CLIA|AAJC

CLIA/LAW SOCIETY CYBER PROGRAM

Introduction

If you use the internet in any capacity, you are a target 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 from a range of cyber attacks.

The Canadian Lawyers Insurance Association and Law Society administer the Mandatory Cyber insurance program and provide an optional enhanced stand-alone cyber insurance product for purchase through CLIA's website.

Coverages

The following table outlines the Mandatory and optional stand-alone cyber coverages:

Coverage	Mandatory Cyber	Stand-Alone Cyber	
		Package	Extension*
Network Security & Privacy Liability	$250K	$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	N/A	$1M or $2M	N/A
Bricking*	$100,000	N/A	$100K or $250K
Electronic Theft, Computer Fraud & Telecommunications Fraud*	N/A	N/A	$100K or $250K
Social Engineering Fraud*	N/A	N/A	$100K or $250K
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	$2,500	$5,000	$5,000

** These coverages are available for an additional fee and must be purchased in conjunction with Stand Alone Cyber.*

CLIA|AAJC

Coverage Explanations

Network 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.

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.

Dependent Loss of Business Income

Covers loss of income as a result of a breach or cyber event at any contracted data/computing services provider that the insured is reliant 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 business.

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 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.

Social Engineering Fraud

Covers any fraudulent electronic communications or websites designed to impersonate the insured or any of the insured's products for the costs of creating a specific press release or establishing a specific website to advise the insured's customers and prospective customers of the fraudulent communications, reimbursement of the insured's clients for their financial losses arising directly from the fraudulent communications and the insured's loss in profits as a direct result of the fraudulent communications.

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.

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.

CLIA|AAJC

How to Report a Claim

Step 1: Assess if email has been compromised and change password

If a lawyer/law firm thinks they may have suffered an email compromise (such as a client notifying you that your email is sending them spam, or phishing emails), before they do anything else, they should change their email password, and enable multi-factor authentication. If they are using a provider that doesn't have a multi-factor authentication option available, then it is highly recommended that they look at a new provider that does provide this option.

Step 2: Engage with your internal of external IT provider

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

The lawyer/law firm should reach out to their IT provider and give them a summary of the situation. As they already know their systems, they should be the quickest to help you start evaluating the situation.

Step 3: Report the Cyber Attack

The Lawyer/law firm should notify the CLIA cyber insurance program via cyberclaims@clia.ca or 1-833-383-1488 you have a potential event unfolding, give a brief overview of the situation.

If they do not have an IT provider, the insurance programs breach coach will help you asses your next steps and recommend an IT provider.

If they 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.
The breach coach will acknowledge the lawyer/law firms email or call and be standing by for updates. If a breach is confirmed or likely to have occurred, then the lawyer/law firm should immediately update the CLIA cyber insurance program and seek their advice to determine the best option for deeper investigation and remediation. The insurance program has access to forensics and other IT professionals which can be brought in to assist who specialize in cyber breaches, as well as vet any offerings. If the event turns out to be nothing, they should simply let the program know that it was a false alarm.

If a law firms or lawyers clients have notified you that they feel they have suffered damages as a result of a breach of your systems, then they should immediately report a claim to cyberclaims@clia.ca.