

Cyber Liability: It's All About Business Critical Protection February 2018



DUAL Asia – About Us

DUAL Asia is an insurance underwriting agency committed to delivering innovative insurance solutions in the Financial Lines area.

Since December 2012, DUAL Asia underwrites solely on behalf of MSIG Insurance (Singapore) Pte Ltd.

We specialize in Directors & Officers Liability, Management Liability, Association Liability, Educators Liability, Professional Indemnity, Information Technology Liability, Investment Manager Insurance and Cyber Liability and Data Protection.

When a cyber attack occurs, who's to blame?

There is no denying that cyber attackers should be held responsible.

However, within each organization, there is an excess of finger-pointing within the c-suite. 50 per cent of IT decision makers would blame their c-suite bosses in the event of a breach, and business leaders expect their IT department to take full responsibility for such incidents.

*Channel NewsAsia – Commentary: stop playing the blame game in a cybersecurity breach
19 December 2017.*

If you are a company director, you need to know that your company is under attack. It's not your fault but it is a problem you must deal with.

Cyber security is not a technical problem that should be left to IT to deal with, it's a business issue and you must be able to demonstrate due care.

- James Turner, founder and facilitator of CISO Lens

Why the need for Cyber Liability Insurance?

Cyber insurance addresses the first and third party risks associated with e-commerce, the internet, networks and information assets arising from:

hacking, viruses, programming errors, false or misleading online content and network or system failures, all of which may not be covered under traditional policies.

Examples of gaps in traditional policies:

- General Liability – do not provide coverage for damage to electronic data, criminal or intentional acts of insured or its employees, or pre-claim expenses (i.e, notification cost and regulatory defence)
- Property – limit coverage to damage or loss of use of tangible property resulting from a physical peril and at specific location. Usually excludes damage to data.
- Fidelity/Crime – limit coverage to direct loss from employee theft of money, securities or other tangible property. Usually exclude theft of data or information.
- Errors & Omissions/PI – limit coverage to claims arising from negligence in performing defined professional services. Usually excludes criminal or intentional act of insured or its employees and pre-claim expenses associated with a privacy breach (i.e notification cost and regulatory defence)

Watch a video on Cyber.....

Facts & Misconceptions

- Not “online” – no risk
 - Electronic files/records
 - Every business uses a computer or network
- Only big businesses at risk
 - SME’s are easy targets, they lack security measures of larger businesses
- Simple mistakes
 - Ever left your company phone, memory stick or laptop out at a bar or in a cab?
- Unanticipated breaches
 - Did you know photocopiers contain a chip that records scanned and printed data?

