VERSION 2.0

BOXX INSURANCE

CYBER BROKER GUIDE

PREDICT. PREVENT. INSURE.

www.boxxinsurance.com

PREDICT. PREVENT. INSURE.

MORE DATA, MORE INFO, MORE RISK.

Technology has revolutionized how individuals and businesses operate. Today's businesses handle vast amounts of interconnected customer, vendor, financial data and more.

And it's crucial for businesses to fulfill their public responsibility and legal obligation to keep this type of data secure, as cyber crime has grown substantially in the past few years, with global costs estimated to reach $10.5 Trillion by 2025.

Today's cyber criminals are constantly evolving how they attack their victims – and they are leveraging the very same technologies that have helped businesses become more efficient to compromise their systems and their data, like AI.

As cyber criminals become more opportunistic and innovative, data protection and cyber security is becoming a challenging task for many small businesses to manage on their own. And unfortunately, legislation, individuals and businesses often find themselves playing catch-up in the face of evolving cyber threats.

Because our digital fingerprints are everywhere, businesses must be aware of the operational, reputational and digital risks that they face. And this is where cyber insurance (like BOXX's all-in-one cyber insurance and protection that reduces risk for small businesses) comes in.

At BOXX Insurance, we are dedicated to supporting our broker partners and clients in managing today's evolving cyber risks.

This introductory guide to the current cyber risk landscape will enhance your understanding of the types of the digital and operational risks your business clients face. It also focuses on how BOXX's offerings not only insure them against cyber risks, but how our predictive and preventive led model will improve their security postures and reduce their chance of having to make a claim in the first place.

We'll also provide you detailed information on how you can communicate today's cyber risks to your clients and the benefits of having a cyber insurance policy.

THREE KEY FACTS ABOUT TODAY'S CYBER RISKS

FACT ONE: Small businesses are targeted 350% more than large enterprises by today's cyber criminals (Forbes)

Why would small businesess be a more frequent target of cyber criminals since they have smaller headcounts, budgets and revenues?

The reason is that they generally have lower cyber security postures and less sophisticated solutions and protocols to keep their information safe, making them easier targets to further cyber criminals' lucrative agendas.

Cyber criminals are targeting SMEs at an alarming rate to get access to their systems, their data and to halt their operations. Here's some data from a recent report by IBC that focused on the impacts of cyber crime on Canadian small businesses in 2021:

- 21% of Canadian small businesses were victims of a cyber-attack. Those with employee counts of 100-499 are significantly more likely to have suffered an attack.
- 78% have at least one type of cyber-attack defence in place for their business – and despite this, they would still be ill-prepared to negotiate with cyber criminals and address the fallout of an attack. 16% don't have any in place at all.
- 47% are spending "none" of their yearly budgets on cyber security, in 2019, only 33% weren't spending on cyber security. This is an alarming statistic, as cyber crime has ballooned 600% since the onset of the pandemic.

As an insurance broker, it's important to be armed with information that can help your clients understand the real risks of operating without cyber insurance and proper security protocols. Guiding them to make a decision with a clear understanding of today's cyber risks will prioritize the long-term health and safety of their business.

FACT TWO: Only 24% of Canadian small businesses have cyber insurance (Insurance Bureau of Canada)

And only 15% have a standalone cyber insurance policy.

This provides a big market opportunity for insurance brokers to protect their clients from ever growing cyber threats, and to grow your book of businesses in a growing field.

In 2020, the Canadian cyber insurance market recorded about $120 million in annual gross written premiums and it continues to grow with more offerings and players in the market.

Global figures show that the cyber insurance market size was valued at $13.33 billion in 2022 ad is projected to grow from $16.66 billion in 2023 to $84.62 billion by 2030, with a CAGR of 26.1% during the forecast period.

