Cyber Application for Small Businesses

Intended for our clients generating less than $100M revenues annually.

Network security and privacy liability

Client name:

Street address:

City: **Prov.:** **Postal code:**

Web address: **Client industry:**

Client contact: **Contact email:**

Revenues (CAD): **Last fully completed year:** $ **Projected annual figure:** $

No. of employees:

1. **Do you currently have cyber coverage in place?** ☐ Yes ☐ No
2. **Please advise approximate number of unique personally identifiable information (PII) records stored on your network, database or system (including those stored on your behalf of third-party networks):** Unknown
3. **If available, please advise exact number of unique PII records stored:**
4. **Do you collect personal health information (PHI) from your customers (excluding employees)?** ☐ Yes ☐ No
   If yes, please advise approximate number of unique PHI records stored on your network, database or system (including those stored on your behalf of third-party networks) Unknown
5. **If available, please advise exact number of unique PHI records stored:**
6. **Are you Payment Card Industry (PCI) compliant?** ☐ Yes ☐ No
7. **Are you involved in the direct supply of goods or services to the cannabis industry?** ☐ Yes ☐ No
8. **Are you involved directly with the use or supply of cryptocurrency?** ☐ Yes ☐ No
9. **Is your OT environment segmented from both your IT environment and the internet (if applicable)?** ☐ Yes ☐ No

Email security

10. **Do you pre-screen emails for potentially malicious attachments and links?** ☐ Yes ☐ No
11. **Do you conduct phishing training on an annual basis?** ☐ Yes ☐ No
12. **Are employees required to complete security training on at least an annual basis?** ☐ Yes ☐ No
13. **Do you require dual control when transferring funds in excess of CAD 25,000?** (Dual control refers to a process by which a transfer must be approved or confirmed by someone other than the initiator of the transfer.) ☐ Yes ☐ No

Multi-factor authentication

14. **Is multi-factor authentication (MFA) required for access to privileged user accounts?** ☐ Yes ☐ No
15. **Do you enforce MFA for all users, including third parties and those connecting remotely to the network?** ☐ Yes ☐ No

Encryption, endpoint protection, patches, and backups

16. **Do you have access control procedures and hard drive encryption to prevent unauthorized access on your databases, servers, and data files?** ☐ Yes ☐ No

17. **Do you use a paid-for endpoint protection (EPP) product across your enterprise?** ☐ Yes ☐ No

18. **Do you install critical and high severity patches across your enterprise within one month?** ☐ Yes ☐ No

19. **Are your backups kept separate from your network ("offline") or in a cloud service designed for this purpose?** ☐ Yes ☐ No

20. **Are all your backups taken monthly and stored on a separate device or service which cannot be accessed from your network?** ☐ Yes ☐ No

21. **Do you have procedures to back up, archive, and restore sensitive data and critical business systems?** ☐ Yes ☐ No

22. **Have you tested the successful restoration and recovery of key server configurations and data from backups?** ☐ Yes ☐ No

    If yes, how often are backups tested for restoration and recovery of key server configurations and data? Over 12 months

Media and miscellaneous

23. **Within the last three years, has the client been subject to any complaint concerning the content of its website, advertising materials, social media or other publications?** ☐ Yes ☐ No

24. **Do you have procedures in place to review media content prior to release on your website?** ☐ Yes ☐ No

25. **Does the client have procedures to remove content (including third-party content) that is libelous, infringing, or otherwise controversial?** ☐ Yes ☐ No

Loss history

26. **Has the insured had any prior cyber-related claims or incidents in the last five years?** ☐ Yes ☐ No

27. **Has the insured had any prior cyber-related claims where outside vendors were used for remediation?** ☐ Yes ☐ No

28. **Has the insured had any prior cyber-related claims where the costs incurred would have been above the retention of the cyber policy?** ☐ Yes ☐ No

29. **Has the insured had any legal action brought or threatened against them in the last five years as a direct result of a cyber event?** ☐ Yes ☐ No

If yes to any of the questions above, please provide details on the loss including the cost incurred and post-loss improvements that were implemented. Disclaimer: do not include items fixed in-house without cost.

Please provide any additional commentary on your risk posture:

This application must be signed and dated by a member of the control group. Control group means any principal, partner, corporate officer, director, member, general counsel (or most senior legal counsel) or risk manager of the insured organization, and any individual in a substantially similar position.

Signature: _____ **Date:** _____

Disclaimer: By signing this form you agree that the information provided is both accurate and complete and that you have made all reasonable attempts to ensure this is the case by asking the appropriate people within your business. Aon will use this information solely for the purposes of providing insurance services and may share your data with third parties in order to do this. We may also use anonymized elements of your data for the analysis of industry trends and to provide benchmarking data.

Privacy notice

The collection, use and disclosure of personal information through this site and Aon's services is governed by Aon's Privacy Policy http://www.aon.com/canada/about-aon/privacy.jsp.

