

AGENDA

Lunenburg County Multi-Purpose Centre Corporation

Thursday, May 19, 2022 6:00 p.m.

Held in Multi-purpose room, LCLC / Virtually via Microsoft Teams

- 1. Call to Order**
- 2. Information Sharing (Questions by Board Members and attending members of the public)**
- 3. Approval of Agenda**
- 4. Approval of Minutes – April 21, 2022**
- 5. Business Arising from Minutes & Unfinished Business**
 - 5.1 Strategic Plan Review
 - 5.2 Reply from Minister Pat Dunn re Covid emergency funding 2
 - 5.3 Cyber Security Insurance Option 3-36
- 6. Correspondence**
- 7. New Business**
 - 7.1 General Manager Q&A
 - 7.2 “Recognizing Volunteerism” membership rates (Councillor Hubley)
- 8. Information/Updates**
 - 8.1 General Manager’s Monthly Report..... 37-38
 - 8.2 Aged Receivables 39-41
 - 8.3 Financial Statements To Follow
- 9. In Camera**
 - 9.1 Contract Negotiations under Section 22(2)(e) of the MGA – Lumberjacks Update
 - 9.2 Contract Negotiations under Section 22(2)(e) of the MGA – Facility Sponsorship
- 10. Next Meeting – Thursday, June 16, 2022 at 6:00 p.m.**
- 11. Adjournment**



**Communities, Culture, Tourism and Heritage
Office of the Minister**

1741 Brunswick Street, PO Box 456, Halifax, Nova Scotia, Canada B3J 2R5
Telephone 902-424-4889 • Fax 902-424-4872 • novascotia.ca

April 13, 2022

Councillor Pam Hubley
Chair, LCMPCC
Lunenburg County Lifestyle Centre
135 North Park Street
Bridgewater NS B4V 9B3

Dear Councillor Hubley:

As Minister for the Department of Communities, Culture, Tourism and Heritage, the Premier has asked me to respond to your letter dated March 17, 2022 regarding eligibility of the Lunenburg County Multi-Purpose Center Corporation (LCMPCC) for the Non-Profit Recreation Facilities COVID-19 Emergency Funding program in 2021.

As you noted, the province recognized the substantial impact the pandemic was having on recreation facilities in the province and their role in offering services to support the quality of life and health and wellbeing of residents. As a result, the Department of Communities, Culture, Tourism and Heritage worked with the Recreation Facilities Association of Nova Scotia (RFANS) to establish a one-time, emergency fund, to assist those facilities most in need: registered non-profits that own and operate recreation facilities that were financially impacted by COVID-19 and who were not supported by or associated with a municipality. The fund is now exhausted, and the program has been closed since the fall. While we aren't considering additional projects, if the municipality would like to meet with staff of the Communities, Sport and Recreation Division to discuss our grant programs, contact Colleen Strickland at colleen.strickland@novascotia.ca who will arrange the meeting.

The province is truly grateful for the services and opportunities provided by facilities like the LCMPCC. Your role in providing safe recreation, sport and cultural opportunities is a significant contributor to the mental and physical health of the residents in your communities.

Sincerely,

Pat Dunn
Minister

cc : Justin Huston, Deputy Minister
Melissa MacKinnon, Associate Deputy Minister
Bill Greenlaw, Executive Director

Cyber Liability Quote

Lunenburg County Lifestyle Centre

March 7, 2022

This Summary of Insurance is for information purposes only. The insuring agreements, general terms, conditions and exclusions of the actual policy will govern specific application of the various coverages referred to herein. The actual policy documents will supersede the Summary of Insurance



TABLE OF CONTENTS

1. CYBER INSURANCE	1
2. COVERAGE DESCRIPTIONS	3

1. CYBER INSURANCE

Insurer: Option A) Coalition Option B) CFC Underwriting

Term: Date of Binding for 12 months

Limits	Coverage Description
\$1,000,000	Media Content Insurance
\$1,000,000	Security & Privacy Liability Insurance
\$1,000,000	Network Interruption Insurance
\$1,000,000	Event Management Insurance
\$1,000,000	Cyber Extortion Insurance
\$1,000,000	Aggregate Limit all coverages above

Deductibles Coalition - \$50,000 per claim with a \$125,000 Aggregate Retention
8 hour Waiting Period with respect to Network Interruption Insurance

CFC Underwriting - \$5,000 per claim

Retroactive Date Inception Date

Premium: **Option A1)** \$4,862 (Coalition)
Option A2) \$2M Limits - Available – Not Quoted
Option B1) \$2,860
Option B2) \$2M Limits - Available – Not Quoted



Forms Coverage Forms applicable (Coalition):

DECLARATIONS	CYBCAN 0009 0420
COALITION CYBER POLICY	CYBCAN 0001 0320
SERVICE OF SUIT ENDORSEMENT	CYBCAN 0005 0420
REPUTATION REPAIR ENDORSEMENT	CYBS 0005 0420
CAP ON LOSSES FROM CERTIFIED ACTS OF TERRORISM	
CYBCAN 0011 0520	
DISCLOSURE PURSUANT TO TERRORISM RISK INSURANCE	
ACT	CYBCAN 0010 0520
QUOTA SHARE ENDORSEMENT	CYBS 0021 0221
WRONGFUL COLLECTION EXCLUSION	CYBCAN 0015 1020
\$0 RETENTION FOR SERVICES FROM COALITION INCIDENT	
RESPONSE	CYBCAN 0024 0121
MULTI-FACTOR AUTHENTICATION (MFA) RETENTION	
REDUCTION	CYBS 0001 0420

Coverage Forms applicable (CFC)

Cyber, Private Enterprise (CA) v3.0
 Schedule of Information
 Choice of Law
 Jurisdiction and Service of Suit Condition Amendatory Clause

See Attached Risk Assessment Report
 See Attached CFC Feature Sheet

NOTES: This quote is valid for 60 days.