FACT THREE: Phishing, malware and unauthorized access are the leading cause of cyber attacks on Canadian SMEs (Government of Canada)

Through various methods, cyber criminals infiltrate businesses' systems by taking advantage of system vulnerabilties and/or human error by orchestrating sophisticated attacks against small businesses. Here's the most common tactics that cyber criminals use to attack Canadian small businesses:

Phishing attacks can trick your employees or executives into revealing sensitive personal data to a threat actor pretending to be another employee, a CEO or executive (known as "CEO whaling") and/or trusted vendor. And unfortunately, these types of attacks have increased in sophistication over the years due to social engineering strategies and email spoofing that make the messages look familiar or expected to the end recipient.

In addition to phishing, cyber criminals target businesses' employees through SMSishing attacks, where they send them urgent messages to reveal sensitive information to their personal phone numbers with data obtained from popular business directories like LinkedIn or ZoomInfo.

Malware is a malicious file or code that's been unwittingly loaded onto an employee's device with the intent to steal, infect or give an attacker control of the system.

Ransomware is a commonly used type of malware that locks down a computer system and encrypts its data. As a result, the cyber criminals then demand payment from the organization for them to regain access or prevent the attackers from selling it on the dark web or to other criminal organizations.

Malware and ransomware are generally installed on an employee's computer, unbeknownst to them, after they click on a malicious link or download an infected file, which are usually orchestrated through phishing and social engineering attacks.

Unauthorized System Access occurs when someone gains access to an organization's information, devices or networks without authorization. This can be caused by access to vulnerable systems, malware code or insider threats within the business itself.

CLAIMS SCENARIOS

How BOXX Helped an Unsuspecting Client Avoid the Crippling Cost of a Zero-Day Cyber Attack

The BOXX Hackbusters™ team responded to the news of a potential zero day incident risk by scanning all their clients' networks and informed those that were most vulnerable. Most of the clients followed the instructions that the Hackbusters provided, however one client denied they were at risk.

Fortunately, the Hackbusters guided them to an older server that had been turned on years ago for a specific project, but was never shut down. It turned out they had forgotten about this server and had it not been for the Hackbusters' intervention, they could have been vulnerable for a potential cyber attack.

How BOXX Helped Track Down Responsibility for Invoicing Fraud

Invoice fraud is one of the most common types of financial fraud. Recently, one of our clients' vendors paid a scammer an invoice they had issued – but when the client approached the vendor about the missed payment, they refused to take ownership of the error.

Using BOXX's Hackbusters service and expertise, our client was able to pinpoint the problem and resolve the payment issue. The Hackbusters team explained to the vendor that their systems were compromised by a social engineering attack and instead paid a scammer – and not their vendor.

As a result, BOXX's client didn't need to make a claim for any lost revenues.

> *"Our mission is to provide the most effective combination of cyber threat prediction, prevention, response, recovery and insurance coverage uniquely suited to small businesses at the most affordable price."*
>
> - ***Vishal Kundi, Co-Founder and CEO of BOXX Insurance***

BOXX INSURANCE

PROTECT YOUR CLIENTS WITH cyberboxx™ /BUSINESS

BOXX protects small businesses 24/7 with our all-in one cyber insurance protection and support from cyber security experts — just like the big guys. Here's an overview of the coverage and services provided:

Breach Response with the Hackbusters™

Breach response experts will contain the cyber incident and re-secure your network if needed.
No claim necessary.

Hacker Damage

Costs to repair, replace, or restore websites or electronic data

Insider Threats

Damages that result from malicious acts by an employee to either yours or any third-party system.

Cyber Deception

Money wrongly transmitted or paid to a third party from a deception scheme, also known as social engineering.

Reputation Damage

Coverage to help you manage your reputation following a cyber breach or attack.

Loss of Business

Lost profits if a cyber incident interrupts your business operations.

Legal & Regulatory Costs

Legal costs due to regulatory fines or requirements to notify customers.

Third-Party Liability

Costs associated with claims against you for a breach of any privacy law with respect to protection of third-party data.

Online & Media Liability

Protection if your online content infringes someone's IP rights, including defamation, libel, and slander.

Bricking Costs

Costs to replace damages to your hardware, in addition to replacement and recovery of data.

Cyber Services to Data Breach Victims

Costs of services to affected individuals including I.D. restoration management and additional services.

