



Cover your cyber risk.

One of the biggest threats facing businesses today is the dramatic rise of cyber extortion and ransomware worldwide and the Asian market has had its fair share of cyber attacks recently. The immediate impact of a cyber attack and its flow on effects can seriously hinder a company's ability to operate. Our cyber policy provides you with wraparound crisis management services that give you peace of mind in the the event of a cyber attack and the help you need to minimise the likelihood of an attack in the first place.

With our newly launched Cyber Liability Version 2 wording, your company is now better protected against the fast evolving cyber threats in today's environment. Coverage enhancements include new policy coverage (such as Reconstitution Costs, Social Engineering Cover, Reputation Harm and more) and broader definitions, to provide you a comprehensive 360 cyber protection on your business operations.

Speak to your Delta's Underwriter to find out more.

BENEFITS



24/7 rapid response from the top IT security experts locally and internationally

Immediately contain a cyberattack, restrict third party access & secure the perimeter of your IT infrastructure.



Cyber risk management specialists

We research and publish a white paper on the specific cyber risks and exposures in Singapore and highlight risk management practices that minimise the risk of a cyber attack.



Tailored Claims Response



Value-add risk management product suite

STATISTICS

Ransomware remains the most prominent malware threat for business

Datto, 2020



The average ransom fee has increased from

\$5k to \$200k

Due to COVID-19, malicious emails are up

600%

ABC News, 2021



Experts estimate that a ransomware attack occurs

Cybercrime Magazine, 2019

every 11 secs



Average downtime for a company after a ransomware attack is

*Source: Coveware, 2021

21 days

60%

of hacked companies had a loss of revenue after an attack

Cybreason, 2021, 2020



POLICY COVER

EXISTING COVERAGE UNDER VERSION 1

Business Interruption

Covers your loss of profits if your IT systems are attacked, the resulting in staff unable to work or customers unable to transact.

Third Party Liability

Hacked personal information to accidentally emailing confidential information, the policy covers any resulting claims

Hacker Theft Cover

This provides cover where funds are stolen as a result of your network being hacked.

Costs to Restore

Research, replace, restore or recollect software and any electronic data due to a network attack.

Data Forensic Services

Analysis of 'root-cause' using forensic techniques.

Network Extortion, Triage & Breach Consultation

When you notify a claim, we appoint an IT specialist or a law firm, depending on the nature of the breach. Our IT specialists prevent further attack, restore systems and deal with demands.

Notification Services and Credit Monitoring

Your customers can be notified if required and their credit history monitored to prevent damage from identity theft.

Mandatory breach reporting

Covers any government or privacy reporting required & media statement preparation where relevant.

Public Relations Expenses

Cyber breaches hit the press every day. Urgent action may be needed to manage your reputation should this happen to you.

WHAT'S NEW ON VERSION 2

Reconstitution Costs

Covers cost to employ specialist or overtime costs for IT employees to recover the company's network.

Reward Expenses

This pays for reward amount to seek for information which leads to arrest and conviction of the responsible threat actor.

Telephone Hacking

Reimbursement of cost due to unauthorised calls, usage of bandwidth or data as a result of your telecommunication system being hacked.

Social Engineering Cover

Covers you for costs incurred as a result of social engineering fraud impersonation.

Third Party Contractor Liability

The policy can be now extended to cover 3rd party contractor's liability which arises from providing services on behalf of your company.

Reputation Harm

Provides cover for business interruption cost due to adverse public relation.

Human Error

Policy covers for relevant costs and expenses as a result of errors and omission by an employee or 3rd party contractor in managing the company's network

Programming Error

Policy covers for relevant costs and expenses as a result of error in software programming affecting the company's network.

TERRITORY



> Worldwide

CAPACITY















\$25M

COVERHOLDER

Coverholder at **LLOYD'S**

CYBER RISK MANAGEMENT

CLAIMS HANDLING

| | Triage and forensic investigation | Data and system restoration | Public relations and notification services | Legal support | Loss assessment |
|---------------------------|---|--|--|--|---|
| Crisis Containment |  <p>Triage – identify problem and commission resources</p> |  <p>Prevent any attack or infection from spreading</p> |  <p>Initial PR response</p> |  <p>Appoint lawyers to ensure confidentiality & privilege</p> |  <p>Assess potential for cyber loss</p> |
| Crisis Management |  <p>Forensic investigation to establish extent of breach or loss</p> |  <p>Restore system and lost data</p> |  <p>Ongoing PR, notification to third parties, set up credit monitoring</p> |  <p>Communicate with affected third parties</p> |  <p>Investigate business interruption losses</p> |
| Crisis Resolution | |  <p>Review security & identify steps to reduce future incidents</p> |  <p>Ongoing credit monitoring</p> |  <p>Resolve third party claims</p> |  <p>Quantify and settle business interruption losses</p> |

POST-LOSS SERVICES

A cyber incident may have exposed weaknesses in your cyber security or incident response plan. You might also be vulnerable to further attacks by the same cyber criminals. In the right circumstances, part of our claims response may assist to link you up with our partners to help strengthen your cyber security baseline.