2. COVERAGE DESCRIPTIONS

General Description Provides the Town of Mahone Bay with first party and third party protection against Security and Privacy Liability, Regulatory Actions, Event Management, Cyber Extortion, and Network Interruption.

Security and Privacy Liability (including Regulatory Action) Pays loss the Insured incurs as a result of a Security Failure or Privacy Event (failure to protect Confidential Information)

Loss means compensatory damages, judgments, settlements, pre-judgment and post-judgment interest and defence costs, including:

- ✓ Punitive damages (where permissible by law)
- ✓ Civil fines or penalties resulting from a Regulatory Action (where permissible by law)
- ✓ Monetary amounts the Insured is required by law or agreed to by settlement to deposit into a consumer redress fund
- ✓ Amounts payable in connection with a PCI-DSS Assessment (payment card fines or penalties associated with the Insured’s non-compliance of PCI Data Security Standards)

Network Interruption Pays loss the Insured incurs as a result of a Security Failure

Loss means costs incurred for 120 days following the date of first interruption that would not have been incurred if not for the interruption (including net income that would have been earned and continuing normal operating expenses incurred, including payroll)

Event Management Pays loss the insured incurs as a result of an alleged or actual Security Failure or Privacy Event

Loss means reasonable and necessary expenses and costs within one year of the discovery of the Security Failure or Privacy Event:

- ✓ To conduct investigation as to cause
- ✓ To retain advice from PR Firms, Crisis Management, or Law Firms to mitigate damages, including reputational damage
- ✓ To notify victims of the breach
- ✓ For identity theft education and assistance, including call centre services, credit monitoring, victim reimbursement
- ✓ To restore, recreate or recollect Electronic Data



Cyber Extortion Pays loss the Insured incurs as a result of a Security Threat or Privacy Threat

Loss means monies paid by the Insured:

- ✓ To terminate the threat (with the Insurer’s prior consent), including the obtaining of Bitcoin or other cryptocurrency to be surrendered as payment
- ✓ To conduct an investigation to determine cause of the threat

- Coverage Extensions**
- \$50,000 Criminal Reward coverage
 - \$50,000 Claim Preparation Costs
 - Cyberterrorism
 - Single deductible applies even if more than one coverage is triggered during a loss

- Major Coverage Exclusions**
- Cyber Crime (Funds) including Social Engineering Fraud, Invoice Manipulation and Phishing (*Note – CFC includes up to \$250,000 for some of these coverage lines*)
 - Technology Errors and Omissions (IT services you provide to others)
 - Bodily injury or property damage liability
 - War
 - Power failure unless caused by a security failure or privacy event
 - Property insurance risks (fire, smoke, lightning, hail, flood, earthquake, etc.)
 - Purchase or sale of securities or violation of securities law
 - Employment practices liability
 - Satellite failure



THIS DOCUMENT WAS ISSUED AT:

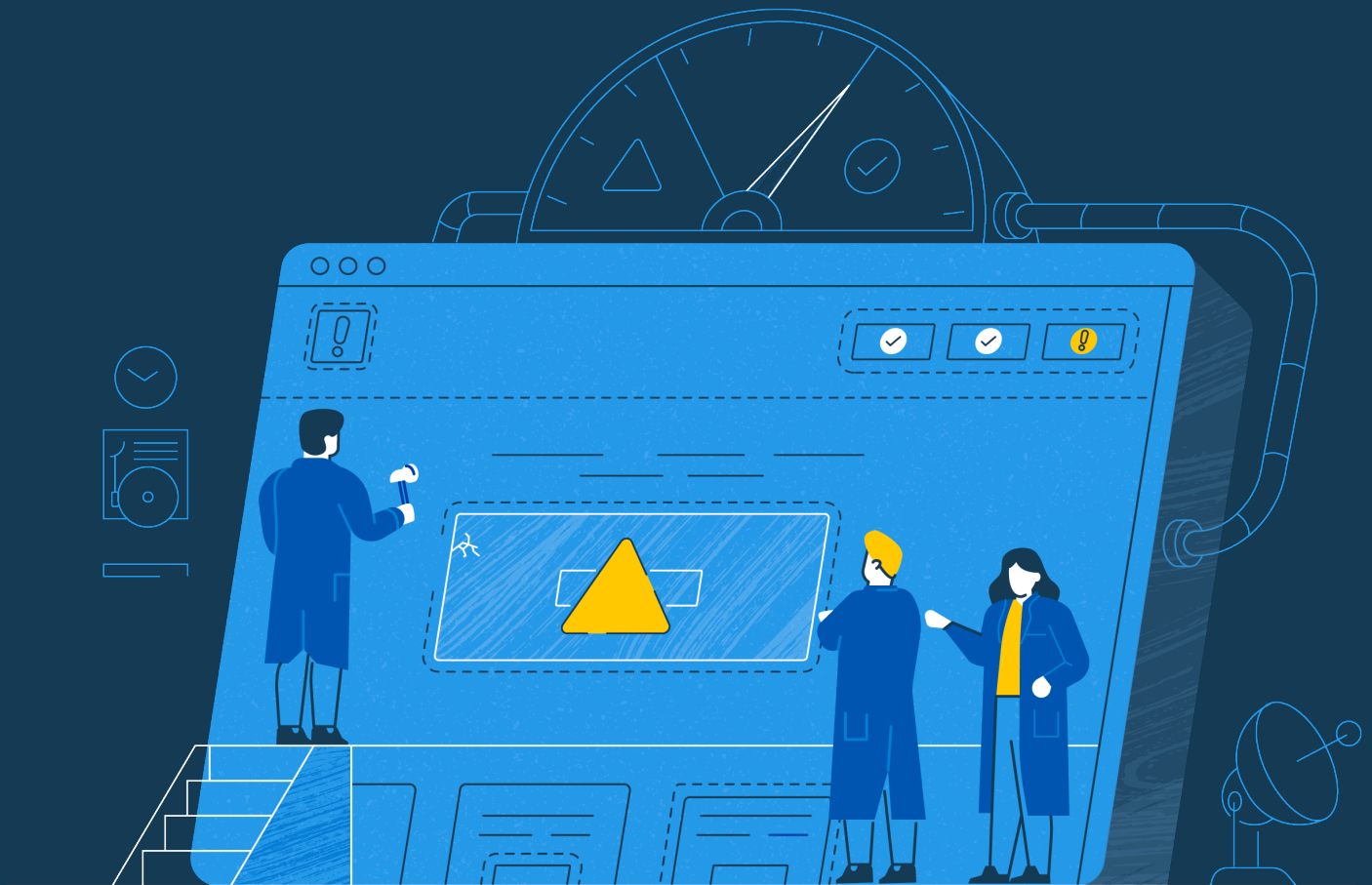
BFL CANADA Risk and Insurance Services Inc.
306-1595 Bedford Highway, Bedford, NS B4A 3Y4

