APOLLO

CYBER INSURANCE
from APOLLO

Cyber Insurance is a specialist insurance product used to protect businesses from Internet-based risks, and more generally from risks relating to information technology infrastructure and activities. As cyber risks evolve, this important coverage has never been more critical. (Refer to Cyber Quick Facts document)

The APOLLO product Includes enhanced liability coverage, comprehensive breach response coverage, and extensive service provider resources. When a cyber incident occurs, a Breach Coordinator is assigned to engage specialists to respond and provide full coordination and project management to resolve the crisis. (Refer to Breach Response document)

Eligible risks

This standalone cyber product has limits **up to $2M** and is available for companies with revenues up to $50M.

Key features and coverages

- **Privacy Regulation** - The coverage will pay for regulatory expenses incurred when the organization becomes legally obligated to pay a Privacy Regulation Claim. A Privacy Regulation Claim is a civil proceeding, civil investigation, or request for information brought against any Insured for an actual or alleged violation of any Privacy Regulation. It could be brought by a federal, provincial, local, or foreign government.

- **Ransomware Attack Coverage*** - A ransomware attack is the insertion of malware on a computer system that prevents or limits the ability to access data for the purpose of obtaining a ransom from the victim to end or remove the attack.

- **Social Engineering Fraud Coverage*** - A social engineering fraud attack is a scheme that intentionally misleads an employee into sending money or diverting a payment based on fraudulent information that is provided to the employee in a written or verbal communication such as an email, fax, letter or phone call. The loss is the actual money or securities transferred by the insured entity.

Other coverages included:

- Enterprise Security Event
- Crisis Management
- Fraud Response
- Forensic / Legal Services
- Public Relations
- Cyber Extortion
- Website Media Liability
- Business Interruption
- Data Restoration
- Telecom Fraud Coverage

Monthly pay option is available.

* Subject to eligibility.

Cyber Quick Facts:

- **1/3 of businesses and 1/4 charities** reported having cyber security breaches or attacks in 2019
- **Reported breaches are higher among medium businesses** (60%), large businesses (61%) and high-income charities (52%)
- **Average cost** of a breach reported is on the rise:
  - → $3.3k USD 2017
  - → 28% increase in 2018
  - → 32% increase in 2019 ($5.5k USD)
  - → 48% of companies lack staff with the technical, incident response, and governance skills needed to manage their cyber security
- **Average investment in cyber security per organisation is less than .01%!**

- Our biggest **line of defense** should be a combination of:
  - → Equipment
  - → Software
  - → Culture (Culture being #1!)
- **Human Fact:** Consistency works far better than Intensity! (Having a cyber security week once a year DOES NOT help you)

Cybercrimes are not JUST an IT Problem!

BREACH RESPONSE

Incident reported → **Initial Triage Call** → **Incident response**

24 x 7 Call centre	Breach Coordinator	Specialists	
• Receive first notification of a loss from a client • Appoint a Breach Coordinator to manage the incident	• Gather relevant information – "Fact Find" • Initial advice /immediate action plan • Engage specialists to initiate response • Provide full coordination and project management • Communicate and action to conclusion	**Forensic**	• Investigate and determine the scope of the breach • Advice on next actions
		Cyber breach response	• Resolve and report • Evaluation of loss • Preservation of data
		Notification	• Draft notification letter • Deliver notifications • Operate hotline and draft script
		Legal	• Access/prevent litigation • Representation if sued • Filed response
		PR	• PR response
		Stakeholder management	• Data protection, government, regulator, police etc.

Insights & Implications

- **High speed of response** to incidents is essential, requiring a global operating call centre to support clients 24x7.
- **Forensic investigations** are the most important services in breach response:
  - This identities, the scope and impact of breach, **affecting the scale and complexity of remediation plan associated costs.**
- **Good coordination between specialists** would help to deliver a holistic and smooth breach response solution to clients. This require an efficient and effective operating model, which is further described as part of the broader crisis management proposition.