



# Risk Transfer Solution – Cyber Insurance

*Lockton Greater China*



April 2022



# Table of contents

---

04

Lockton Overview

06

Cyber Risk and Regulations

07

Cyber Insurance

10

What can Cyber Insurance do  
in response to a data breach?

12

The current Cyber Insurance market

13

Practical tips on arranging Cyber Insurance in Mainland China

15

Our Team



# Lockton Overview

What makes Lockton stand apart is also what makes us better: independence.

We're purposefully unconventional, insatiably curious and **Uncommonly Independent.**

The 8,500+ professionals of Lockton Companies serve more than 65,000+ clients around the world with risk management, insurance, employee benefits consulting and retirement services. Lockton is the world's largest privately owned, independent insurance broker, with 2021 revenue of \$2.16 billion and offices on six continents, and we are recognized for our leadership and innovation in client service.

Despite our size and market dominance, we are most proud of the personal service we provide. You might think you're our only client based on the way your dedicated Lockton team will attend to your needs. You can count on our people to help make your business better.





Our independence lets us challenge the norms of what a brokerage can be. Our service-minded culture and entrepreneurial spirit foster innovation, creativity, and the ability to do what's best for our clients and their businesses.

### *What sets Lockton apart*

- 01 Lockton Associates demonstrate a **PASSION** for delivering service.
- 02 Our **ENTREPRENEURIAL CULTURE** rewards excellence.
- 03 Private ownership allows more **INVESTMENT IN OUR CLIENTS AND OUR ASSOCIATES.**
- 04 Marketing efforts are led by **SENIOR SERVICE TEAM MEMBERS.**
- 05 We maintain senior-level **RELATIONSHIPS** with the major domestic and international markets.
- 06 Our Associates have a passion for **MAKING OUR COMMUNITIES BETTER.**

#### LOCKTON BY THE NUMBERS

\$2.16B

2021 GLOBAL REVENUE

8,500+

ASSOCIATES WORLDWIDE

65,000+

CLIENTS WORLDWIDE

100+

OFFICES WORLDWIDE

97%

CLIENT RETENTION

13.4%

ORGANIC GROWTH

13

CONSECUTIVE YEARS AS  
BEST PLACES TO WORK

# Cyber Risk and Regulations

In addition to ensuring compliance, it is imperative to take into consideration on the risk transfer solutions to protect the company in the event of a cyber breach. With the growing implementation and enforceability of different cyber laws around the globe, can a multinational organisation be certain that their internal global policies do not deviate with their local cyber laws, not to mention China's Personal Information Protection Law (PIPL) and EU's General Data Protection Regulation (GDPR) which are applicable globally?

