How to lower your cyber insurance costs: 3 key steps

September 13, 2022

This is the last article in a three-part series. Check out part two for examples of cyber insurance exclusions (plus insight into how insurers and insureds usually negotiate these issues) and part one for need-to-knows about business interruption coverage and your cyber insurance policy.

As the cyber insurance industry matures and demand for cyber coverage skyrockets, insurers are becoming more particular about who they'll cover. Canadian organizations obtaining coverage may find premiums cost more, coverage is limited and their policies now include deductibles and cost sharing (also called co-insurance). Given rising costs and greater scrutiny by insurance companies, is cyber insurance still worth it? (Spoiler alert: The answer is a resounding yes, as we briefly explain below.) When it's policy renewal time, these three steps will increase your chances of getting the nod from your insurance company and show you how to lower your cyber insurance costs.

Is cyber insurance worth the cost?

The answer is almost always yes.

As cyber insurance lawyers, we've helped insurers navigate some of Canada's largest claims. We've also provided advice to business owners. Our experiences at both ends of the spectrum have taught us one important lesson: as technology and data become increasingly integral to the mission critical and everyday activities of organizations, cyber insurance has moved from a nice-to-have to a need-to-have.

Here are some reasons cyber insurance is worth the cost:

- Cyber insurance will cover a significant portion of your costs, including breach coaching from a lawyer, digital forensics, crisis communications, system restoration and business interruption. It also provides defense and indemnity for certain claims against you. With each incident costing Canadian businesses an average of US$310,000 in 2020, insurance is money well spent.
- Ransomware is increasingly automated, which makes it cost-effective for criminals to go after small organizations.

- 98 per cent of Canadian organizations reported experiencing a ransomware attack in 2021.
- Cybersecurity regulation by the Canadian government, including fines, is increasing. Examples are Bill C-26 and Bill C-27, both introduced in June 2022.

Now that we've established the value of cyber insurance, follow these three steps to help with insurer approval and lower your costs.

Step 1: Implement cyber security best practices

Robust cybersecurity practices will make your organization more attractive to insurance companies. Our 11-point cyber hygiene checklist is a helpful guide to the type of practices your insurance company will be looking for. The bullets below are a quick summary:

- multifactor authentication for all users
- endpoint detection and response software
- network security monitoring
- regular employee cybersecurity training, including simulated attacks
- mandatory password changes and complexity practices
- software and hardware update policies
- restricted admin-level access
- a comprehensive data map
- a data retention policy
- off-site data back-ups
- a privacy compliance program

A number of the measures are inexpensive, particularly for small and medium-sized businesses. In 2020, a leading cyber insurance provider looked at several data sources, including claims from the more than 25,000 Canadian and U.S. businesses it insured at the time, and reported that low-cost and no-cost measures — such as multifactor authentication and regular off-network data back-ups — could have prevented most losses. Organizations without basic cybersecurity protocols are now being denied cyber insurance altogether at policy renewal time.

Step 2: Have some skin in the game

Many organizations are able to navigate this turbulent market by taking on some of the risk, either by increasing their deductibles, accepting lower limits or sub-limits for certain coverages, or through self-insured retentions (where the organization is responsible for paying a pre-set dollar amount towards the claim before the policy kicks in). Using these approaches, organizations can still obtain cyber coverage for catastrophic claims, while directly covering the cost of less impactful incidents themselves.

To truly save money using this approach, it is critical that you implement the cyber hygiene practices outlined in Step 1. Otherwise, you'll be vulnerable to costly incidents and won't have insurance to cover them. A good strategy is to invest any savings from reduced premiums into your cybersecurity improvements.

If you're interested in increasing your deductible or self-insured retention, discuss your options with your broker.

Step 3: Carefully complete your application

Renewal will likely look different this year — either you'll receive a new, longer application form to complete from your broker, or the insurance underwriter will follow up with additional questions. A third-party security expert hired by your insurance company may even interview you or perform an external assessment to determine your preparation, resilience and risk management related to cyber threats.

The evaluation of your application and any supplementary intel gathered by your insurance company will determine the extent of your coverage and your premiums. From application to decision, it could be a three- to six-month process.

Invest the time and resources to comply with the requirements of your broker and insurance company. Have the right people at the table so the answers you give are accurate. Provide evidence of your due diligence when it comes to cybersecurity: arrange for your own third-party audit, provide proof that you're following credible recommendations, and be ready with a show-and-tell of your relevant cybersecurity policies and plans.

Summing it all up

In summary, the cyber insurance market is hardening and the onus is on organizations to demonstrate they're a good risk for coverage. If, after following the steps in this article, you still can't secure affordable insurance, you'll certainly have a better understanding of your needs and can rest assured that you've taken important actions to protect yourself.

If your insurance renewal is around the corner, contact Eric or Neda for preparation help, including drafting your incident response plan, satisfying your cyber hygiene checklist, and understanding your organization's unique cyber risk profile in the context of insurance.

By

Eric S. Charleston

Expertise

Cybersecurity, Privacy & Data Protection, Insurance Claim Defence, Technology

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2026 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.