GENERATED ON MARCH 7, 2022

Risk Assessment

PREPARED FOR

Lunenburg County Lifestyle Complex



Coalition is the leading provider of cyber insurance and security, harnessing the power of technology and safety of insurance to help organizations solve cyber risk. This Coalition Risk Assessment is the first step in this continuous monitoring process. Using externally observable data, this report provides an objective, evidence-based assessment of your cyber risk and overall security preparedness. As your dedicated risk management partner, our security team is available to provide additional context and help you to implement security and loss controls. Coalition policyholders receive 24/7 continuous security monitoring, all at no additional cost.

Sections

- 1 Executive Summary
- 2 Loss Costs & Benchmarking
- 3 Email Security
- 4 Vulnerabilities
- 5 IP and Domain Reputation
- 6 Malware
- 7 DNS
- 8 Sensitive Information Exposed
- 9 User Behavior

[What is Cyber Insurance?](#)

[Coalition Features](#)

[FAQs](#)

[Glossary](#)

This assessment is provided for informational purposes only. Risk-related analyses and statements in this assessment are statements of opinion of possible risks to entities as of the date they are expressed, and not statements of current or historical fact as to the security of any entity. YOUR USE OF THIS ASSESSMENT IS AT YOUR OWN DISCRETION AND RISK. THE ASSESSMENT IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. TO THE MAXIMUM EXTENT PERMITTED BY LAW, COALITION EXPRESSLY DISCLAIMS ALL WARRANTIES AND CONDITIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. COALITION DOES NOT WARRANT THAT (i) THE ASSESSMENT WILL MEET ALL OF YOUR REQUIREMENTS; (ii) THE ASSESSMENT WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR-FREE; OR (iii) THAT ALL ERRORS IN THE ASSESSMENT WILL BE CORRECTED.



1 Executive Summary

This assessment evaluates cybersecurity risk using data-driven, objective, and publicly available metrics together with Coalition’s proprietary claims data. The findings and recommendations in this report are intended to help proactively identify, quantify, and manage cybersecurity risk. All findings can be investigated in greater detail using Coalition Control.

Lunenburg County Lifestyle Complex

Domain: lclc.ca

Last scan: March 7, 2022

Revenue: \$3,200,000

Industry: Consumer Discretionary

Employees: 50

Records: 100,000

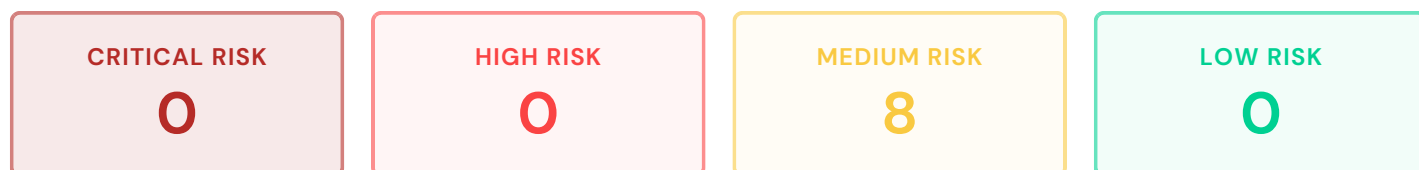
Your rank relative to all Coalition policyholders

Discovered vulnerabilities will not impact your coverage. However, resolving them may reduce your premium.



Vulnerabilities by Criticality

Prioritized list of vulnerabilities we found on your assets. Critical vulnerabilities represent an active threat and should be remediated as soon as possible.



Detected Assets

Outside-in view of the Web properties we identified.

DOMAINS

6

IPS

23

APPLICATIONS

1

SERVICES

29

HOSTING

6

Vulnerabilities by Category

Security vulnerabilities found associated with your assets by level of security impact.



2 How Much Would a Cyber Incident Cost?

Most cyber incidents are manageable, however it is catastrophic loss that organizations need to be prepared for. Using demographic data on your organization, together with Coalition's claims data, we've modeled the probability that organizations in your peer group will experience a cyber loss over the next 12 months, as well as the expected severity of loss using a statistical model derived from 10,000 simulated years of cyber incidents. By comparison, we've also included benchmarking on the insurance limits purchased by your peer group.