## SUMMARY OF CYBER REGULATIONS GLOBALLY



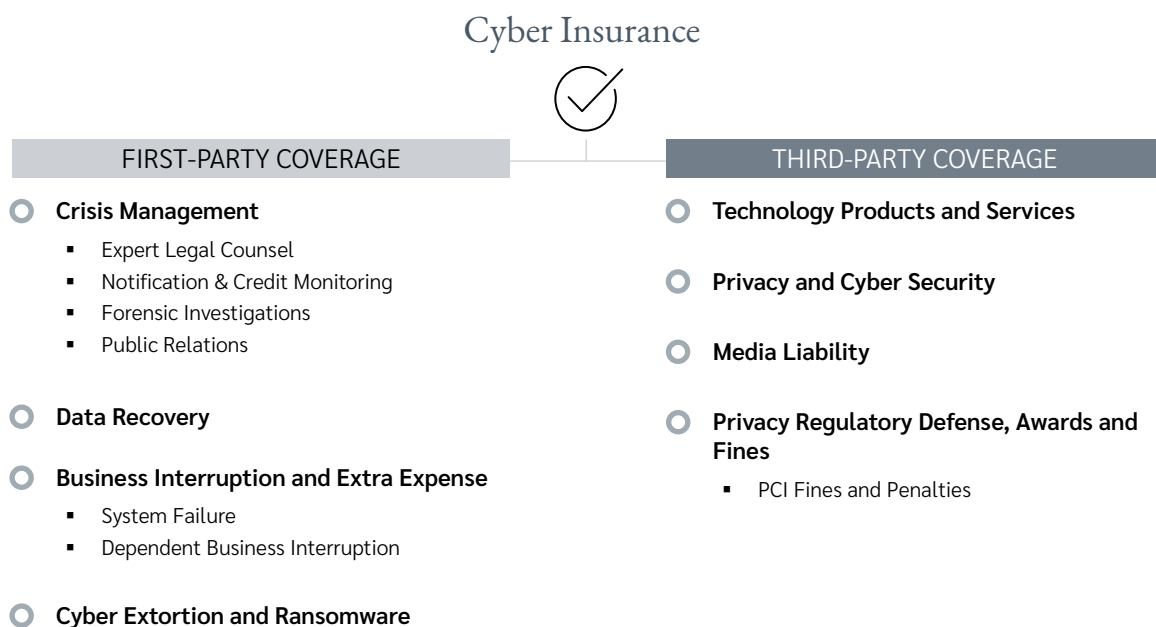
Source: Munich Re

# Cyber Insurance






The ramifications subsequent to a cyber breach / incident extends far beyond merely violating the PIPL and GDPR but threatening the organisations future business prospects, relationships and reputation:

- Reputational damage
- Disruption to business operations
- Legal and Regulatory costs
- Loss of business or investment opportunities
- Risk convergence and cascading effects
- Lawsuits and threat of lawsuits
- Damage to supplier or any third-party relationships






Given the extent of the loss potential, risk mitigation measures tend to protect first party (i.e. the organisation itself) risks while minimising the risks of third parties in taking legal action against the organisation. Thus utilising the company's resources to respond and tackle with these issues, a cyber insurance policy would provide coverage to reimburse the costs associated with these issues in order to keep losses suffered to a minimum. To gain a better understanding of what is covered within a cyber policy, an initial step is to separate the losses incurred into first party costs and costs which are borne as a result of damage done to a third party, namely third party and defence costs.



## FIRST-PARTY COVERAGE

				
<b>Breach response costs</b> <ul style="list-style-type: none"> <li>• Legal</li> <li>• Forensic costs</li> <li>• Mandatory notification costs (comply with security breach notification laws)</li> <li>• Voluntary notification costs</li> <li>• Call centre</li> <li>• Credit monitoring and/or identity monitoring/insurance</li> <li>• Public relations/crisis management costs</li> </ul>	<b>Cyber extortion</b> <ul style="list-style-type: none"> <li>• Reasonable and necessary expenses incurred as a result of a ransom demand due to the threatened release of PII as a result of a breach of a computer system</li> <li>• Reasonable and necessary expenses incurred to prevent or end an attack against a computer system</li> </ul>	<b>Network business interruption</b> <ul style="list-style-type: none"> <li>• Loss of net income and extra expenses as a result of a security failure of the insured's computer systems</li> <li>• Broader coverage available in the marketplace</li> </ul>	<b>Data restoration</b> <ul style="list-style-type: none"> <li>• Costs to restore or replace destroyed data as a result of a security failure of the insured's computer systems</li> <li>• Broader coverage available in the marketplace</li> </ul>	<b>Reputation harm</b> <ul style="list-style-type: none"> <li>• Loss of net income as a result of clients deciding to no longer do business with the insured following a cyber event where data is lost or stolen</li> <li>• Components of reputational harm coverage can be found within business interruption insuring agreements</li> </ul>

