

What is a Reciprocal

- Reciprocals are “non-entities” for tax purposes
- Therefore, no tax on income (i.e. investment income/underwriting income etc.)
- Premiums subject to PST/HST where applicable – paid by insureds
- Premiums subject to premium tax –paid by insurers
- Must follow OSFI rules and is regulated by the Superintendent of Insurance in jurisdiction where office is located.

CLIA Insurance Products

- Mandatory Errors and Omissions coverage
- Excess Errors and Omissions coverage
- Defalcation – Compensation Fund coverage
- Mandatory cyber crime coverage
- Stand Alone excess cyber crime coverage

Mandatory Errors & Omissions

(Purchased at the Lawyer Level)

- Covers errors/omissions in the rendering of professional services to others
- Law Society Rules require lawyers to be insured
- Limits provided are $1 million per claim and $2 million in the aggregate (for all claims in the policy year)
- Individual lawyer responsible for deductible ($5,000 for first claim)
- CLIA responsible for the management of the claim up to $1 million

CLIA Excess Coverage

(Purchased at the firm level)

- VEP is 100% reinsured to commercial insurance markets
- Provides a variety of limits up to $34 million
- Policy period –July 1st to June 30th
- Rates driven by global reinsurance markets
- VEP is a follow form policy to the mandatory insurance

Cyber Coverage

- CLIA administers a **Mandatory Cyber insurance** program:
  - Purchased by each CLIA Subscribing Law Society
  - Provides coverage for their members who were required to be insured by mandatory lawyers' professional liability insurance at the time of Discovery.

- CLIA also provides an optional, enhanced **Stand-alone Cyber** insurance
  - Can augment your protection
  - Provide your firm with robust coverage for it's potential expenses and lost revenues in the event of a breach or attack.

Cyber Coverage

The following table outlines the Mandatory Cyber and optional Stand-Alone Cyber Coverages:

Coverage	Mandatory Cyber (deductible $5,000)	Stand-Alone Cyber	
		Base Coverage	Extension*
Network Security & Privacy Liability	$250,000	$1M or $2M	N/A
Data Recovery and Loss of Business Income	$100,000	$1M or $2M	N/A
Event Management Expenses	$100,000	$1M or $2M	N/A
Data Extortion (Including Ransomware)	$100,000	$1M or $2M	N/A
Bricking	$100,000	$250,000	N/A
Electronic Theft, Computer Fraud & Telecommunications Fraud*	N/A	N/A	$100,000 or $250,000
Social Engineering Fraud*	N/A	N/A	$100,000 or $250,000
Multimedia & Intellectual Property Liability	N/A	$1M or $2M	N/A
Reputational Damage	N/A	$1M or $2M	N/A
Dependent Network Interruption & Recovery	$100,000	$1M or $2M	N/A
Deductible	$5,000	$5,000	

** These coverage extensions are available for an additional premium and are purchased in conjunction with Stand Alone Cyber.*

Mandatory Cyber Eligibility Requirements

Good data, computer and network hygiene is critical for any business. The following minimum standards are necessary for coverage respond:

Eligibility Requirement	Why its Required	Helpers for Lawyers
Backup Controls: Weekly backups of data, stored offsite, and tested at least annually.	Backups ensure that your organization can be restored after a ransomware attack. It is important that one set of regular backups is kept completely disconnected from your organization's network.	Backing up data is a minimum IT "hygiene" requirement. If a lawyer/law firm is unsure if they back their data up, they should reach out to an IT provider. Most IT providers should be able to assist in setting up data backups. Ridge Canada recommends **inCyber** for assistance on a fixed fee consultation.
Patching: Application of critical patches to your systems, anti-virus software, and anti-spyware software must be made within two weeks of release.	Patching repairs any vulnerabilities that are discovered in your systems and software over time.	There are multiple patch management software applications that IT or security teams can leverage, and in many cases, this is as simple as turning on an automatic update feature.
Anti-Virus/Firewalls: Installation and maintenance, and active monitoring within reasonable business practices, of firewalls and endpoint protection (also known as anti-virus and anti-spyware)	Firewalls and endpoint protection help to prevent unwanted access to IT systems.	A firewall is typically a part of the hardware provided by the internet company you use. End point protection (such as antivirus software) including the free Windows Defender software included with Windows is typically automatically installed or can easily be installed on the firm's systems/computer to protect them from intruders and viruses. Lawyers/law firms should ensure these are turned on and in place.