Notification Costs

Costs to provide notification of a Data Breach to affected Individuals.

BOXX INSURANCE

THE BOXX HACKBUSTERS™ IS AT YOUR SERVICE

BOXX's innovative PREDICT, PREVENT and INSURE model goes beyond traditional insurance by combining a mix of cyber threat prediction, prevention, response, recovery, and insurance coverage. When an incident occurs, the BOXX's Hackbusters team are on hand to contain the breach and minimize the potential damage – which quickly gets clients back on track.

Working in close coordination with globally recognized privacy and security providers and experts the Hackbusters' dedicated team of security specialists, risk management, legal, and public relations experts is at the client's side to contain a cyber incident and re-secure their network.

Get the details about our Cyber Insurance Coverage and Protection Services for Small Businesses

Reach out to a BOXX Representative here.

Virtual CISO

Add a Virtual Chief Information Security Officer to your team. Your in-house security team at a fraction of the cost.

BOXX Mobile App

The cyber protection app to monitor, preserve and enhance your business's digital health on-the-go.

Breach Response Services

Respond to and resolve business cyber incidents quickly with our expert Hackbusters™ team.

Employee Cyber Awareness Training

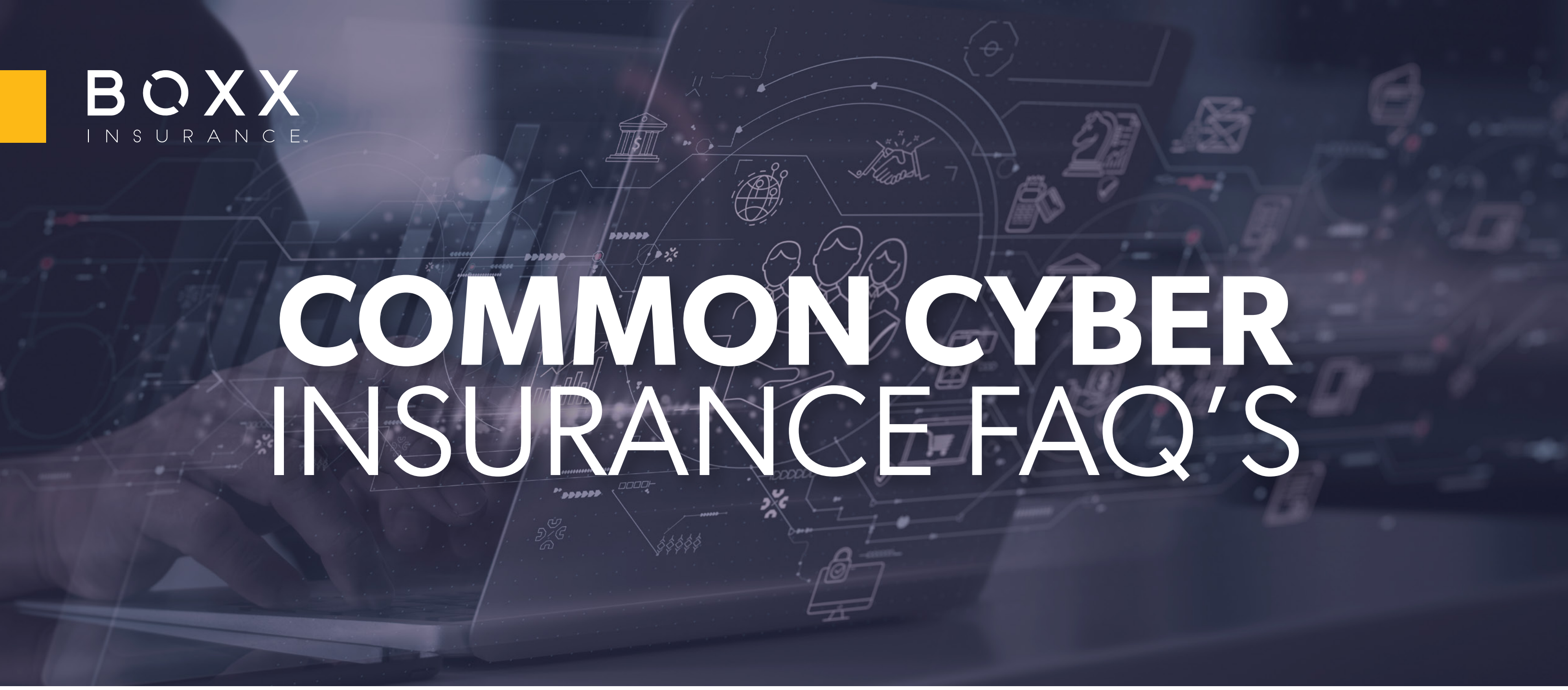
Strengthen your human firewall and raise cyber awareness across your organization.

