CLIA|AAJC

Cyber insurance has been purchased on behalf of the Law Society's members who are in active private practice.

Coverage has changed over the previous coverage. Please note the new coverages and limits.

Limits:

Per claim limits, by insuring agreement:

1.) Security and Privacy Liability $250,000

SECURITY LIABILITY

Covers damages and claims expenses associated with lawsuits alleging the unauthorized access to, degradation of, or disruption to the insured's network, failure to prevent transmission of malicious code or viruses, and use of the insured's network to perform a denial of service attack (DDOS).

PRIVACY LIABILITY

Covers damages and claims expenses associated with lawsuits alleging the unauthorized collection, disclosure, use, access, destruction, or modification of personal protected Information.

2.) Data Recovery and Loss of Business Income $100,000

DATA RECOVERY

Covers cost to restore the network and data to the point it was at before the event occurred.

LOSS OF BUSINESS INCOME

Covers loss of income as a result of a breach on the insured's computer systems. This loss of income can be caused by decreased productivity, inability to deliver products or services, or inability to access data.

3.) Event Management Expenses $100,000

BREACH COACH SERVICES

Covers the costs of a breach coach to provide advice in responding to and assisting you in responding to a security or privacy breach, including determining your legal obligations to provide notice of a security breach, privacy breach or breach of privacy regulations.

NOTIFICATION COSTS

Covers costs associated with letting all those affected by the breach (including individuals, entities, and regulators) know that it has occurred, regardless of whether this notification is required by regulators or voluntary. This would include costs such as: mailing campaigns, credit monitoring, and call centres to handle questions.

FORENSIC INVESTIGATIVE COSTS

Covers costs associated with hiring a professional third party to determine where, when, and how the breach occurred; also, to ensure that no future problems occur as a result of that particular system issue.

CRISIS MANAGEMENT COSTS

Covers costs incurred in hiring a professional public relations team to help prevent reputational harm to your business.

4.) Data Extorsion $100,000

DATA EXTORTION

Covers ransom costs when there is a demand for compensation to stop a cyber-attack, such as ransomware.

5.) Bricking $100,000

BRICKING

Covers costs to replace computer & network hardware rendered useless after a cyber related event.

Note: Coverage available under any insuring agreement shall be reduced by, and may be completely exhausted by, payments made under any other insuring agreement.

E.g. If insuring agreements 1, 2, and 3 are triggered, the maximum amount the insurer will pay is $250,000 (the limit available under agreement 1). However, if losses under agreements 2 and 3 are in excess of $100,000, they will be capped at $100,000 combined, and the remaining limit of $150,000 will be available for agreement 1, as it carries a higher limit.

All claims arising out of the same, related, or continuing acts, facts, or circumstances, without regard to the number of insureds, claims, or claimants shall be considered a single claim and only one Limit of Liability will apply.

Aggregate annual limit for all claims: $1,000,000

Retention:

1.)	Security and Privacy Liability	$2,500
2.)	Data Recovery and Loss of Business Income	$2,500 / 12 hours
3.)	Event Management Expenses	$2,500
4.)	Data Extortion	$2,500
5.)	Bricking	$2,500

Only the highest applicable deductible will apply. i.e. the deductible will be $2,500 regardless of which or how many insuring agreements are triggered.

Who is covered:

The Law Society and the Law Society Members who were required to be insured by mandatory lawyers professional liability insurance at the time of Discovery and includes a Law Firm through which said Law Society Member was practicing law at the time of discovery.

<u>IMPORTANT</u>: IT requirements for coverage to respond:

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

1. Weekly backups of data, stored offsite, and tested at least annually.
2. Installation of critical patches, anti-virus software, and anti-spyware must be made within two weeks of release.
3. Installation and maintenance, and active monitoring within reasonable business practices, of firewalls and endpoint protection.

How to Report a Claim or Potential Cyber Incident:

If you need urgent crisis management or legal advice, please call or email the policy's Cyber Incident Breach Coach:

Blake, Cassels & Graydon LLP ("Blakes")

24/7 Hotline: 1-833-383-1488

Email: cyberclaims@clia.ca, ATTN: Imran Ahmad – Ridge Canada

Note: An email will be required for formal notice of claim or circumstance to the insurer.