DUAL

CYBER LIABILITY & DATA PROTECTION PRODUCT PROFILE

Put simply, Cyber Liability & Data Protection Insurance covers a business for the cyber exposures it faces.

What does it Cover?

Cyber Liability and Data Protection Insurance covers a business for the cyber exposures it faces from both third party claims (such as actions brought by the Privacy Commissioner, or clients suing for breach of privacy) and first party cover including Business Interruption and other expenses the Insured might incur as a result of a cyber attack. The first party expenses an Insured might incur include, but are not limited to, costs to repair or restore their systems, credit monitoring services if data has been breached, and public relations expenses.

What are the Key Elements of Cover?

1. First Party Costs

The Insured's own costs to respond to the breach, including but not limited to IT Forensic Costs, Credit Monitoring Costs, Cyber Extortion Costs, Data Restoration Costs, Legal Representation Expenses, Notification Costs and Public Relations Costs.

2. Third Party Claims

The Insured's liability to third parties arising from a failure to keep data secure, including data held on behalf of the Insured by either an outsourcer, or cloud service provider for which the Insured is legally liable. Coverage is available for claims for compensation by third parties, investigations, defence costs and fines & penalties for breaching the Personal Data (Privacy) Ordinance (Cap. 486).

3. Business Interruption

Reimbursement for the Insured's lost profits resulting from a Business Interruption Event. Unlike many of our competitors, coverage is not just limited to malicious attacks. Coverage is available for Business Interruption Loss arising from unauthorised access, any damage to the Insured's data (including data held on behalf of the Insured by either an outsourcer, or cloud service provider for which the Insured is legally liable) and/or programs, and any system outage, network interruption or degradation of the Insured's network.

4. Social Engineering, Phishing, Phreaking and Cyber Fraud

To protect you in the event of the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

4 Reasons Why SMEs are Easy Targets for a Cyber Attack

1 Lack of resources

23% of Hong Kong organisations have experienced a cybersecurity incident and 25% are not sure if they have had a cybersecurity incident as they have not performed a proper forensic or data breach assessment.* SMEs often lack the resources or expertise to understand their cyber exposures.

2 Less educated on cyber risks

13% of organisations who have encountered a cyberattack will consider cybersecurity at the start of a digital transformation project compared to the 43% of organisations who haven't. The remaining 44% do not think about cyber security at all.*

3 Weaker network security or IT infastructure

SMEs typically handle their own IT systems and security themselves, or outsource to someone as they lack the expertise.

4 SMEs hold valuable data

There is a common misconception that SMEs don't think they will be a target of cyber threats as they have no data or information that is of value or worth stealing. SME data is more valuable than people think. Even if the SME isn't the direct target, the SME might be a great pivot point into the integrated supply chain of their valued partners.

*Microsoft and Frost & Sullivan Study.

Claims Scenario

Background: A hacker impersonated a supplier of the Insured, using an identical email address. The hacker emailed the Insured advising that future payments should be made to a new bank account.

When the Insured was due to pay the supplier, they paid HKD205,000 into the fraudulent account.

Outcome: Indemnity was granted for the direct financial loss suffered by the Insured as there was Social Engineering, Phishing, Phreaking and Cyber Fraud cover under the Policy.

Payment: HKD205,000.

This document is only intended to be a summary of the highlights of the cover available. We encourage you to read the full policy wording for a full description of the terms and conditions. This policy summary does not form part of the policy terms and conditions.

Scary Statistics

27 hacking attacks on **12 licensed financial firms** in 2017 resulted in a **loss of HKD110 million**

- Microsoft and Frost & Sullivan Study.

3 out of 4 organisations in Hong Kong **have experienced job losses** over the past year **due to cyberattacks**

- Microsoft and Frost & Sullivan Study.

56% of organisations with fewer than 10 cybersecurity solutions **said that they can recover from cyberattacks within an hour**

- Microsoft and Frost & Sullivan Study.

Malware emerged as **the main form of attack in 2018** (52%) follwed by Phishing Email (49%). CEO Scams (35%), Other Malware Attacks including Botnet (25%) and DDoS (Distributed Denial of Service) (10%)

- HKCERT.

Over 9,000 cyberattacks were reported to Hong Kong Computer Response Team (HKCERT) in 2018, **an increase of 55%** from 2017

- HKCERT.

70 per cent of SME businesses have been **hacked** or had **data comprised**

- South China Morning Post.

Financial loss due to **Technology crime** in Hong Kong was **HKD2.7 billion**

Microsoft and Frost & Sullivan Study.

Hong Kong is in the Top 5 Global destinations to encounter a cyber attack

LexisNexis Risk Solutions

This document is only intended to be a summary of the highlights of the cover available. We encourage you to read the full policy wording for a full description of the terms and conditions. This policy summary does not form part of the policy terms and conditions.