## THIRD-PARTY COVERAGE

				
<b>Network security liability</b> <ul style="list-style-type: none"> <li>• Claim expenses and damages emanating from network security breaches</li> </ul>	<b>Privacy liability</b> <ul style="list-style-type: none"> <li>• Claim expenses and damages emanating from a violation of a privacy tort, law, or regulation</li> </ul>	<b>Privacy regulatory proceedings and fines</b> <ul style="list-style-type: none"> <li>• Claim expenses in connection with a privacy regulatory inquiry, investigation, or proceeding</li> <li>• Damages/fines (varies by market) Consumer Redress Fund</li> <li>• Privacy regulations fines and penalties</li> </ul>	<b>Payment card industry data security standards liability (PCI-DSS)</b> <ul style="list-style-type: none"> <li>• Fines, penalties, and assessments that are incurred as a result of a breach of contract with a card brand or payment processor</li> <li>• Assessments can include fraud assessments, card reissuance costs, etc.</li> </ul>	<b>Media liability</b> <ul style="list-style-type: none"> <li>• Claim expenses and damages emanating from personal injury torts and intellectual property infringement (except patent infringement)</li> <li>• Claim expenses and damages emanating from electronic publishing(website) and some will provide coverage for all ways in which a company can utter and disseminate matter</li> </ul>



Despite the fact that cyber insurance equips an organisation with the cash flow required to recover from a cyber breach while the crisis management & IT-DR plans sets out the activities required, it should be noted that a cyber insurance policy also contains exclusions which may also be classified as a cyber related incident within an organisation's risk register, meaning that should these incidents occur, the cyber policy will not trigger and the organisation will have to bear the associated costs by alternative means. Some key exclusions captioned below:

- Conduct Exclusion (e.g. intentionally dishonest, criminal, fraudulent or malicious acts, wilful breach of duty, or attempt to gain a personal profit by an insured.)
- Bodily Injury and Property Damage
- Terrorism / War/ Governmental Acts
- Natural Perils e.g. electromagnetic fields, radiation, earthquake, windstorm, flood etc
- Infrastructure or Security Failure e.g. mechanical failure, electrical power interruption, outage to Internet access service
- Contractual Liability
- Prior Claims and Circumstances
- Trade Secrets and Intellectual Property
- Securities Claims
- Trading Losses/ liability

For example, monetary value of any electronic fund transfers by or on behalf of the Insured which is lost, diminished or damaged during transfer from, into or between accounts.

Different policy might have other different exclusions so do make sure to have a professional to go through your policy to ensure that your concerns are addressed.



# What can Cyber Insurance do in response to a data breach?

On top of the requirements set forth in the PIPL, cyber insurance as a risk transfer mitigation can critically assist an organisation when most needed. Most insurance companies provide 24/7 hotlines to align respective parties required to immediately deal with the situation, such as legal support, IT forensics and public relations in case the organisation is under media spotlight. As one of the requirements of the 3 China cyber regulations require reporting to the regulators within an 8 hour timeframe as well as remedial actions within 5 working days after investigation, the lack of resources and impaired systems may well impede the organisation's response within such timeframe, regardless of the level of sophistication of the organisation.



The following examples highlight the potential scenarios which may trigger a cyber insurance and may well formulate a subsequent violation of the PIPL:

Insuring agreement	Definition	Claim scenario	Coverage response
<b>Privacy breach notification</b>	Coverage for costs to notify and provide services to individuals or entities who have been affected by a data breach. Examples include call center services, notification, credit monitoring and the cost to purchase identity fraud insurance.	A fraudster hacks into the insured's internal processing system. Names, addresses and Social Security Numbers for more than 50,000 of the insured's customers are captured from the system, requiring notification to all 50,000 customers.	Costs to deliver notice to impacted customers, and to provide credit monitoring, a call center, and an ID fraud policy for impacted individuals.
<b>Cyber extortion</b>	Coverage for ransom and related costs associated with responding to threats made to attack a system or to access or disclose confidential information.	The insured's system is infected with a virus that encrypts the insured's data. A ransom payment is demanded to unlock the system.	Costs to manage and mitigate the incident, and if necessary, payment of the ransom demand.
<b>Data restoration</b>	Coverage for costs to restore or recover electronic data, computer programs, or software lost from system damage due to computer virus, denial-of-service attack or unauthorized access.	A computer virus corrupts the insured's software and data.	Costs for recovery and restoration of the insured's electronic data and computer programs.
<b>Public relations</b>	Coverage for public relations services to mitigate negative publicity resulting from an actual or suspected privacy breach, security breach, or media act.	The insured's chief financial officer has his laptop stolen. The laptop contains more than 100,000 customer records, including Social Security Numbers.	Costs for hiring a public relations firm to mitigate negative publicity generated from the incident.