Incident likelihood compared to average Coalition insured

0.5x as likely

Limits purchased by peer organizations



Estimated loss based on your organization's risk profile

	Overall	Ransomware	Funds Transfer Fraud	Data Breach
MEDIAN	\$168,935	\$52,496	\$101,893	\$14,546
1 IN 10 YEAR LOSS	\$788,887	\$129,439	\$545,929	\$113,520
1 IN 100 YEAR LOSS	\$2,674,283	\$227,542	\$2,145,130	\$301,611

* Data is from multiple sources, including Coalition's own data. Actual numbers may vary significantly from calculator estimates based on additional factors for a given business. The data provided is for informational and educational purposes only. Use of the Coalition Coverage Calculator should not be used as a replacement for a company's own due diligence in regards to their cyber risk. Access and use of the Coalition Coverage Calculator is predicated upon the acceptance of Coalition, Inc. [Terms of Service](#).

3 Email Security

Improperly configured email servers make it easier for cybercriminals to commit fraud against your organization. Social engineering and email compromise are the leading root cause for losses reported by Coalition policyholders. This section identifies common email security measures to protect your organization.



3.1 DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol that is designed to give email domain owners the ability to protect their domain from unauthorized use (known as email spoofing). The purpose of implementing DMARC is to protect a domain from being exploited in business email compromise attacks, phishing emails, email scams, and other cyber threat activities.

PASS
1

FAIL
0

Pass (1)

lclc.ca

Fail (0)

None

3.2 SPF

Sender Policy Framework (SPF) is an email authentication method designed to detect forging sender addresses during the delivery of an email. This measure specifies what email servers are allowed to send email from your domain. It helps ensure that someone cannot create an email server and send it as your domain unless you have authorized them to do so in your DNS records.

PASS
1

FAIL
0

Pass (1)

lclc.ca

Fail (0)

None

4 Vulnerabilities

This section describes the security vulnerabilities we detected on your assets, including vulnerabilities identified on your web applications and services.



4.1 Web Application Security

Securely configuring web applications can prevent cybercriminals from compromising your, and your user, systems and data.

Scan performed and no results were found.

‡ Shared host (this issue was detected in a 3rd party asset not directly controlled by your organization)

4.2 Services

Issues found with technologies and software running on your assets.

HTTP Service without SSL/TLS found

HTTP service found without SSL/TLS. HTTPS (Hypertext Transfer Protocol Secure) is an internet communication protocol that protects the integrity and confidentiality of data between the user's computer and the site. Users expect a secure and private online experience when using a website. Using SSL/TLS provides three layers of protection: Encryption, Data integrity, Authentication.

MEDIUM RISK

1

Assets

Recommendations

- Review the service usage and implement HTTPS.

References

- [SSL Research: SSL and TLS Deployment Best Practices](#)
- [Mozilla Wiki: Security/Server Side TLS](#)

Asset	Source	Found
104.152.168.28:80 ‡	DNS A	Jan, 06 2022

Email Service without SSL/TLS found

Email service was found without SSL/TLS. This enables applications to communicate across a network in a private and secure fashion, discouraging eavesdropping, tampering, and message forgery. Using SSL/TLS provides three layers of protection: Encryption, Data integrity, Authentication.

MEDIUM RISK

5

Assets

Recommendations

- Review the service usage and implement SMTPS.

References

- [Wikipedia: SMTPS](#)

Asset	Source	Found
104.152.168.28:110 ‡	DNS A	Feb, 22 2022
104.152.168.28:587 ‡	DNS A	Feb, 23 2022
104.152.168.28:143 ‡	DNS A	Feb, 25 2022
104.152.168.28:26 ‡	DNS A	Feb, 19 2022
104.152.168.28:25 ‡	DNS A	Feb, 20 2022

‡ Shared host (this issue was detected in a 3rd party asset not directly controlled by your organization)

MySQL Service found

A MySQL service was found running on the host. When found exposed this service becomes targeted by malicious actors trying to gain access. This is a huge risk from a data leak perspective as anyone could try to access your entire database.

MEDIUM RISK

1

Assets

Recommendations

- Disable the service if not in use.
- Limit access only to the specific IP addresses that need to access it, either with filtered access or via VPN.

References

- [MySQL Website](#)

Asset	Source	Found
104.152.168.28:3306 ‡	DNS A	Feb, 13 2022

FTP Service without SSL/TLS found

FTP service was found without SSL/TLS. This enables applications to communicate across a network in a private and secure fashion, discouraging eavesdropping, tampering, and message forgery. Using SSL/TLS provides three layers of protection: Encryption, Data integrity, Authentication

MEDIUM RISK

1

Assets

Recommendations

- Review the service usage and implement FTPS.
- Disable FTP and use SFTP.

References

- [Wikipedia: FTPS](#)

Asset	Source	Found
104.152.168.28:21 ‡	DNS A	Mar, 06 2022

‡ Shared host (this issue was detected in a 3rd party asset not directly controlled by your organization)

5 IP and Domain Reputation

Your organization's IP reputation depicts the quality of your email sending environment. This section lists reputational issues found with your IPs and domains, such as sending spam or performing malicious actions. These assets' reputations impact your organization's ability to send email from your IP.



5.1 Blocklisted Domains

Domains found in public blocklists - if one of your assets is found on these lists typically means that some type of malicious activity was performed.

NO RISK

0

Domains

Scan performed and no results were found.

5.2 Honeypot Events

Our distributed network of honeypots constantly listens for unsolicited connections and attacks. There is no reason for any of your assets to communicate with these honeypots. If an event appears in this section, there is a high probability of malware or malicious activity on your network. Some shared hosts randomly scan the internet to test delivery speeds, so if the asset shown is tagged as shared hosting, it might not be a malicious event

NO RISK

0

Domains

Scan performed and no results were found.

