



# 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 Protection Act 2012 (PDPA) or any other similar legislation applicable where the Insured operates.

#### 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

SMEs often lack the resources or expertise to understand their cyber exposures. 1/3 of SMEs report that they have no cyber protection\*. Singapore Police Force (SPF) report the growing threat to SME businesses in Singapore is e-mail impersonation scams. Victims may not realise their business partners' email address has been hacked or spoofed and follow directions to transfer funds. Normally these scams involve large sums of money.

## 2 Less educated on cyber risks

Cybersecurity is an afterthought in 25% of organisations who have encountered a cyberattack and 46% in organisations who have not encountered an attack\*\*.

\*Singapore Cyber Landscape 2017.  
\*\*Microsoft and Frost & Sullivan Study.

## 3 Weaker network security or IT infrastructure

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.

## 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 SGD41,000 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: SGD41,000.**

# Scary Statistics

**7 cases of e-commerce scams** are reported **everyday** in Singapore

- Cyber Security Awareness Alliance.

Singapore is ranked **1st in SEA** for experiencing **the most business email compromise attacks**

- 2018 Security Roundup Report by Trend Micro.

**33%** of organisations are **unaware if they have had a cybersecurity incident** as they have not performed a proper forensic or data breach assessment on their business

- Microsoft and Frost & Sullivan Study.

**Phishing** emerged as the **main form of attack** with **39%** reported to SingCERT in 2018, followed by Compromised Systems (21%), Ransomware (17%), Spoofed e-mails (11%) and Tech Support scams (6%).

**20%** of organisations **have experienced a cybersecurity incident**

- Microsoft and Frost & Sullivan Study.

**40% of cyberattacks** in Singapore **are aimed at SME's**

- Cyber Security Agency of Singapore (CSA).