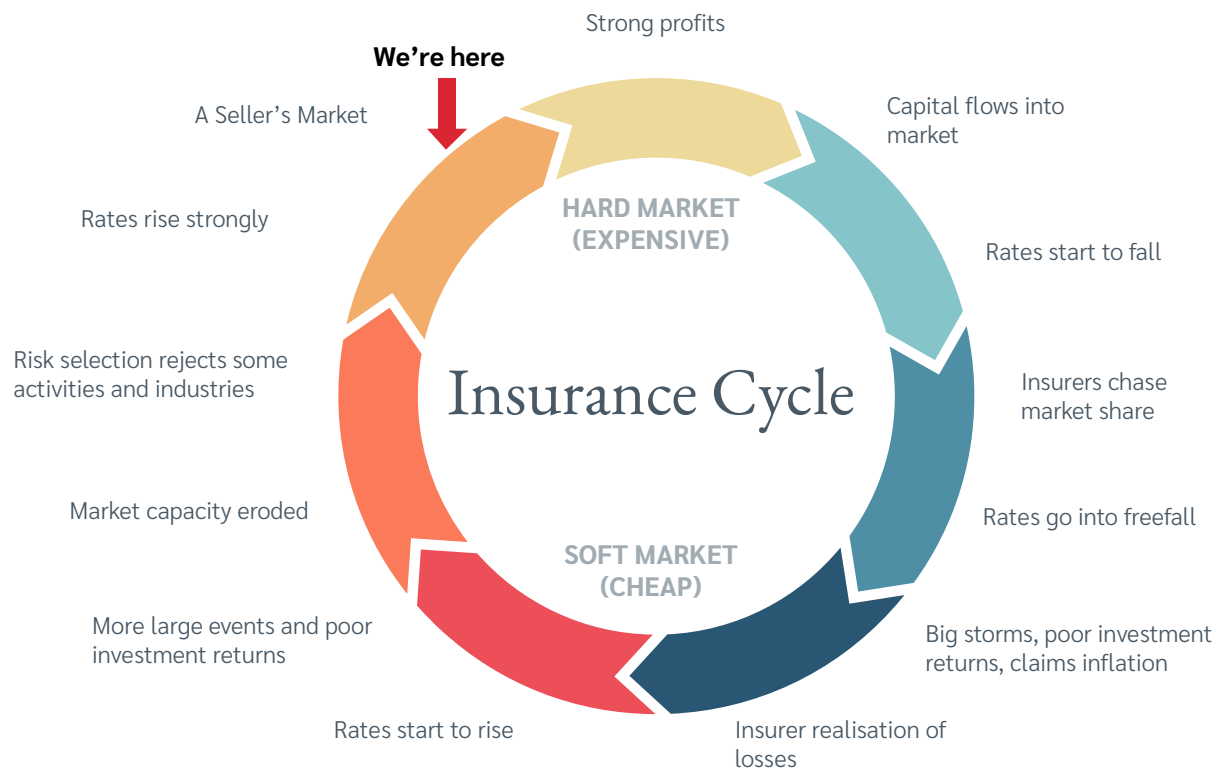
# The current Cyber Insurance market

Due to the prolonged global pandemic leading to a new WFH (Work From Home) culture, premiums for cyber insurance have increased the most for midsize and large companies, with estimated premiums rising by approximately 20%+ for this market segment.

Insurers in some high-risk sectors are reducing their exposure by reducing coverage limits or reducing coverages, and also placing lower limits on ransomware payouts (50% co-insurance clause). Some of the industries where insurers have reduced their exposures include health care and education.

Some insurers have been reducing their cyber risk exposure by adding more restrictive policy terms and including additional exclusions to their cyber and non-cyber policies.

Most insurers are limiting their risk appetite to US\$5m for new business and max. US\$10m for renewals.