Evidence of the unpreparedness

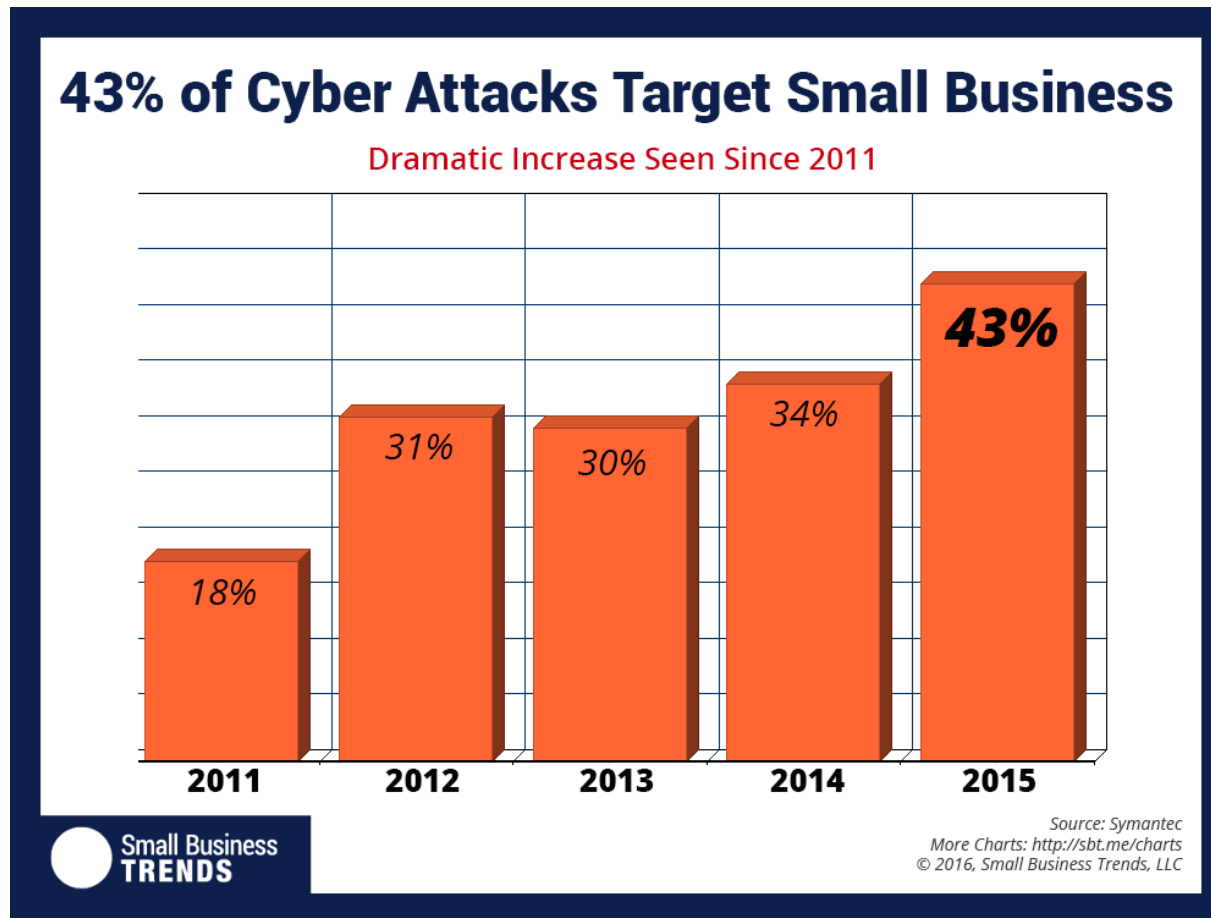
If large entities are vulnerable, what hope do SME's have?

- Petya ransomware disrupted Rosneft, Maersk, WPP, DLA Piper, Cadbury, more dangerous and intrusive as compared to WannaCry.
- WannaCry ransomware infected tens of thousands of companies in nearly 100 countries, disrupting Britain's health system and global shipper FedEx.
- Singapore MINDEF internet system breach, personal data of 854 national servicemen and employees stolen.

However, SME's were actually the most targeted organisations

- 60% of cyber attacks target SME's
- SME's lack the resources to invest in security

Who are the TARGETS?