‡ Shared host (this issue was detected in a 3rd party asset not directly controlled by your organization)

6 Malware

This section lists your assets that have been connected in 3rd party blocklists (that are typically used by enterprise companies to block IP addresses or domains from contacting their assets) with recent malware infections or indicators of compromise.



Assets Associated with Malware

Assets we discovered where malware activity was detected.

NO RISK
0
Assets

Scan performed and no results were found.

Assets Associated with SPAM

Assets we discovered that send unsolicited communication.

NO RISK
0
Assets

Scan performed and no results were found.

‡ Shared host (this issue was detected in a 3rd party asset not directly controlled by your organization)

Malicious Events

Any assets that performed malicious actions detected by us or third-party partners.

NO RISK

0

Events

Scan performed and no results were found.

7 DNS (Domain Name System)

We found the following DNS records associated with your organization. DNS records let the Internet know how to reach your email server, website, and other key functions, and are used by cybercriminals to assess your organization's attack surface.



A Records

Address Records are used to translate a human-readable string into a machine-readable IPv4 address.

www.lclc.ca	104.152.168.28
cpanel.lclc.ca	104.152.168.28
lclc.ca	104.152.168.28
autodiscover.lclc.ca	40.97.223.120 • 52.96.166.232 • 52.96.18.8 • 52.96.64.200 • 52.97.146.184 (+3)
mail.lclc.ca	142.227.60.120

AAAA Records

Address Records are used to translate a human-readable string into a machine-readable IPv6 address.

autodiscover.lclc.ca	2603:1026:c06:140b::8 • 2603:1026:c06:140f::8 (+8)
--	--

CNAME Records

Canonical Name Records are used as an alias. This enables the utilization of external resources, and for those resources to appear as part of the organization's domain.

www.lclc.ca	autodiscover.lclc.ca
--	--

MX Records

Mail Exchange Records denote where mail for a particular domain should be routed.

www.lclc.ca

lclc.ca

NS Records

Name Server Records indicate the hosts that should be used as an authoritative source for records for a particular domain.

www.lclc.ca

lclc.ca

SOA Records

Start of Authority Records contain metadata around the parameters of retrieving records for a particular domain. These records contain a serial number, refresh duration, retry duration, expiry duration, and time to live duration.

www.lclc.ca

lclc.ca

TXT Records

Text Records are used for a variety of purposes. One of the most common functions is to hold Sender Policy Framework(SPF) strings. It is also frequently used to verify domain ownership.

www.lclc.ca

_dmarc.lclc.ca

lclc.ca

8 Sensitive Information Exposed

This section details information found in 3rd party vendor leaks that are associated with your organization or assets.



Leaked data in 2022

There were no 3rd party data breach events in your organization.

Leaked data in 2021

There were no 3rd party data breach events in your organization.

Leaked data in 2020

Phone numbers, Physical Addresses, Document Titles, Hashed Passwords, Names

Nitro

1 leaks

1 email address found in leaks:

ckelly@lclc.ca

Leaked data in 2019

Phone numbers, Geographic locations, Names, Email addresses, Job titles, Physical addresses, IP addresses, Employers, Dates of birth, Genders

[Verifications.io](#)

2 leaks

2 email addresses found in leaks:

ileslie@lclc.ca, info@lclc.ca

Leaked data in 2018

There were no 3rd party data breach events in your organization.

Leaked data in 2017 and older

Passwords, Email addresses

[8tracks](#)

1 leaks

1 email address found in leaks:

ckelly@lclc.ca

9 User Behavior

This section details risky behavior we've observed from individuals within your organization. We use open source intelligence to measure the cyber hygiene of user accounts. If compromised, these accounts could compromise your organization as well.



9.1 Password Quality

Using strong, unique passwords for all services can help prevent common criminal techniques such as 'brute forcing' or 'credential stuffing.' This section shows an analysis of the complexity and length of passwords found in data leaks for your organization.

Analysis by Characters

We recommend using longer passwords or passphrases, which are more challenging to guess or brute force.

No passwords were detected at this time.

Analysis by Composition

We recommend creating complex passwords that use a combination of alphanumeric characters and symbols.

No passwords were detected at this time.

9.2 Torrents

Torrent downloads are often illegal and very often bring files infected with malware into your network. In this section we list the torrents seen being downloaded by your assets.

Scan performed and no results were found.

What is Cyber Insurance?

Cyber insurance (a.k.a. Cyber Liability, Internet Liability, Electronic Media Liability, and Network Security & Information Security Liability insurance, among other countless monikers) helps companies weather the storm from many technology-based risks they face. This includes the risks associated with a company's information technology infrastructure and data that may be impacted by a systems failure, ransomware attack, funds transfer loss, or data breach.



Our coverage

We protect your entire business from today (and tomorrow's) cyber threats, with up to \$15 million of cyber and technology errors and omissions insurance coverage.

3rd Party Liability Coverages

We cover the expenses to defend you and any damages resulting from your liability to a 3rd party.

- 
Network & Information Security Liability

We cover the expenses to defend you and any damages resulting from your liability to a 3rd party, or for regulatory fines & penalties, multimedia wrongful acts (such as infringement, defamation, piracy, etc.), and PCI fines & assessments resulting from a failure in your security, data breach, or privacy violation.
- 
Regulatory Defense & Penalties
- 
Multimedia Content Liability
- 
PCI Fines & Assessments

- 
Bodily Injury & Property Damage - 3rd party












We pay for the costs of defense and damages from your liability to a 3rd party when a failure in your security results in physical damage or injury.

- 
Technology Errors & Omissions

We pay for the costs of defense and damages from your liability to a 3rd party when the failure of your technology service or product is the cause of loss.