Managed Firewall & Monitoring

Maintain your firewall and protect your network perimeter - BOXX provides professional-grade security firewall and monitoring services.

Data Back-Up & Recovery

Get professional data backup, protection and recovery services – 24/7 data safety and confidence.



COMMON CYBER INSURANCE FAQ'S

Our underwriters clarify common privacy exposure and coverage questions for clients and brokers regarding cyber insurance.

CYBER INSURANCE FOR SMALL BUSINESSES

1 I had a cyber liability endorsement added to my other policy. Isn't that enough?

Usually not. Most endorsements offer limited coverage with a small dollar amount. For instance, they may only cover first-party costs up to $20,000. A comprehensive privacy/data breach policy provides peace of mind, ensuring that the costs of a breach won't be catastrophic to your business.

2 Do I need a policy if my only exposure is first-party data?

Yes, all companies have a duty to protect employee and confidential business information. No company is immune to attacks. Our policy covers employee data and safeguards your business.

3 Why should I worry about cyber security if I'm not a high-profile target?

Small businesses often go unnoticed in the news, but the reality is that data breaches are a matter of "when," not "if." Hackers are constantly improving their skills, and there's a thriving black market for stolen records. Even large organizations with dedicated risk analysis departments have experienced breaches. Smaller companies without proper network security and resources become easy targets for hackers.

4 Why not trust my IT Department's assurance of security?

Even large companies like Target, with dedicated IT security departments, have suffered breaches. Simple errors, such as outdated software or weak authentication procedures for third-party vendors, can expose vulnerabilities. Lost unencrypted laptops or rogue employees with malicious intent can also pose significant risks. As technology advances, hackers become increasingly sophisticated, making it crucial to stay vigilant and take proactive measures to protect against cyber threats.

5 Do I need coverage if no client data is stored on my network?

Yes. It's access to client data that poses risk. Breaches may violate contracts. Our policies cover corporate info and employee data liabilities.

6 Is my (very) small company at risk of data breach?

All companies have data breach exposures, including employee info, payments, services, etc. Even small companies are liable for third-party data. Breaches cost an average of $188k, regardless of size. Costs escalate rapidly.

7 If my client information is stored in the cloud, the liability rests with the cloud provider, right?

Not necessarily. It's important for the insured to review contracts with legal counsel. Even with risk mitigation, the liability may still be the insured's responsibility.

CYBER EXPOSURES

1 What is a client's exposure?

Typical exposure includes personally identifiable information (e.g., employee SSNs, driver's license numbers, payment card data) and sensitive client data such as healthcare records.

2 Why do you need to know how many records a company has?

More records mean greater exposure and potentially higher post-breach costs.

3 What are the main types of cyber exposures small businesses need to be aware of?

First Party Exposures

Include any expenses triggered after a breach but not requiring a lawsuit:

- Computer forensics expenses (to identify the size and scope of a breach or loss of information) can vary greatly depending on breach size/complexity
- Notification of affected individuals
- Credit monitoring after loss of social security numbers is widely available on the open market at upwards of $20/year.
- Regulatory fines and penalties
- Public relations expenses
- Ransomware payments for cyber extortions
- Financial Fraud e.g. phishing payments

Understanding Regulatory Exposures

The landscape of federal and provincial regulations is constantly evolving based on new exposures and threats.

