Cornerstone insurance SERVICES INCORPORATED
Built on trust.

SWIFT Digital Insurance

IMPORANT INFORMATION

CYBER LIABILITY

*****This document is a generalized discussion of coverage. At all times, and in all instances, the coverage afforded by your policy is as described on your policy declaration and within the applicable policy wordings.*****

Cyber Liability Insurance is designed to protect businesses from the financial consequences of cyberattacks and data breaches. As businesses increasingly rely on technology and store sensitive information online, the risk of cyber threats grows. This type of insurance covers the costs associated with data breaches, cyberattacks, and other cyber-related incidents that can disrupt operations and harm your reputation.

Why Your Company Needs Cyber Liability Insurance

- **Data Protection:** If your business handles sensitive personal information (such as customer data, payment details, or employee records), you're at risk of a data breach. How many records containing personal information does your organization retain or have access to?
- **Cyberattacks Are on the Rise:** Hackers are constantly evolving their tactics to target businesses of all sizes, and these attacks can result in costly downtime, lost revenue, or reputational damage.
- **Regulatory Compliance:** Many industries require businesses to adhere to strict data protection laws. Failing to comply can result in hefty fines or legal penalties.
- **Business Continuity:** A cyberattack can halt your operations, leading to significant downtime. Cyber insurance helps cover lost income and recovery expenses.
- **Third-Party Claims:** If a breach affects your customers, clients, or partners, they could take legal action against your business for failing to protect their data.
- **Reputation Management:** The aftermath of a data breach or cyberattack can severely harm your company's reputation. Cyber insurance helps mitigate the costs of restoring your brand's image.

Common Types of Cyber Attacks Your Business May Face

- **Ransomware:** A type of malware that locks or encrypts a business' data and demands a ransom for its release.
- **Phishing:** A method of fraud where attackers impersonate trusted entities to steal sensitive information such as login credentials or financial data.
- **Data Breach:** Unauthorized access or disclosure of sensitive company or customer information, often by hackers.
- **Denial of Service (DoS) Attack:** An attack where the hacker overwhelms the company's website or servers with traffic, rendering them unusable.
- **Insider Threats:** A cyberattack that comes from within the organization, typically by an employee or contractor, either intentionally or due to negligence.

First-Party vs. Third-Party Coverage in Cyber Liability Insurance

First-Party Coverage

First-party coverage protects your own business from financial losses resulting from a cyber event that directly affects your organization. It covers the costs that you, as the insured party, incur due to a cyberattack or data breach.

Examples of First-Party Coverage:

- Data Breach Response: Costs related to notifying affected individuals, providing credit monitoring, and handling legal fees.
- Ransomware Payments: Expenses involved in paying a ransom to cybercriminals (if deemed necessary) and the cost to recover from the attack.
- Business Interruption: Coverage for lost revenue and operational costs if your business experiences downtime due to a cyber incident.
- Forensic Investigation: Costs associated with hiring experts to investigate the breach and determine the cause and extent of the damage.

Third-Party Coverage

Third-party coverage, on the other hand, protects your business from liability for damage caused to others due to a cyber event. It covers the legal costs, settlements, and damages if a cyber incident results in harm to clients, customers, or business partners.

Examples of Third-Party Coverage:

- Privacy Liability: If your company's data breach exposes customer or client personal information, third-party coverage helps cover the cost of legal defense and compensation for affected individuals.
- Third-Party Cyber Liability: Covers claims made by other businesses or partners if your cybersecurity failure results in their financial loss, such as losing access to critical systems or proprietary information.
- Regulatory Penalties and Fines: If your company violates data protection laws (ex: PIPEDA) during a cyber incident, third-party coverage may help cover the fines and penalties.

In short, first-party coverage helps your business recover from direct financial losses, while third-party coverage protects your company from legal consequences and damages to others that result from cyber events. Both are critical for comprehensive cyber protection.

Common Exclusions of Cyber Liability Insurance

Liability coverage contain exclusions. It is important to refer to your policy and its applicable wording to understand your coverage. In general, the following are some of the losses that are not insured unless expressed otherwise.

- **Employee Negligence**: If an employee unintentionally causes a breach, the coverage may not apply, especially if the employee ignored company protocols.
- **Intellectual Property**: Losses related to stolen or misused intellectual property, like trademarks or patents, are often excluded.

- **Pre-existing Vulnerabilities**: Cyberattacks that exploit known vulnerabilities that were not patched before the policy began might not be covered.
- **Physical Damage**: Cyber insurance does not cover physical damage to equipment or property. For example, if a hacker physically damages your office hardware, that would be outside the scope of cyber insurance.
- **War and Terrorism**: Attacks that are considered acts of war or terrorism are often excluded, as these are seen as large-scale, unpredictable events outside of a business's control.

Talk to your Broker:

As cyber threats become more sophisticated, protecting your business with Cyber Liability Insurance has never been more important. Whether you're facing a data breach, a ransomware attack, or a simple phishing scam, this coverage can help mitigate the financial risks and keep your operations running smoothly. Speak with your insurance broker today to find out how you can secure your business from the growing threat of cyberattacks.

Cornerstone insurance SERVICES INCORPORATED
Built on trust.

DEFINITIONS

SWIFT Digital Insurance

This list of coverages can vary depending on the insurer and the specific cyber liability policy, but these are common types of protection offered to businesses.

- **Data Breach Coverage:** *Covers the costs associated with a breach of sensitive customer or employee data, including notification and credit monitoring services.*
- **Ransomware Coverage:** *Pays for the costs associated with a ransomware attack, including ransom payments (if applicable) and recovery expenses.*
- **Business Interruption Coverage:** *Covers lost income and extra expenses due to a cyber event that causes operational downtime or disruption.*
- **Third-Party Liability Coverage:** *Protects against legal claims from clients, customers, or partners if their data is compromised or services are disrupted due to a cyberattack.*
- **Cyber Extortion Coverage:** *Covers expenses related to extortion attempts, including ransom demands and negotiation fees.*
- **Network Security Liability:** *Protects against claims arising from the failure to secure a network or systems, leading to a breach or loss of data.*
- **Media Liability Coverage:** *Covers legal fees and settlements related to intellectual property infringement, defamation, or copyright violations in digital media.*
- **Privacy Liability Coverage:** *Covers legal expenses and fines related to the violation of privacy laws, such as the unauthorized disclosure of personal data.*
- **Forensic Investigation Coverage:** *Pays for the costs of hiring experts to investigate a cyberattack, identify the breach, and assess damages.*
- **Legal and Regulatory Response Coverage:** *Covers legal costs, fines, and penalties for failing to comply with data protection regulations and laws like GDPR or PIPEDA (Personal Information Protection and Electronic Documents Act in Canada).*
- **Employee and Insider Threat Coverage:** *Covers damages caused by intentional or negligent actions of employees, contractors, or insiders leading to a cyber event.*
- **Social Engineering Coverage***: Covers losses caused by social engineering tactics, such as phishing or pretexting, which trick employees into revealing sensitive information or making fraudulent transactions.*
- **Reputation Management:** *Pays for the cost of public relations efforts to manage and mitigate damage to your business's reputation after a cyber incident.*