Highlights

Aon collects, uses and discloses personal information:

- To determine eligibility and process applications for products and services and to provide information and services
- To understand and assess ongoing needs of clients and potential clients and offer products and services to meet those needs
- For communication, service, marketing, billing and administration
- For claims administration and data analysis
- For fraud detection and prevention
- For analytics purposes by aggregating or otherwise de-identifying personal information
- To develop proprietary tools and databases
- To provide consulting services to insurance companies
- To comply with legal, audit, security and regulatory requirements
- To obtain and update credit information with appropriate third parties, such as credit reporting agencies, where transactions are made on credit
- Other purposes disclosed in our Privacy Policy or our terms of business or disclosed to you at the time of collection, use or disclosure

Each Applicant authorizes Aon to collect and/or disclose the Applicant's personal information from/to third parties such as insurance companies, other brokers, adjusters, agencies, motor vehicle/driver licensing authorities and others as may be required for the above purposes. If the Applicant is providing any additional insured personal information, the Applicant providing this information warrants having obtained the prior written consent from each additional insured for the collection, use and disclosure of their personal information as set out herein.

Aon uses affiliates and/or third service providers. These affiliates and service providers may operate outside of Canada and, therefore, your personal information may be subject to the laws of other jurisdictions.

For further information, including how to contact Aon's Privacy Officer, please read Aon's Privacy Policy available at http://www.aon.com/canada/about-aon/privacy.jsp.

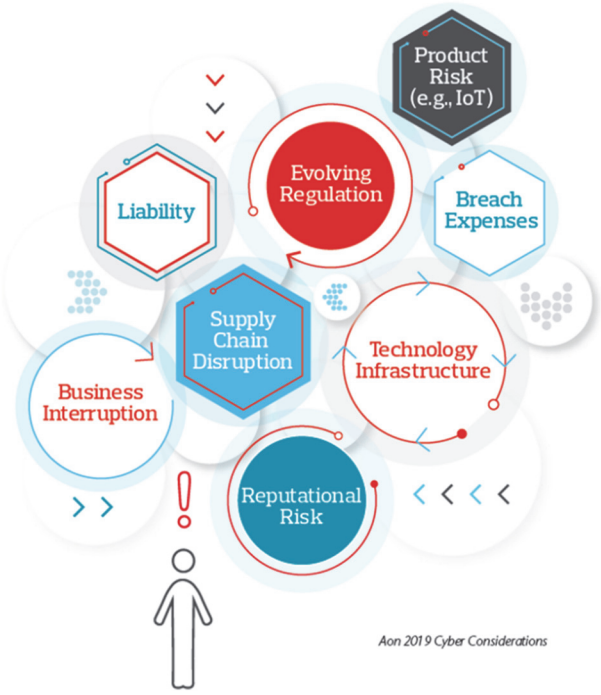
Setting the Scene…

~$600bn

Total cost of cybercrime in 2018

$2tn – $6tn

Total cost of cybercrime in 2022



$5.4M
Average cost of a data breach in Canada

$216
Average cost per lost record in a data breach in Canada

Average number of records breached in a single data breach in Canada
24,400

Average time to identify and contain a data breach in Canada
164 days (identify) **60** days (contain)

$4.24M
Global average cost of a data breach

$180
Global average cost per lost record in a data breach

Global average number of records breached in a single data breach
26,611

Global average time to identify and contain a data breach
212 days (identify) **75** days (contain)

Source: 2021 Ponemon Cost of a Data Breach Report

Canadian Cyber Market Snapshot

Claims and losses

Claims data is being analyzed as more breaches are being reported and remediated.

- Complexity of breaches has driven an increase in incident response expenses incurred by insureds.
- Increasingly punitive legal and regulatory environment.
- There has been a significant increase in frequency and severity of ransomware claims with some carriers reporting nearly 500% increase in ransomware claims. Currently this is the number one cause of the hardening of the cyber market.
- A recent vulnerability discovered relating to SolarWinds Orion Platform software has potential to be a systemic loss significantly impacting the global cyber insurance market.

Coverage

Insurers are evolving their policy wordings in light of claims experience to protect cyber portfolio profitability

- Coverage is starting to decrease as carriers being to implement sublimits to reduce amounts paid out following a ransomware incident. Coinsurance is also being imposed by some carriers all in an effort to help manage their exposure to ransomware loss.
- Exclusionary language to protect carriers from the impact of SolarWinds is also being explored.
- Insurers are differentiating their offering with prebreach risk management services and online information portals.
- Emphasis on pre-arranged claims response vendors, with some insurers stipulating use of their own vendors in order to control cost.

Capacity

Insurers are reviewing their capacity deployed, new entrants and exits common.

- Capacity is available globally: domestic, London, and Bermuda.
- Decreases in capacity may be seen where insured risk control metrics are subpar or insured participates in a high-risk industry sector.
- The impact of work from home and enhancements made by insurers to improve/elevate insured's cybersecurity measures are being reviewed and may affect deployment of capacity.
- Maximum capacity for primary placements is now capped at 5M. Excess capacity is required to access additional limits.

Retentions

Retentions are being reviewed.

- Retention can vary greatly based on industry class, size and unique exposures.
- Insurers are using retentions as a tool to manage claims experience and portfolio profitability.
- Minimum retentions are being set by insurers on a portfolio basis that are dependent on revenue bands and industry classes.
- Generally speaking, retentions tend to be increasing.

Pricing

The cyber market is hardening. We expect rates to continue to increase into the foreseeable future.

- Insurer's profitability has been materially impacted by the uptick in frequency and severity of ransomware incidents, as well as the recent SolarWinds vulnerability.
- Premiums are increasing, degree depends on industry, claims history and cyber risk posture.
- Required rate on lines continue to increase for excess layers.

Note: This is a general summary and could vary based on client industry and size.