1st Party Liability Coverages

We cover the direct expenses and damages your organization incurs as a result of a cyber incident.

 Bodily Injury & Property Damage - 1st party	<p>In the event of a security failure (i.e., physical cyber attack), we'll even cover losses resulting from bodily injury or damage/impairment to your tangible property, as well as damages resulting from any liability you may have to a 3rd party, including regulatory fines & penalties and pollution liability.</p>
 Pollution	
 Computer Replacement	<p>We cover the costs to replace your computer systems that are permanently impacted by malware.</p>
 Fund Transfer Fraud	<p>We pay for funds transfer losses you incur from a failure in your security or social engineering.</p>
 Service Fraud	<p>We pay for the additional amounts you're billed by a cloud or telephony provider when you incur fraudulent charges.</p>
 Digital Asset Restoration	<p>We pay for the costs to replace, restore, or recreate your digital assets that are damaged or lost following a failure of your security.</p>
 Business Interruption & Extra Expenses	<p>We cover financial losses resulting from a failure in your security, data breach, and even systems failure, as well as the extra expenses you incur to bring your company back online.</p>
 Cyber Extortion	<p>We cover the costs to respond to an extortion incident, including money, securities, and even virtual currencies paid.</p>
 Breach Response	<p>We pay for the costs to respond to a breach including 3rd party incident response and public relations experts, customer notification costs and credit monitoring, media purchases, and legal fees; and advise in connection with the incident, among others.</p>
 Crisis Management & Public Relations	
 Reputation Repair	

Global Coverage

Our coverage is global, providing you with protection from cyber threats near and far.



Worldwide Coverage



Cyber Terrorism



Internet of Things



Social Media

In the event of a security failure (i.e., physical cyber attack), we'll even cover losses resulting from bodily injury or damage/impairment to your tangible property, as well as damages resulting from any liability you may have to a 3rd party, including regulatory fines & penalties and pollution liability.

Our features

These are some of the tools available to help you improve your cybersecurity.

On-demand Support and Training



Security & Incident Response Team (SIRT)

Coalition is the only cyber insurance provider with a dedicated team of cybersecurity experts available to you at all times.



Security Awareness Training

Send simulated phishing tests targeting your own employees. Curricula's phishing awareness training simulates real-world phishing attacks, then trains your employees how to defend against them.

Proactive Monitoring and Alerts



Attack Surface Monitoring

Continuous monitoring, attack surface discovery, scanning, reporting, and alerting for organizations of any size.

Security Solutions



DDoS Prevention

Distributed denial of service (DoS) attacks attempt to make your Internet-based services inaccessible when you need them. Protect your websites and applications, and prevent disruptions from malicious traffic through our partnership with Cloudflare.



Endpoint Detection and Response (EDR)

Coalition offers a comprehensive threat detection solution, with a Coalition-negotiated discount, that includes protection from dangerous attacks such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions.

FAQs

Frequently Asked Questions about Coalition Risk Assessment.



Who is Coalition?

Coalition is the leading provider of cyber insurance and security, combining comprehensive insurance and proactive cybersecurity tools to help businesses manage and mitigate cyber risk. Backed by leading global insurers Swiss Re Corporate Solutions, Arch Insurance Group, Lloyd's of London, and Argo Group, Coalition provides companies with up to USD \$15 million of cyber and technology insurance coverage in all 50 states and the District of Columbia, as well as CAD \$20M of coverage across 9 provinces in Canada. Coalition's cyber risk management platform provides automated security alerts, threat intelligence, expert guidance, and cybersecurity tools to help businesses remain resilient in the face of cyber attacks. Headquartered in San Francisco, Coalition has presences in New York, Los Angeles, Chicago, Dallas, Washington DC, Miami, Atlanta, Denver, Austin, Vancouver, and Toronto.

How does Coalition determine my security ranking?

Our security ranking provides a relative measure of an organization's risk and security posture compared to other organizations we have evaluated. In order to determine the ranking of an insured, we correlate identified risk conditions with Coalition's proprietary loss and claims data. Unlike traditional security ratings, that make arbitrary assumptions on the relative impact of an identified risk condition to generate a security score, Coalition uses actual loss and claims data to identify the most significant risks to an organization. The result is not only a more accurate assessment of risk, but actionable prescriptions to help an organization invest its resources against the most impactful remediation actions.

Where does the underlying data from Coalition's risk assessment come from?

Coalition passively collects external data on an organization's Internet facing IT infrastructure, compromised system events, file sharing events, and configurations from many different sources. Coalition does not perform active collection of information, including penetration testing against an organization's networks, without the explicit permission of that organization.

How can I learn more?

To learn more about Coalition visit coalitioninc.com, or our knowledge base at help.coalitioninc.com. As a dedicated risk management partner to our policyholders, Coalition's team of security and insurance experts are committed to helping you implement security and loss controls, all at no additional cost.

Glossary

This section defines some of the terminology used throughout this report.

Asset

Web properties that your organization owns, such as an IP Address, Domain, or Subdomain.

Data breach

A cyber incident where your customer or employee data is accessed, and possibly exfiltrated, by a third party.

Domain

Web address associated with the organization. Example: coalitioninc.com

Hosting

Some type of hosting provider or hosting technology being used in one or more of your assets.

IP Address

An IP address associated with your company. Example: 1.1.1.1.

RDP

Remote Desktop Protocol (also known as a Remote Desktop or RDP) is a feature that enables employees to remotely log into their corporate computer from home. While it may be convenient for employees, RDP can also function as an open door for hackers to break into your corporate network.

Services

Technologies used to deliver services from your assets.

