HUB International HKMB Limited
595 Bay Street, Suite 900, Box 81
Toronto, ON, Canada M5G 2E3
T: 1 (855) 565-4626
oao@hubinternational.com
www.hubinternational.com

OAO – CYBER FAQ

Cyber insurance continues to face challenges. OAO members have suffered numerous losses in the last 2 years, and the Canadian cyber insurance market has seen losses increase nearing 500% since 2020.

While the OAO Professional Liability policy ceased offering a minor cyber extension back in 2022, members still have cyber coverage options to consider, via a cyber extension available to purchase as part of the PLI renewal process or a stand-alone cyber policy to protect your practice on a broader basis.

What is cyber insurance?

Cyber insurance is a specialty insurance product that is intended to protect clinics/practices, and individual OD's, from Internet-based risks, including privacy breaches. These include bad actors (hackers) accessing a clinic's records (including private patient information) and damaging a clinic's IT infrastructure.

Cyber insurance provides two main sections of coverage:

1) First Party costs (out of pocket costs) – costs borne by the clinic in the event of a privacy breach/cyber-attack. These include breach response costs, notification costs, data restoration, business interruption, cyber-extortion/ransomware payment.

2) Third Party liability – when a third party (likely a patient) makes a claim against a clinic and/or individual OD's because of their privacy being breached due to a cyber-attack. This coverage would provide defense costs and claims settlement, subject to the terms and conditions of the policy.

What do common cyber claims look like?

In Canada, over 80% of claims are for first party (out of pocket) costs. Privacy breach (third party) liability claims are not as common in Canada, but they have a potential for a high payout, as is evidenced by many class action lawsuits that have been seen in the U.S.

The largest single cause of loss is cyber-extortion/ransomware attack. This is when a bad actor (hacker) holds a clinic/practice's computer systems and patient data for ransom.

HUB International HKMB Limited
595 Bay Street, Suite 900, Box 81
Toronto, ON, Canada M5G 2E3
T: 1 (855) 565-4626
oao@hubinternational.com
www.hubinternational.com

What risks do OAO members face?

An optometry clinic/practice could face significant financial hardship in the event of a cyber-attack. There could be out of pocket costs including clinic downtime, contracting a third party to determine cause of attack and remediate computer systems, notifying patients of a potential breach and providing credit monitoring services to those patients. Additional costs include loss profits if the practice cannot operate and potential ransom payments should the clinic face a cyber-extortion/ransomware attack.

In addition, both clinic/practices and individual OD's face exposure to third party privacy breach claims coming from patients where they are named in said claim.

It should be noted that **Associates who are practicing at multiple clinics** on an annual basis are exposed to a greater risk of third party privacy breach claims (i.e. cyber liability claims) since they are working with multiple sets of patient data.

What cyber coverage is provided under the extensions available to purchase as part of OAO PLI Program?

The cyber extensions are provided by Totten Group via Tokio Marine Canada (new provider for 2023).

The OAO cyber extension offerings include a liability only option for $100,000, as well as broader offerings for both first party and liability losses at the $500,000 and $1,000,000 limits.

NEW for 2023 – The liability only option (Option 1) will NOT require confirmation of Multi-Factor Authentication (MFA); however remaining extension options (2&3) will require MFA as they provide broader coverage.

It is the recommendation of the OAO and HUB that Associates consider the $100,000 liability only option and that clinic/practice owner/operators consider the higher limits with broader coverage, or discuss a stand-alone cyber/privacy breach policy with HUB.

Further information on cyber coverage can be found on the HUB OAO website or on the OAO PLI glossary

HUB International HKMB Limited
595 Bay Street, Suite 900, Box 81
Toronto, ON, Canada M5G 2E3
T: 1 (855) 565-4626
oao@hubinternational.com
www.hubinternational.com

What is Multi Factor Authentication (MFA)? Why is this a requirement to purchase most OAO cyber extensions?

Due to the increases in losses across the cyber insurance landscape, most insurers are requiring insureds to use multi-factor authentication when they are logging into their email or servers remotely (i.e. outside of the clinic in the case of OAO members).

Multi Factor Authentication (MFA) is a method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber-attack / privacy breach. These factors can include the use of an app to verify or provide a code sent via text/email/phone call.

How does a stand-alone cyber policy compare to the extensions and why should clinic/practice owners consider it?

A stand-alone policy provides broader coverage limits per claim, since the policy would provide the full policy limit per loss ($1MM, $2MM, etc) vs. any sub-limits. Also, many stand-alone cyber policies do not have an aggregate for first party losses, which means that a clinic could potentially have coverage for multiple $1MM+ cyber claims within a single policy year.

In addition, a stand-alone cyber policy would extend to all clinic/practice partners, associate OD's, employees, technicians and contractors on staff. Depending on certain factors further savings could be realized when cover is placed over multiple clinic locations.

A stand-alone cyber policy starts with premiums around $2,000 with deductibles around $2,500.

Stand-alone policies also include cyber-crime coverage. This coverage would respond to incidents of social engineering, phishing, cyber transfer fraud, etc.

Finally, a stand-alone cyber policy has the benefit of a single deductible. If multiple clinic/practice owners had individual cyber extensions, each partner would have to pay their own deductible when making a claim.

Based on the above, HUB recommends that clinic/owners consider a stand-alone cyber insurance policy, which would protect all clinic/practice owners and entities, associated OD's and employees.

Your HUB International broker would be pleased to discuss this with you and can provide more information about this option if you are interested.

If you wish to discuss best options for you in your practice, or you have any questions/concerns, please contact your HUB OAO by email at oao@hubinternational.com or by phone at **1-855-565-4626**.