Mandatory Cyber Eligibility Requirements

Eligibility Requirement	Why its Required	Helpers for Lawyers
Multifactor Authentication (MFA): MFA is an authentication method that requires the user to provide two or more verification factors to gain access. MFA must be enabled on email accounts and for remote network access (also known as VPN or Virtual Private Networking, or remote desktop access).	Hackers are gaining unauthorized access to networks by stealing log-in credentials, often times through phishing. By requiring multi-factor authentication, you drastically reduce the likelihood of an unauthorized third-party in possession of a username and password from accessing your computer email and network.	If you use Office 365, you can click here for instructions on setting up MFA. If you use Gmail, go to this link for support on MFA https://safety.google/authentication/ If you use an email system other than Microsoft or Gmail, you should contact your service provider for guidance on turning MFA on.
Email Scanning: Email scanning must be enabled on your mail services to ensure each email is scanned before entering your inbox or leaving your sent box for malicious attachments, links, or other content.	Phishing emails continue to exploit people within organizations. Scanning inbound and outbound emails for malicious links, attachments, and content helps strengthen overall defence of the organization by drastically reducing the amount of harmful messages that reach your inbox.	If you use outlook or Gmail, you should check your settings to see if e-mail scanning is enabled. It should automatically be turned on but if not, you should turn it on. For Microsoft support on email scanning click here. For Google support on email scanning click here. If you use a different email system, you should contact your service provider for guidance on turning this feature on.
Employee Awareness Training: Engage in cyber awareness training on at least an annual basis.	Employees continue to be the most exploitable element of organizational security in Canada; therefore, it is imperative they are trained properly.	The training is not prescriptive, and it could take any form, including law society courses, third party CPD courses, or in-house training, that would qualify as training. There are a number of free online options available for cyber awareness training. The following training has been approved by the cyber insurer: https://www.clia.ca/loss-prevention#cyber

CLIA Insurance Products

Errors and Omissions

Excess Insurance
CLIA Mandatory Insurance
Law Society Retention
Claim Deductible

Defalcation

Excess Insurance
CLIA Retention
Law Society Retention

Cyber

Stand Alone Cyber
Mandatory Cyber

Website - www.clia.ca

Questions About The Policy

1. Claims-made vs Occurrence-based?

Definition:

- **Claims-made:**
  - Covers claims that occur – and are reported- within the specific time period set by the policy
- **Occurrence-based:**
  - Protects the insured from any claim that happens during the policy period, regardless of when claim is reported

1. Claims-made vs Occurrence-based?

CLIA Mandatory Policy = <u>Hybrid</u>

- **Claims-made**: any claim or potential claim must be reported within the policy period in which the insured had knowledge of claim or potential claim
- **Occurrence-based**: For members no longer insured at the time a claim is made.
  - Retired, resigned, died or been disbarred (Legal Professions Act)
  - Policy will cover any claims that arise (subject to policy exclusions) as long as the occurrence took place during the period in which the member was insured

1. Claims-made vs Occurrence-based?

CLIA Excess Policy = Claims-made coverage

- Insurance needs to be in place when a claim is made and not when the error occurs
- Firms that do not renew their insurance will not have coverage for losses reported after the expiry date of the policy

2. Do You Need Excess Coverage?

- Excess insurance provides another layer of security should your defence and indemnity costs exceed the primary mandatory limits.
- As the value of client's transactions increases over time, so too does the need to secure adequate levels of Errors and Omissions (E&O) insurance.
- One large claim could quickly erode the primary policy, leaving you or your firm exposed to significant personal liability.
- **Not Just for 'Higher Risk' Areas or Large Firms**: All legal work can have exposure to large value claims. Don't equate the amount charged to a client with the potential claims amount if an error occurs. Even 'small matters' like a will prepared by a small firm in a rural community could result in a claim over the $1M limit.
- **Assess Risk of Firm, Not Individual**: Assess the risk for the firm, not just you individually.
- **Low Investment in Added Security**: Professional liability insurance is the cheapest form of insurance that there is. Lawyers can purchase $1M in coverage for $500.00 (2023) and the price per million goes down as the limit increases. For example, in 2023, $19M coverage = $102.00 premium/million (total $1951.00 premium).

