clia

[CANADIAN LAWYERS INSURANCE ASSOCIATION]

MANAGING AND REPORTING A CYBER ATTACK

MANAGING AND REPORTING A CYBER ATTACK

You are a member in a CLIA jurisdiction and you think you've been a victim of a cyber attack – what should you do?

First, 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.

WHAT TO DO IF YOU BELIEVE YOU HAVE SUFFERED A CYBER ATTACK?

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

1

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.

Step 2: Engage with Your Internal or External IT Provider

2

(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.

Step 3: Report the Cyber Attack

3

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.

AFTER REPORTING

- The breach coach will acknowledge your email or call and be standing by for updates.
    - If **a breach is confirmed or likely to have occurred**, then you 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**, you should simply let the program know that it was a false alarm.
- If clients have notified the you that they feel they have suffered damages as a result of a breach a system, then the lawyer/law firm should immediately report a claim to **cyberclaims@clia.ca**.

FAQS

What constitutes notice to the insurer?

An email to **cyberclaims@clia.ca** will be required for formal notice of claim or circumstance to the insurer.

Are there costs for calling the phone-line or emailing the CLIA cyber program?

If you require the services of the breach coach beyond providing initial overview of the claim situation, costs may be incurred for their assistance. You will not be charged for simply calling the cyber phone-line or emailing the cyber claims inbox, but if there is a legitimate claim and actual assistance is provided then there will be charges. To the extent coverage responds, you will be responsible for your deductible and potentially costs over and above what the coverage provides for. If coverage does not apply, then you will be responsible for the costs. **Note:** you should be mindful of obligations, both professionally and legally with respect to privacy breaches - although there may be costs to manage an event, failing to manage a privacy breach could be far more costly than paying for professional assistance.

How does an insured get reimbursed?

Insureds (i.e., lawyer or law firm) will be reimbursed directly from the insurer.

What if I have other cyber insurance through other providers?

Lawyers and law firms may have other cyber insurance through other providers. If an Insured has or had at any time insurance placed with another insurer that applies to a Claim or Loss covered by the CLIA Law Society Mandatory Policy, unless specifically scheduled as underlying, the Mandatory policy will apply as excess insurance over the other insurance to the extent that the other insurance is valid and collectible. To the extent that other policies have the same clause, the insurers typically come to some proportionate share agreement. Either 50/50 or based on the proportion of the limits available.

When making a claim, the insured should notify all parties of the relevant insurance policies it has in place. The insurers will then coordinate a response from that point on.