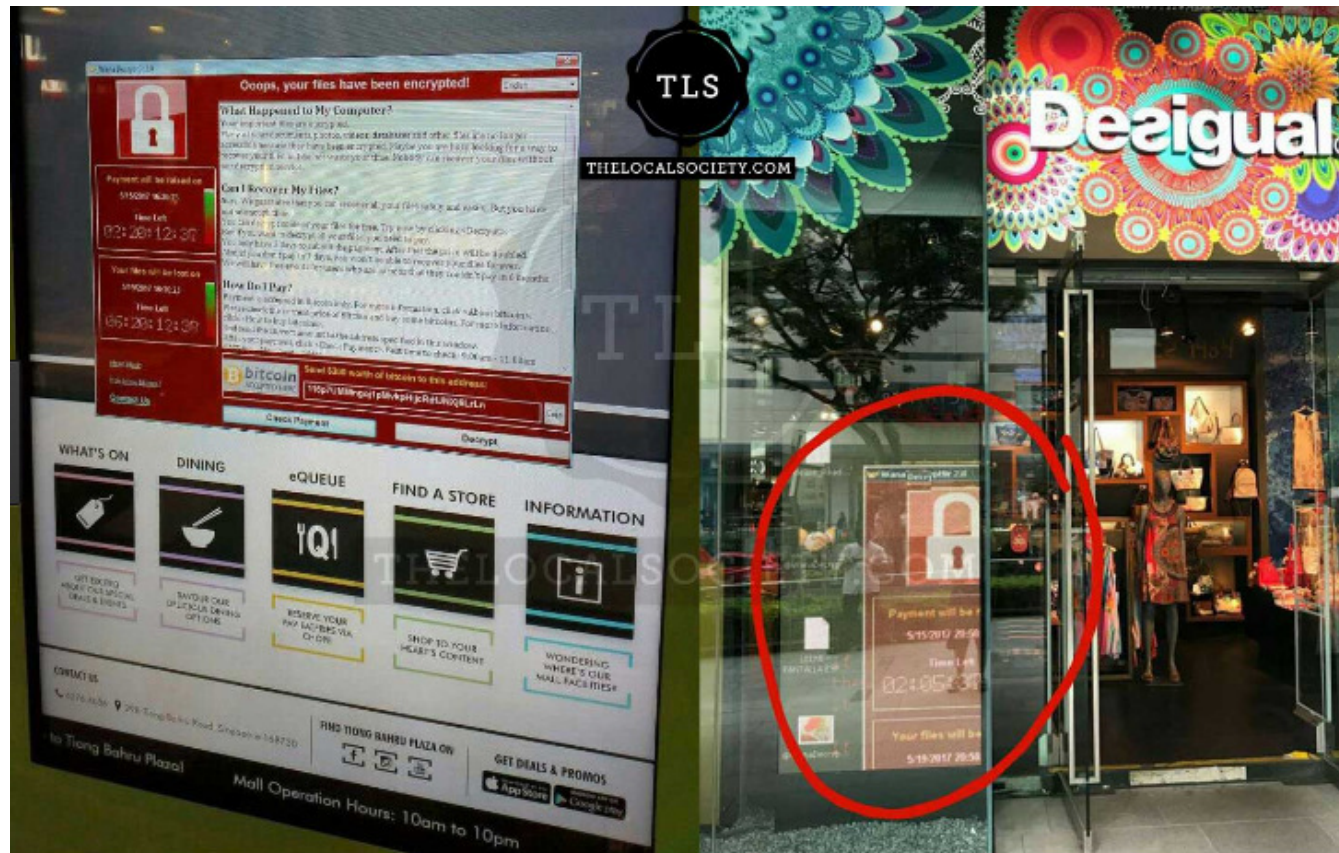
The Threat Landscape: SME's

- The critical exposure for SME risks and globally is not data loss or breach of privacy legislation....



Ransomware locally....

- Affecting Tiong Bahru Plaza and Desigual outlet



Employees are the weakest link in the company

Cyber extortionists tricked employees into opening malicious malware attachments to spam emails that appeared to contain invoices, job offers, security warnings and other legitimate files.

From: Tiffany&Co Jewelry Discount <news4@bigoff.net>

Date: 1 March 2017 at 6:34:46 pm AEDT

To: <mussher@dualaustralia.com.au>

Subject: Tiffany&Co Jewelry 80% OFF end today

Up to 50%-80% off storewide—Never miss

[View as a web page](#) | [Unsubscribe](#) | [Subscribe](#)

Now start the fantastic discount journey with us

TIFFANY & CO.

FREE SHIPPING WORLD WIDE

[HOME](#)

[BANGLE BRACELETS](#)

[CUFF LINK](#)

[EARRINGS](#)

[CONTACT US](#)

STOREWIDE
GREAT DISCOUNT

80%
OFF

SHOP NOW

Welcome to our Tiffany& Go online store. Here you can find all kinds of fantastic Tiffany& Go items. We promise our customers high quality and wholesale price. You can always find great discount here. Low price and fashion at the same time, you can realize this dream right here.

SHIPPING WORLD WIDE 5-7 DAYS

TIFFANY & CO.



TIFFANY & CO.



FedEx:Delivery problems notification



Kennedy <eliasi496@ekhn-kv.de>

Yesterday, 1:58 PM

You ↕



↩ Reply | ▾

This message was identified as spam. We'll delete it after 9 days. It's not spam

FedEx

December 27, 2013


Not possible to make delivery.

An package containing confidential personal information was sent to you.