# Practical tips on arranging Cyber Insurance in Mainland China

Although Cyber Insurance is not a mandatory class of insurance, many countries require that insurance held by companies operating in their jurisdiction is issued by local insurers, and subject to local laws and regulations. The insurance must be written on locally approved policy forms by an insurer licensed, registered or authorised to do business in the country where the insured risk is located.

Non-admitted insurance refers to the placing of insurance outside the regulatory system of the country where the risk is located.

A policy may be issued abroad, or a risk (Cyber) may be included in a global master policy, by an insurer which is not authorised in that country. An authorised insurer is one which is permitted to do business in a country (or region) by the local supervisory authority. The consequences for breach also vary between jurisdictions. Some examples will serve to highlight the complexities of the issue.

In some countries, for example the United Kingdom, Singapore and the USA, non-admitted insurance is permitted. In these countries the insured is generally free to purchase Cyber insurance anywhere it chooses. There may be a liability for premium taxes in the event of the purchase of non-admitted insurance but there is no prohibition per se. In other countries non-admitted insurance is prohibited and locally procured policies are required. Examples include China and India. In China, where admitted insurance is required, policies in breach may be declared null and void.

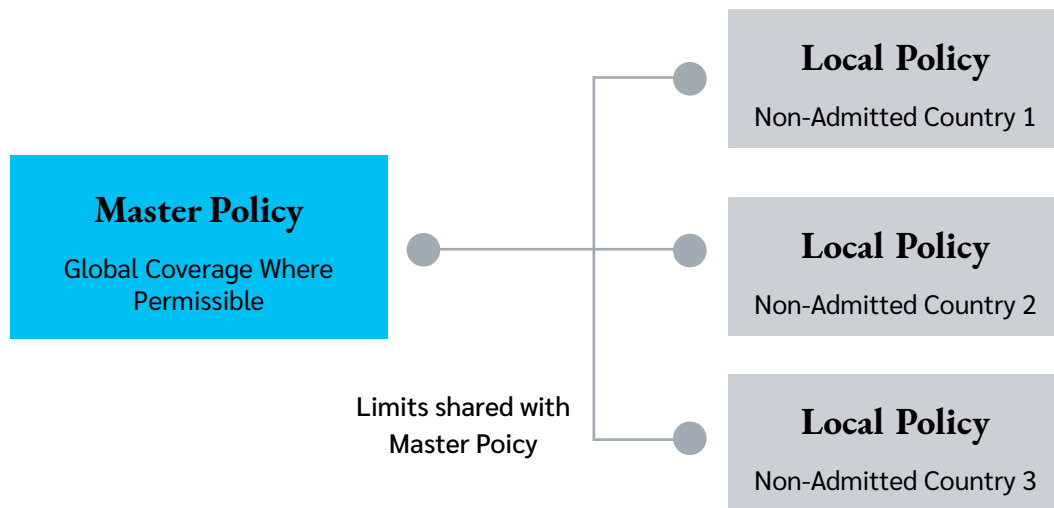
Due to foreign exchange controls that may exist, it may be difficult to repatriate claims payments. Collection from claims settlements paid by the parent company to a local subsidiary in a foreign currency, might be subject to conversion into local currency at an arbitrary rate resulting in a loss on exchange.

In the event a claim occurs in a country where non-admitted insurance is prohibited, the payment of the claim to the parent company, the foreign subsidiary or to a local director or officer of the foreign subsidiary, may be considered illegal and result in civil or criminal penalties.

Non-admitted policies attempt to escape local premium taxes – a situation which is looked unfavorably upon by local authorities and one that is being investigated vigorously in many territories. As a result, potential tax liabilities are becoming an important risk for buyers and providers of non-admitted insurance to consider.

In solving this dilemma, issue separate policies in foreign jurisdictions with shared limits, with a Parent Company Master Policy, where permissible.





