

## **CLIA Cyber Liability Program**

Lawyers and law firms are potential targets for hackers, ransomware and cyber criminals. However, the mandatory Professional Liability Insurance Policy has always excluded claims arising out of cybercrime. Now, CLIA has arranged a new program which will provide cyber coverage protection for lawyers and their clients. This new policy will take effect on July 1, 2017 for all lawyers required to be insured under the mandatory Professional Liability policy.

This new program will provide initial/first response coverage in the event of a cyberattack. The amount of coverage and the deductible will vary depending on the size of firm at the date the incident is discovered and the nature of the claim. The coverage is conditional on your firm taking certain steps to protect itself from cyberattack.

### **Damage from Disclosure of Client information**

If a client's confidential information ends up all over the internet or is disclosed inappropriately because of a cyberattack against a law firm, the client may have a claim for damages against the firm. One aspect of this new program provides coverage for the damages suffered by the client because of such disclosure. The following chart sets out the amount of coverage and the deductible, based on the number of lawyers in the firm, for damage claims resulting from disclosure of client confidential information arising out of a cyberattack.

<u>Firm size at date of discovery</u>	<u>Coverage Limit</u>	<u>Deductible</u>	<u>Aggregate</u>
1 lawyer	\$50,000	\$1,000	\$50,000
2 – 10 lawyers	\$50,000	\$1,000	\$100,000
11 – 25 lawyers	\$100,000	\$2,500	\$100,000
26+ lawyers	\$200,000	\$5,000	\$200,000

(Occurrence aggregate limits also apply).

### **Privacy Breach Notifications**

When a law firm's systems are compromised by cyberattack, the law firm may have a legal obligation to notify clients and third parties of a privacy breach which can be a time consuming and unfamiliar process. The policy covers firms for reasonable expenses to contain, investigate and mitigate a privacy breach and to notify the affected clients and third parties. The limits and deductibles for privacy breach notification coverage are set out below.

<u>Firm size at date of discovery</u>	<u>Coverage Limit</u>	<u>Deductible</u>
1 – 10 lawyers	\$5,000	\$1,000
11 – 25 lawyers	\$10,000	\$2,500
26+ lawyers	\$25,000	\$5,000

(Policy period and occurrence aggregate limits also apply).

### **System and Data Rectification Costs**

A cyberattack can result in your firm losing or misplacing data that you need to get your clients' work done. This coverage applies to retrieve, restore and replace any of the law firm's computer

programs or any other data and to repair, restore or replace any of the firm's computer systems damaged by a cyberattack so that client data is preserved and protected. The limits and deductibles for system and data rectification coverage are set out below.

<u>Firm size at date of discovery</u>	<u>Coverage Limit</u>	<u>Deductible</u>
1 – 10 lawyers	\$5,000	\$1,000
11 – 25 lawyers	\$10,000	\$2,500
26+ lawyers	\$25,000	\$5,000

(Policy period and occurrence aggregate limits also apply).

### **Cyber Threat and Extortion Costs**

In some cyberattacks, hackers hijack computer systems and deny access until you pay a ransom (usually in an online currency known as bitcoin). This program provides coverage for the costs associated with ransomware and other cyberattacks where client data in the law firm's computer system is held hostage. The limits and deductibles for cyber threat and extortion coverage are set out below.

<u>Firm size at date of discovery</u>	<u>Coverage Limit</u>	<u>Deductible</u>
1 – 10 lawyers	\$2,500	\$1,000
11 – 25 lawyers	\$5,000	\$2,500
26+ lawyers	\$10,000	\$5,000

(Policy period and occurrence aggregate limits also apply).

One of the best things about this new program is once your firm discovers that you have been the victim of a cybercrime, you have access to the program's 24 hour emergency response number. You will then be referred to the appropriate cyber response team so that you don't have to deal with a cyber incident on your own, without professional assistance.

There are some conditions of coverage which you should ensure your firm has in place. Your firm must have:

1. a firewall between the firm's systems and the internet;
2. up-to-date antivirus and malware endpoint protection on computers and laptops; and
3. weekly data back-ups.

If you purchase Voluntary Excess Insurance from CLIA, additional coverage is also available for damages to third parties arising from the disclosure of confidential client information as the result of a cyber incident. You can purchase a Cybercrime Endorsement providing limits of \$250,000 per claim per year at a cost of \$80 per lawyer. You can apply for this excess cyber coverage when you renew your Voluntary Excess insurance for July 1, 2017.

Coverage, as always, is subject to the final terms and conditions of the policy, please review the policy carefully once available and look out for additional information on this new coverage.