[Delivery Manager](#)

◆ FedEx 1995-2013 | [Global Home](#) | [Terms of Use](#) | [Security and Privacy](#)

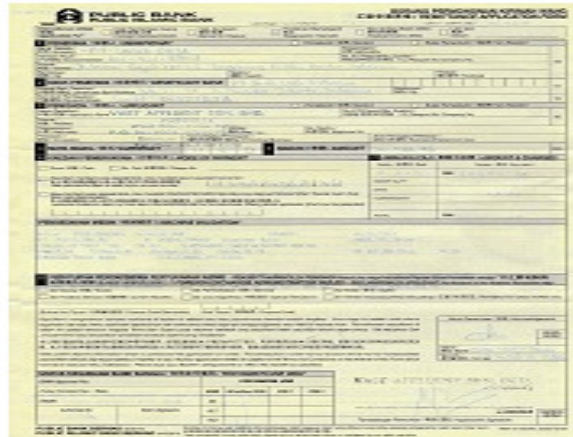
Possible SPAM: Payment Confirmation Advice on Premium
Hitesh Khristy <hk@indoarabre.com>

 You forwarded this message on 10/01/2018 11:47 AM.

Sent: Wed 10/01/2018 11:24 AM

To: Sebastian Phua

Retention Policy: Dual_Inbox_2Year_Delete (2 years) Expires: 10/01/2020



Hi

Find attached transfer sent out per our last transaction.

Payment # : 11100097
Registered on: 05.12 2017
Paid on: 02.01 2018
Payment Methode: Swift

Thanks & Regards



Hitesh Khristy
Executive Director
Indo Arab Insurance & Reinsurance Brokers DMCC, Dubai
P-10 Dubai Gate One Tower, Cluster Q, JLT
Board No: +971 4 4254327
Fax No: +971 4 3608518
Cambodia No: +855 70839174
Email: hk@indoarabre.com
P.O.Box: 380612 Dubai, UAE

WORST PASSWORDS OF 2017 Top 100



RANK	Password
1	123456
2	password
3	12345678
4	qwerty
5	12345
6	123456789
7	letmein
8	1234567
9	football

RANK	Password
18	dragon
19	passw0rd
20	master
21	hello
22	freedom
23	whatever
24	qazwsx
25	trustno1
26	654321

RANK	Password
35	daniel
36	andrew
37	lakers
38	andrea
39	buster
40	joshua
41	1qaz2wsx
42	12341234
43	ferrari



Major issues facing SME's

Causes of claims:

- Ransomware and cryptolocker
 - Over 1M new pieces of malware (i.e. a virus) are created everyday
- Server outages (network downtime from inadvertent or malicious)
- Phishing emails / Security Compromise – 23% of recipients open a phishing email and 11% click on attachments
 - Any fraudulent funds transfer loss is crime not Cyber

Most claimed sections:

- Business Interruption
 - Covers the loss of net profits and other related expenses to maintain operations
- Remediation costs
 - IT and forensic experts will charge hundreds of dollars to thousands an hour

1 Symantec, Internet Security Threat Report, 2016

2 Trend Micro and KSN Ransomware Report, June 2016

Why SMEs are most at risk?

- **Easy targets because:**

- Lack of resources
- Weaker Network Security / IT Infrastructure
- Less educated on Cyber Risks

Larger companies, government offices and Critical Information Infrastructure Operators have plans to minimise risk, said Dr Wong, but “the same might not be true for small and medium enterprises (SMEs) due to the lack of awareness, knowledge or expertise in cyber security”. These SMEs may become the weak link in Singapore’s cyber security efforts, he added.

- Seven Wong, President of Association of Information Security Professionals

Only 1 in 4 Small Businesses Well Prepared for Cyber Attack



Examples in the Public Eye

Critical hardware flaws put billions of computers and smartphones at data security risk.

Meltdown and Spectre

MELTDOWN



- Breaks down the most fundamental isolation between user applications and the operating systems.
- Allows a program to access the memory, and also the secrets of other programs and operating systems.
- If a computer has a vulnerable processor and runs an unpatched operating system, it is not safe to work with sensitive information without the chance of leaking the information. This applies to both personal computers and cloud infrastructure.
- There are currently software patches against Meltdown.

SPECTRE



- Breaks down the isolation between different applications.
- Allows an attacker to trick error-free programs, which follow best practices, into leaking their secrets.
- The safety checks in best-practice applications, in fact, make them more susceptible to the attack.
- Harder to exploit than Meltdown but also harder to mitigate.
- Possible to prevent specific known exploits based on Spectre through software patches.