2. Do You Need Excess Coverage?

Factors to Consider:

- The type of transactions and the potential impact on your clients;
- The size and frequency of large transactions;
- Whether former associates and partners have coverage that is either inadequate or excludes their past activities; and
- Whether the impact of the advice you've provided (and therefore potential liability) may grow over time.

4. Retirement Coverage?

Mandatory Insurance Coverage after Retirement

- Mandatory insurance exists as long as you are a member of the Law Society.
- Any status as long as you are not disbarred on dead.
- Claims made policy changes to occurrence-based policy upon retirement.
- Coverage up to $1 million is available to the retired insured through the Law Society Mandatory insurance.

4. Retirement Coverage?

Excess Coverage After Retirement

- Retirees remain responsible for work performed prior to retirement.
- Your excess coverage only applies to claims that occurred when you or your firm have CLIA excess coverage in place. If the firm decides to purchase excess insurance elsewhere, you may want to consider purchasing excess coverage
- CLIA offers discounted excess insurance to retired lawyers on an individual basis.

5. How to Report a Claim – Errors & Omissions

- Required to report a claim as soon as practicable after:
  - learning of a claim; or
  - Becoming aware of circumstances which might give rise to a claim
- Failure to report in a timely manner can jeopardize your coverage under the CLIA 'claims-made' policy
- Examples of when to report include:
  - Mistake is discovered which has or may have caused damage to a client
  - Any threat or communication of intention to sue made by a client
  - Another lawyer, on behalf of your client, requests your file
  - Client expresses dissatisfaction with the handling of a matter and there is an indication the client believes a loss has occurred

5. How to Report a Claim – Errors & Omissions

- In Nova Scotia:
  - Claims for errors and omissions handled through LIANS
  - Lawyers required to report to LIANS as soon as possible after learning of claim to becoming aware of circumstances that might give rise to a claim
- To report:
  - Use the insurance Claim Report Form available on the LIANS website www.lians.ca/members/report-a-claim

- **Don't Forget**: If your excess insurance coverage isn't with CLIA, consult your policy regarding required procedures.

6. How to Report a Claim – Cyber

How do you know if a cyber attack has occurred?

Here is a list of examples of indicators of a cyber attack:

- Your systems are locked, and you receive a demand for funds, property, or services to regain access
- Your sensitive data has been exposed or has been threatened to be exposed publicly
- Data migrates off the network and is being sent to an unknown source
- There is malware discovered on the system that has gone undetected for some time
- Your computer system performance has deteriorated or is interrupted, and you suspect that it may be due to malware
- A client or vendor alerts you of a third party attempting to impersonate your business.

Reporting a Claim – Cyber

1

Step 1: Assess If Email Has Been Compromised and Change Password

If you think you or your law firm may have suffered an email compromise (such as a client notifying you that your email account is sending them spam or phishing emails), before you do anything else, change your email password, and if you haven't already done so, enable multi-factor authentication (MFA).

If you are using a provider that doesn't have a multi-factor authentication option available, then it is highly recommended that you look at a new provider that does provide this option. Note: MFA is a requirement to be eligible for insurance.

2

Step 2: Engage with Your Internal or External IT Provider

(if you don't have an IT provider, go to Step 3)

Reach out to your IT provider and give them a summary of the situation. As they already know your systems, your IT provider should be the quickest to start evaluating the situation.

3

Step 3: Report the Cyber Attack

Notify the CLIA cyber insurance program via **cyberclaims@clia.ca** or **1-833-383-1488**:

- Communicate that you have a potential event unfolding, and
- Give a brief overview of the situation. If you have an IT provider, specify in your report that they are looking at the issue. This will make sure that the insurance program is ready to assist should the need arise.
- If you do not have an IT provider, the insurance programs breach coach will help to assess the next steps and may recommend an IT provider.

If you have any questions or are interested in more information contact:

Canadian Lawyers Insurance Association
#1530 – 2002 Victoria Avenue
Regina, Sask. S4P 0R7
(306) 347- 3050

Website - www.clia.ca
Blog – Not So Risky Business