The benefits of this program structure can be summarized as follows:

- The insured holds admitted policies that conform to local insurance regulations and industry practice, and are tailored to local laws and exposures with appropriate language
- The policies allow for locally allocated premiums and corresponding tax concerns
- The cost is less expensive than separate stand-alone policies due to the shared aggregate limit
- It involves relatively simple underwriting based on local revenues or headcount
- The local insured may have access to the parent company's policy limits via a difference in limits (DIL) feature in countries where allowed
- It allows for centralised coordination by both the insurer and broker thereby minimizing the administrative burden
- It also assists with local claims adjustment by providing a local claims representative who is an expert in the local jurisdiction

# Our Team



## Kegan Chan

Senior Vice President  
Head of Analytics - Greater China  
+852 2250 2867  
kegan.chan@lockton.com

### EXPERIENCE

Coupled with his consultancy experience in risk management (ERM/BCP/ORM/Cyber), Kegan has a proven track record in providing a holistic risk solution to corporations across multiple disciplines in both risk mitigation and transfer. Prior joining Lockton in 2021, Kegan was with Marsh for 10 years under various positions acting as a Team Leader under Marsh Risk Consulting and Analytics Leader in Asia for which he was responsible for driving and delivering risk consultancy & analytics' services across the region.

His diverse industry expertise span across a vast number of multinational conglomerates ranging from financial institutions, real estate, manufacturing, FMCG, telecommunications, hi-tech semiconductors, hospitality, etc.



## Melody Qian

Senior Vice President  
Head of Global Professional and Financial Risks - Greater China  
+852 2250 2672  
melody.qian@lockton.com

### EXPERIENCE

Melody was appointed as the Head of Global Professional & Financial Risk (GPFR) of Greater China team in May 2021. Melody has been specialized in Directors and Officers Liability insurance (D&O), Prospectus Liability insurance (POSI), Professional Indemnity (PI), Crime Insurance and Warranty and Indemnity Insurance (W&I) etc., and has served a wide range of industries including financial institutions, fund management, technology and e-commerce, biotech and pharmaceutical, manufacturing and etc. She also specializes in product design, coverage and policy drafting.

His diverse industry expertise span across a vast number of multinational conglomerates ranging from financial institutions, real estate, manufacturing, FMCG, telecommunications, hi-tech semiconductors, hospitality, etc.

For further information, please contact us at [enquiry.asia@lockton.com](mailto:enquiry.asia@lockton.com).



---

**UNCOMMONLY INDEPENDENT**

**LOCKTON COMPANIES (HONG KONG) LIMITED**

Office +852 2250 2828 Fax +852 22502038  
16/F, Berkshire House, Taikoo Place, 25 Westlands Road, Quarry Bay, Hong Kong  
Licensed Insurance Broker Company (Licence No. FB1055)

**LOCKTON COMPANIES (CHINA) INSURANCE BROKERS LTD.**

Office: +86 21 5081 2338 Fax: +86 21 5820 6260  
Unit A, 5/F, Lujiazui Finance Plaza, 1217 Dongfang Road,  
China (Shanghai) Pilot Free Trade Zone 200127, China

**GUANGDONG BRANCH**

Office: +86 20 3883 6066 Fax: +86 20 3891 1500  
Room1705, CITIC Plaza, 233 Tianhe N. Road, Guangzhou 510613, China

**LOCKTON COMPANIES (TAIWAN) LIMITED**

Office: +886 (0)2 2502 0566 +886 (0)2 2502 0599  
7/F, No 2, Section 3 Minseng East Road, Zhongshan District, Taipei City 104,  
Taiwan

**MACAU BRANCH**

Office +853 2850 9151 Fax: +853 2856 5120  
Avenida Comercial de Macau, n. 70, FIT Centre, 5 Andar A, Macau SAR  
Insurance Broker Registration No 26/CRE

**BEIJING BRANCH**

Office: +86 10 8514 1088 Fax: +86 10 8514 1086  
Unit 608 & 609, Tower A, Pacific Century Place,  
2A Gong Ti Bei Lu, Chaoyang District, Beijing 100027, China

**KAOHSIUNG LIAISON OFFICE**

Office: +886 (0)2 2502 0566  
4/F, No. 2 Zhongzheng 3<sup>rd</sup> Road, Xinxing District, Kaohsiung City 800208, Taiwan