Platforms affected

- Chips going back to 2011 were tested and found vulnerable, and theoretically it could affect processors as far back as those released in 1995.
- Because Meltdown and Spectre are flaws at the architecture level, all software platforms are equally vulnerable (a huge variety of devices, from laptops to smartphones to servers).
- Meltdown in particular could be applied to and across cloud platforms, where huge numbers of networked computers routinely share and transfer data among thousands or millions of users.

What can I do to protect my devices?

- The Cyber Security Agency of Singapore (SingCert) urged users to apply available security software fixes immediately.
- Intel said in a statement that it has begun providing software and firmware updates to "mitigate these exploits". All three major operating system makers – Microsoft, Apple and Linux – are also issuing updates.



Sources: CYBERSCOOP, TECHCRUNCH STRAITS TIMES GRAPHICS

Examples in the Public Eye

In most recent times, during Nov & Dec 2017:

- Online shopping service provider **ComGateway** and charity organisation **Credit Counselling Singapore** was fined \$10,000 each and social medial marketing firm **Social Metric** was fined \$18,000.
- Due to a vulnerability on ComGateway's shipping webpage, the personal data of 108,085 customers was vulnerable to unauthorised access and could have been harvested by a hacker.
- A staff member of Credit Counselling Singapore accidentally sent out a mass e-mail to 96 individuals under its debt management programme, exposing their e-mail addresses and names.
- Social Metric had "flagrantly" exposed the names, ages, e-mail addresses, contact numbers and occupations of 558 consumers, including the names and ages of 155 children, on its website without any password protection. Some of the data lay exposed for more than two years.

Examples in the Public Eye

Phoon Huat, a homegrown SME baking supplies company, hit by ransomware.

- Malicious software infiltrated their systems. No financial losses. Attackers were sniffing around to see what data they could access
- Attackers had access to image files (JPEG), which includes the company' invoices.
- Previous IT security systems were outdated and not patched since licenses expired.
- IT department only has 2 persons. No resources and technical skills to deal with security breach, despite having suspicious traffic on their network.

Examples in the Public Eye

Toh-Shi Printing Singapore

- Toh-Shi provides mail-out and data-printing services for Aviva.
- Sent erroneous account statements to Aviva Insurance policyholders under the Public Officers Group Insurance Scheme (Pogis).
- 8,022 individual personal data were leaked. This includes dependents data.
- Data are of sensitive nature, which can be socially embarrassing.
- Fined \$25,000 for failure to implement adequate checks in processing personal data.
- Staff had failed to comply with company's security measures and procedures.

Where are the laws heading?

Law on personal data may soon be revised to keep it in step with the rapidly changing digital landscape.

- Mandatory for companies that see breach of personal data to inform affected customers and the privacy commission
- Allow customers to change a leaked password or cancel a compromised credit card
- If breach involves 500 or more individuals, PDPC must be informed within 72 hours to manage breaches at national level
- If breach involves critical infrastructure, CSA must also be informed
- PDPC took enforcement action against 300 organizations till date

Straits Times – 28 July 2017

The need for Cyber Insurance - What does it cover?

- Third Party Claims
 - Claim for compensation including fines & penalties of privacy commissioner
- First Party Claims
 - Credit monitoring, Data Restoration, Forensic Consultant, Extortion Costs
- Business Interruption
 - We will put the Insured in the position they were in pre incident

Policy Coverage: 3rd party cover

- **Includes cover for:**

- ✓ Claims for compensation
- ✓ Investigations
- ✓ Fines & Penalties (where allowed by law)
- ✓ Defence Costs

- **Arising mainly from:**

- Data Liability Event – Loss of data / Breach of Privacy Legislation
- Network Security Event – Virus attack / Unauthorized Access / Fraudulent impersonation
- Media liability Event – E&O associated with materials distributed

Insurable risk categories for 3rd party cover:

- ✓ Media liabilities – harm suffered by others due to an infringement of an intellectual property right or display of any electronic media that results in defamation, slander, libel and etc
- ✓ Privacy liability – harm suffered by others due to disclosure of confidential information
- ✓ Network security – harm suffered by others due to a failure of the network security
- ✓ Virus transmission – harm suffered by others due to virus transmission
- ✓ Regulatory defence – privacy regulatory defence and penalties cover

- **Common claim:**

- Lose your iPad containing confidential client information.
 - The client sues you for breach of privacy, and
 - Client starts a smear campaign and attacks you on social media platforms (reputation at stake)
 - Investigation launched by the office of the Privacy Commissioner for Personal Data

