



clia

[CANADIAN LAWYERS INSURANCE ASSOCIATION]

**CYBER INSURANCE
OVERVIEW**

WHY DO YOU NEED CYBER INSURANCE?



If you use the internet in any capacity, you and your law firm are targets for a cyber-attack. Cyber-attacks are unwelcome attempts to steal, expose, alter, disable, or destroy information through unauthorized access to computer systems. Cyber insurance provides coverage for lawyers and law firms who may fall victim to a wide range of cyber-attacks.

CLIA administers a Mandatory Cyber insurance program. This product is purchased by each CLIA Subscribing Law Society and provides coverage for their members who were required to be insured by mandatory lawyers' professional liability insurance at the time of Discovery.

Now, CLIA also provides an optional, enhanced Stand-alone Cyber insurance product for purchase through [CLIA's website](#) which can augment your protection, and provide your firm with robust coverage for its potential expenses and lost revenues in the event of a breach or attack. Designed by CLIA for law firms, the application is quick and easy, and can be completed in as little as a few minutes.

COVERAGES

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.

ANNUAL LIMIT FOR ALL CLAIMS

Mandatory Policy	Stand-Alone Policy
<p>The aggregate annual limit applicable to the Mandatory policy applies to all claims from all members and is as follows:</p> <p>[\$1,000,000 - YT, NT, NU, PE, NB]</p> <p>[\$2,000,000 – SK, MB, NS, NL]</p>	<p>The aggregate annual limit applicable to the Stand-Alone policy applies only to the individual law firm, and it either \$1,000,000 or \$2,000,000 depending on the option purchased.</p>

COVERAGE EXPLANATIONS

Network Security Liability

Covers damages and claims expenses associated with lawsuits against you alleging your failure to thwart the unauthorized access to, degradation of, or disruption to your network, your failure to prevent transmission of malicious code or viruses, and use of your network to perform a denial-of-service attack (DDOS) caused damage to others.

Privacy Liability

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

Data Recovery

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

Loss of Business Income

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

Dependent Network Interruption & Recovery

Covers loss of income as a result of a breach or cyber event at any contracted data/computing services provider that you rely upon.

Event Management Expenses

The following are covered under event management expenses:

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 law practice.

Data Extortion

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

Bricking

Covers costs to replace computer & network hardware rendered useless (turned into a brick) after a cyber related event.

Electronic Theft, Computer Fraud & Telecommunications Fraud

Covers the money and assets that are lost due to unauthorized access to your networks, systems, and data.
*(*Stand-alone Extension only)*

Social Engineering Fraud

Where fraudulent electronic communications or websites designed to impersonate you or your firm cause you damage, covers the costs of creating a specific press release or establishing a specific website to advise your clients and prospective clients of the fraudulent communications, reimbursement of clients for their financial losses arising directly from the fraudulent communications and your loss in profits as a direct result of the fraudulent communications. *(*Stand-alone Extension only)*

Multimedia and Intellectual Property Liability

Covers actual or alleged defamation, invasion of privacy, or infringement of any intellectual property rights arising out of social or multimedia content or user generated content.

Privacy Regulatory Defense & Penalties

Covers costs associated with being called in front of a civil, administrative, or regulatory proceeding and fines and civil penalties. Also covers monetary assessments, fines and penalties as a result of noncompliance with the published Payment Card Industry Data Security Standards.

Reputational Damage

Covers loss of income as a result of a cyber event in the media causing termination of your services by one or several of your clients.