Canadian Federal Data Privacy Regulations

The legislation crafted by the federal government to protect individuals and their Personally Identifiable Information (PII).

The Personal Health Information Protection Act is a set of national standards to protect Protected Health Information (PHI). It applies to 'covered entities' and 'business associates' and considers any unauthorized access of PHI a 'breach'.

The Personal Information Protection and Electronic Documents Act (PIPEDA) is a Canadian law relating to data privacy.

What is Personally Identifiable Information?

Social security and driver's license numbers, bank account information, online account usernames and passwords, medical and health insurance information

As defined by PIPEDA, personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes the following type of information in any form, like:

- Age, name, ID numbers, income, ethnic origin, or blood type;
- Opinions, evaluations, comments, social status, or disciplinary actions; and
- Employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs).

CYBER INSURANCE COVERAGE

1 What is the difference between first party and third party coverage and when does it matter?

First party coverage includes costs incurred by the insured, such as breach notifications, forensic investigation, remediation, and business interruption. Third party coverage involves claims brought by external parties, like class action suits. Both are important in addressing different aspects of a cyber incident.

2 What is considered confidential corporate information if you exclude trade secrets?

Confidential corporate information includes non-public data that, if disclosed, could harm the business. This encompasses sales and marketing plans, product plans, design notes, customer and supplier information, financial data, and more.

3 What coverage should I consider?

Confidential corporate information includes non-public data that, if disclosed, could harm the business. This encompasses sales and marketing plans, product plans, design notes, customer and supplier information, financial data, and more.

4 What coverage should I consider?

Consider both first and third party coverage, which encompass notification expenses, forensic investigations, regulatory fines, public relations consultants, and third party claims, among others.

5 What limits should I consider?

The limits depend on the company's size and data sensitivity. Larger companies with extensive data holdings may require higher limits of coverage.

6 Does a cyber insurance policy cover the direct loss of funds?

Most cyber insurance policies focus on the loss of information rather than direct monetary loss. However, specific endorsements can be added to address this risk, especially in cases of cyber crime involving stolen banking credentials or social engineering schemes.

7 Does the policy cover 'social engineering'?

Some insurance policies cover the loss of data regardless of how it was obtained, including through social engineering attacks. However, it's important to review the policy wording to confirm the extent of coverage.

8 Does the policy cover a rogue employee event?

Most insurance policies cover data loss regardless of how it occurs, but some may exclude rogue employee events. However, our Cyberboxx insurance policy explicitly covers standard rogue employee events, subject to policy terms and conditions.

9 Does the policy cover paper records?

Most privacy insurance policies cover paper records, but it's important to review the policy wording. The Cyberboxx policy includes Personally Identifiable Information in any form under its coverage, whether it's in your possession or that of a third party for whom you're legally liable.

10 Does Hacker Damage cover the destruction of paper records or is it limited to digital assets only?

The Hacker Damage module specifically applies to "data you hold electronically." It does not cover paper records. This module addresses events like malicious authorized access to websites, intranets, networks, computer systems, and more.

11 Is coverage provided worldwide? What does that mean? Does the lawsuit need to be handled in a Canadian court?

Our coverage extends worldwide, but our jurisdiction in claims handling is restricted to the Canadian courts.

12 Does the policy cover offline exposures as well?

Yes, the policy covers both online and offline/paper data.

13 Can the cyber deception sub-limit be increased?

Yes, it is possible to increase the sub-limit, subject to underwriting by your BOXX Underwriter.

14 How can companies mitigate cyber risks?

- Foster a corporate culture that prioritizes cyber and data security
- Designate one person with ultimate responsibility for data privacy and security
- Implement employee training and awareness programs
- Strengthen contracts with vendors and business associates
- Identify and classify the organization's stored information
- Collect and retain only necessary personal information
- Review and update data security policies, plans, and procedures
- Continually assess risks and find ways to mitigate them through administrative, physical, and technical safeguards
- Prepare for data security incidents
- Mitigate risks with cyber insurance

BOXX INSURANCE™

PREDICT.
PREVENT.
INSURE.

www.boxxinsurance.com