Policy Coverage : 1st Party cover

- Includes cover for the Insured's own costs to respond to a cyber incident, including:
 - ✓ Credit Monitoring Costs
 - ✓ Cyber Extortion Costs
 - ✓ Forensic Costs
 - ✓ Data Restoration Costs
 - ✓ Legal Representation Expenses
 - ✓ Notification Costs
 - ✓ Public Relations Costs

Insurable risk categories for 1st party cover:

- ✓ Non-physical business interruption – business income that is interrupted by computer attack including PR expenses and notification expenses
- ✓ Data loss – forensic experts to help restore data stolen, destroyed or corrupted by a computer attack
- ✓ Cyber extortion – cover for extortion expenses such as ransomware
- ✓ Cyber terrorism – cover for income loss due to an act of terrorism

Cyber Extortion

○ Ransomware (or known as CryptoLocker)

- One form of cyber attack becoming more common on smaller companies.
- Hacker gains entry to a company's network, encrypts the data and makes them unusable, then demand a ransom from the company in return for an encryption key.
- Insurers see a 400 percent increase in ransomware breaches globally this year. Worrying trend.
- Cyber policy can **pay** the **ransom** or **extortion** to mitigate further threat or damage.

Your personal files are encrypted



Your files will be lost
without payment on:

11/24/2013 3:16:34 PM

Info

Your **important files were encrypted** on this computer: photos, videos, documents, etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key **RSA-4096** generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

See files

<< Back

Proceed to payment >>

Payment for private key



Private key will be destroyed on
9/20/2013
6:48 PM

Time left
71 : 57 : 22

Choose a convenient payment method:

Bitcoin (most cheap option)



Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send below specified amount to Bitcoin address **1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh** and specify the transaction ID, which will be verified and confirmed.

[Home Page](#)
[Getting started with Bitcoin](#)

Enter the transaction ID and press «Pay»:

2

BTC

<< Back

PAY



- **Common claim:**

- Your systems are hacked, client credit card data is stolen. We will pay:
 - ✓ Reimbursement of ransom payment to a hacker
 - ✓ Costs to notify all affected clients, and monitor their credit cards
 - ✓ Costs to repair your systems (not improve)



Policy Coverage: Business Interruption

- Reimbursement for lost net income, and
- Necessary expenses to maintain business operations
- **Common claim:**
 - Online retailers systems are attacked and the business is unable to trade, we will cover:
 - ✓ Lost net income from the interruption
 - ✓ Additional expenses such as additional call center staff to handle telephone enquiries from clients trying to buy online

Big Claims for small Companies

- **Profile:** Catering Company, 23 staff, \$2.6M turnover
- **Background:** An employee opened an email attachment that deployed a variant of ransomware malware. This resulted in the insured's network getting infected and forcing them to take their computers offline. It was also found that the ransomware had also encrypted majority of the company files. This resulted in critical network outage and the company wasn't able to process any new orders for next 3 days.
- **Response:** Forensic Investigators responded to the attack and cleanse the insured's network and systems of the ransomware and restored the system's data using the daily backups made by the company.
- **Payment:** \$55,000 in IT expenses and \$38,000 in lost revenue.

Target clients

- Companies that are highly dependent on technology to run their business and have an exposure to system disruption due to cyber attack against them.
- Companies that have a high profile and are therefore targets of theft or extortion incidents.
- Companies that hold, store, or transmit personally identifiable information. This could be customer information or even a companies' employee information.
- IN FACT, all companies that uses technology and collects any form of data should take up a Cyber Liability & Data Protection Policy, as this is a potential BUSINESS OPERATION RISK.



What happens when clients have a Claim / Incident?

Cyber Incident Hotline +65 3163 2126 cyber@ctplc.com



Cyber Offer

- Instant quotes and bindings for SME clients
- No proposal form
- Turnover up to \$50M
- Broad cover: Full sub-limits
- Premiums starting at \$900 + GST

CYBER LIABILITY & DATA PROTECTION INSURANCE OFFER

DUAL Asia designed this simple, instant quotation specifically for SME's. This offer is subject to the Underwriting Criteria and Pricing as noted below and cover will not commence until you have received written confirmation from DUAL Asia.