Secure Sockets Layer (SSL)

SSL is a cryptographic protocol designed to provide secure communications over a computer network.

Technologies

Technologies found being used in one or more of your assets.

Torrents

Torrenting is a peer-to-peer file-sharing mechanism whereby assets that are hosted on your computers may be downloaded by other people who are outside of your organization.



Cyber Risk, Solved.®

This assessment was prepared by
Coalition, Inc.
1160 Battery St. Suite 350
San Francisco, CA 94111

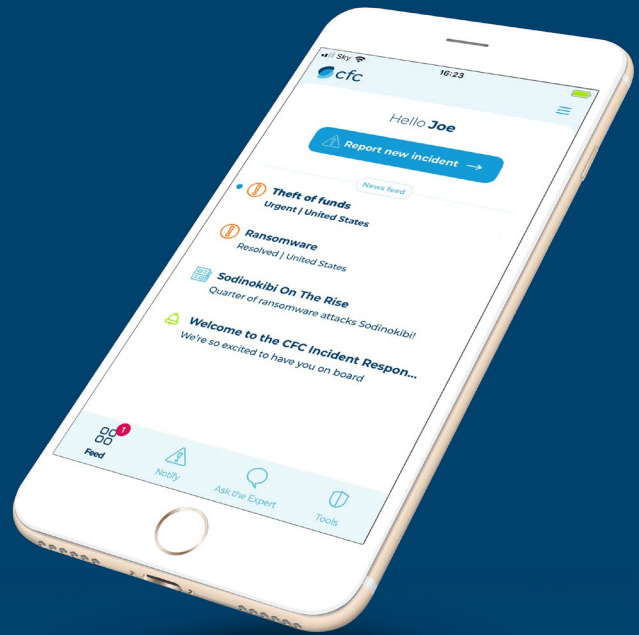
For more information, visit coalitioninc.com





Response

An integral part of our cyber policy, our award-winning mobile app *Response* gives policyholders access to a range of proactive cybersecurity tools and services.



Here's what this valuable tool has to offer:

Access to CFC's cyber risk management tools

- 1 **Phishing simulations** – Targeting members of your team whose credentials are the most vulnerable, these simulations send mock phishing emails in order to raise awareness of this criminal tactic.
- 2 **Dark web monitoring** – This tool scours the dark web for information relating to your business, including corporate login credentials and other breaches of sensitive data relating to your domain name.
- 3 **Deep scanning** – This service actively scans the external client network footprint to identify claims correlated vulnerabilities that lead to cyber attacks and ransomware.
- 4 **Cybersecurity advice** – The “Ask the Expert” section of *Response* allows users to get in touch with our specialist team for help with cyber risk mitigation, best practices, cybersecurity services on offer, and more.
- 5 **Real time threat alerts** – Through continuous monitoring of our customers and analysis of the latest cyber claims, our team is able to spot problems fast. Through *Response*, we send policyholders critical alerts specific to their business along with guidance on how to rectify any issues.

+ ... and instant notification of claims

Suffering an incident? The app allows you to instantly notify our specialist team if you have an issue. This feature of *Response* triggers an immediate call-back from our experience team of responders.

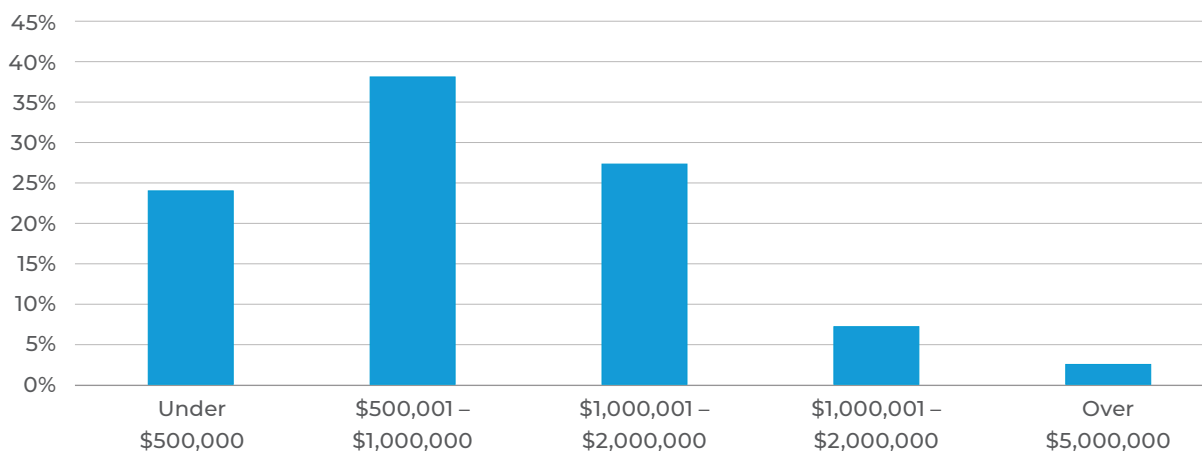


For a free trial, use demo code **DEMOCFC000** to register.
The app is available on the [App Store](#) or [Google Play](#).