KEY ELEMENTS OF COVER

- Third party claims** from a failure to keep data secure, including claims for compensation, investigations, payment of fines and penalties. We will also pay defence costs and legal representation expenses.
- Business Interruption** - Reimbursement for net profits, as well as necessary expenses incurred to maintain operation of the business as a result of the interruption.
- Remediation Costs** - reimbursement of the Insured's own costs including credit monitoring, cyber extortion, data restoration, forensic, notification and public relations costs, and legal representation.

DEDUCTIBLE

- Waiting Period - 8 hours for Business Interruption

Revenue	Deductible
Up to \$1M	\$1,000
\$1M to \$3M	\$1,500
\$3M to \$5M	\$2,500
\$5M to \$10M	\$3,750
\$10M to \$20M	\$5,000
\$20M to \$35M	\$7,500
\$35M to \$50M	\$10,000

OPTIONS & PRICING

(based on past 12 months revenue)

Revenue	\$250,000 Limit	\$500,000 Limit	\$1M Limit	\$2M Limit
Up to \$1M	\$900	\$1,280	\$1,450	\$1,820
\$1M to \$3M	\$1,180	\$1,650	\$1,820	\$2,250
\$3M to \$5M	\$1,450	\$2,100	\$2,350	\$2,950
\$5M to \$10M	\$2,100	\$2,950	\$3,250	\$4,100
\$10M to \$20M	\$2,800	\$4,050	\$4,750	\$5,750
\$20M to \$35M	\$3,700	\$5,000	\$5,750	\$7,250
\$35M to \$50M	\$4,750	\$6,500	\$7,320	\$9,150

(All figures are in SGD and include GST)

COVERAGE CONDITIONS

- Period of Insurance - 12 months
- Retroactive Date - Inception
- Territorial Limits - Worldwide

DUAL ASIA
 4 Shenton Way #21-01 SGX Centre 2 Singapore 068807
 P: +65 6908 0558 W: www.dualasia.com
DUAL Underwriting Agency (Singapore) Pte Ltd

Insured by





MSIG

Cyber Bolt-On

from 1 February 2018

- Offered to insured at **NO** additional premium
- Bolt-on to Professional Indemnity / Information Technology / Directors & Officers / Management Liability / Association Liability / Educators' Liability
- Limit of SGD 100,000
- Deductible of SGD1,000

CYBER STAND ALONE vs CYBER RISKS EXTENSION

Cyber Stand Alone		Cyber Risks Extension
Broadform policy, includes cover for third party actions for: <ul style="list-style-type: none"> • compensation • investigations • payment of fines and penalties • defence costs • legal representation expenses 	Third Party cover	Only includes limited claims for compensation. Doesn't cover fines & penalties as a result of breaching the Personal Data Protection Act 2012 (PDPA).
Covers the Insured's own costs including: <ul style="list-style-type: none"> • credit monitoring costs • cyber extortion costs • data restoration costs • forensic consultants costs • notification costs • public relations costs, and • legal representation expenses 	First Party cover	Only covers: <ul style="list-style-type: none"> • costs to restore or repair systems from a hack attack, and • ransom payments to a hacker
<ul style="list-style-type: none"> • reimbursement for lost profits, and • necessary expenses incurred to maintain operation of the business as a result of the interruption 	Business Interruption	Not Included
Worldwide	Jurisdiction	Singapore only
Up to SGD\$10,000,000	Limit	SGD\$100,000

DUAL ASIA

4 Shenton Way #21-01 SGX Centre 2 Singapore 068807
 P: +65 6908 0558 W: www.dualasia.com
 Dual Underwriting Agency (Singapore) Pte Ltd

5 simple reasons to recommend & buy

- Cyber isn't just about hackers – privacy breaches due to employees' negligence happens more frequently than hacking
- Privacy Commissioner (PDPC) taking more enforcement action
- E&O Protection for Agents/Brokers/FAs – don't leave your client uninsured
- Business Interruption could cripple the insured
- New Revenue for the market
 - 215,000 SME's in SG - less than 1% buy Cyber



Tips for your clients

- Think before you click.
- Keep your computer software, hardware and device apps updated
- Do not post sensitive information on social media sites.
- Back-up.
- Create strong, unique passwords.



Any Questions?

Contact:

Sebastian Phua
Cyber Manager – Asia
Sphua@dualasia.com
+65 6908 0556