Benchmarking

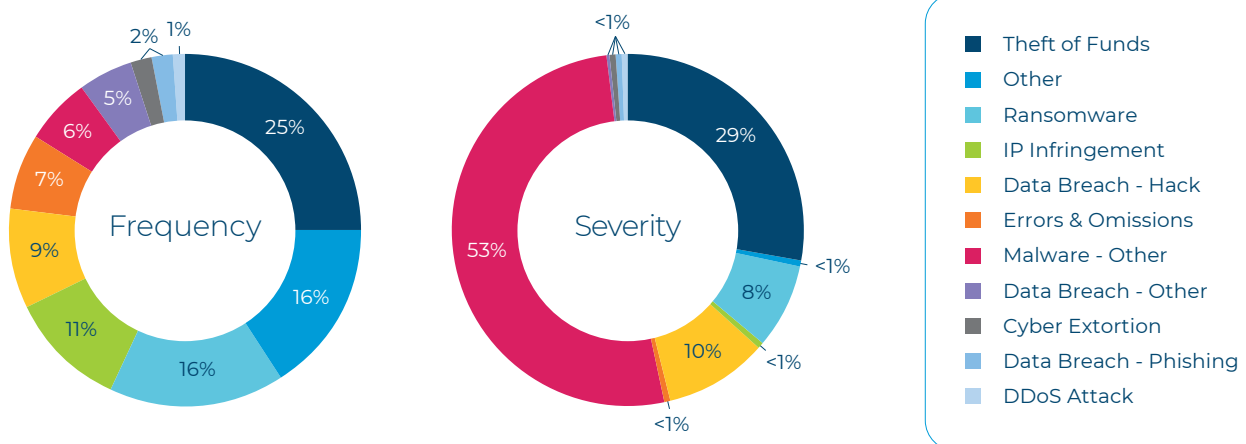
Limit profile

Interested to know what limits businesses like you purchase? Please find below data from current CFC policyholders that are within your direct peer group, showing their primary cyber insurance limits:



Claims profile

Interested to know what claims businesses like you experience? Please find below data from current CFC policyholders that are within your direct peer group, showing claims experience over the last two years, including the most common claims (frequency) and the most financially impactful (severity):



Case studies



Reputational repercussions

We look at how an online retailer of medical products suffered a business interruption loss as a result of notifying customers about a data breach.

The company's website was attacked by hackers who inserted malware on to the site and managed to gain access to a database containing the credit card details of over 90,000 customers. As there were local breach notification laws in place, all the affected individuals were notified of the incident and provided with identity theft restoration services. Immediately after the notification, however, the business noticed a significant drop-off in sales.

Following an investigation by forensic accountants, it was established that the insured had lost a total of 5,196 orders as a result of notification over a 12-month period, resulting in a business interruption loss of \$475,646. This came on top of the \$230,000 incurred to remove the malware from the business's website, provide legal advice and carry out the notification process.

[Read the full case study](#)



Poached payment

We look at how an insurance brokerage was impersonated by a cybercriminal who managed to trick one of the brokerage's customers into transferring funds into a fraudulent account.

The scam began when one of the brokerage's employees fell for a phishing email that resulted in the employee inputting his email login credentials onto a fraudulent site. With these credentials now at his or her disposal, the criminal was able to gain access to the employee's inbox and was able to impersonate the employee and trick the customer into transferring the premium for their insurance policy over to a fraudulent account.

Because it was the broker's email account that was compromised, the customer blamed the brokerage for the loss, and so the brokerage reimbursed the customer for the loss at a cost of \$14,850. Fortunately, the brokerage was able to recoup the reimbursement costs under their cyber policy with CFC.

[Read the full case study](#)



Kitchen calamity

We look at how a manufacturer of kitchen units was hit by a ransomware attack that left them without access to their computer systems for four working days.

During this time, admin staff were unable to book new appointments for sales staff on the CRM system, sales staff were unable to produce quotes for customers using Computer Aided Design (CAD) software and, as all the kitchen units are produced on a made-to-order basis, the manufacturing team could only work on those orders that had already been made prior to the ransomware attack, resulting in a significant drop in output.

This disruption resulted in a business interruption loss of \$130,959, on top of the \$38,371 incurred to deal with the incident.

[Read the full case study](#)



GM Report

Marketing

As our Events and Marketing Coordinator gets fully integrated into her role we are working on a Marketing Strategy (June Meeting) and Annual Marketing Strategy (July meeting) to direct our marketing efforts going forward. Throughout April and May Marketing has been largely focused on the campaign around the Craft Beer and Cider event, upcoming programs and the creation of the Rec guide content.

Events

May 14-15 will be the Provincial Cheerleading competition with over 1300 athletes competing.

May 21 Craft Beer and Cider Event is on track to be a success we have 18 vendors committed to the event, live music and food vendors onsite.

June 4th Michelin Tire Trot is a 5k race starting at the LCLC and 1k kids run.

June 18th the Michelin Junior Bike Event for children aged 5-11 will run in the LCLC parking lot.

June 27th Parkview Graduation

July 1st Benjamin circus (2 shows)

Hockey Canada has provided dates for the Canadian Tire Para Hockey Cup Nov.27 to Dec.3

With the formal announcement of the World Juniors we are working towards what hosting options may be open to the facility.

Facility Use

Our Spin Bikes arrived and are being assembled, lots of excitement about that increase in our program offering and the demographic it will attract. TOB Rec were planning to run an 8 week "Essentrics" exercise program, we worked together to bring it here and the program has been a great success, we will continue offering it on an ongoing basis.

Member Type	Members March	Members April	% Change
Adult	95	94	-1%
Adult Swim	18	15	-17%
Couple	40	40	0%
Family	517	550	6%
Family Swim only	22	18	-18%
Seniors	199	202	2%
Seniors swim only	84	81	-4%
Student	15	13	-13%
Youth	12	12	0%
Total	1002	1025	2%

Regional Collaboration

The Rec Guide partners are working towards alternatives to the current Rec Guide to find less expensive and more effective means of communicating that content.

C2R APP is moving from testing to going live, we have promoted the app in the Rec Guide and it will be available for the upcoming round of program registration.

Engineering Projects-

Everything is moving along on schedule, buffer tank has been delivered and installed, there are no anticipated equipment delivery delays.