

WHAT ARE CYBER RISKS?



“A range of interlinked intangible (non-physical) risks that give rise to a wide range of first and third party exposures”

Examples of these risks include:

- Loss of intangible data
- Human error
- Employee sabotage
- Malware
- Denial of service attack
- Viruses
- Network downtime
- Cyber extortion

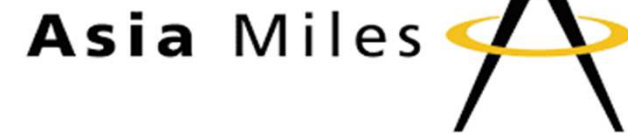
RECENT CLAIMS



香港大學
THE UNIVERSITY OF HONG KONG



香港中文大學
The Chinese University of Hong Kong



日本年金機構
Japan Pension Service



- **Key coverages include:**

- 1st party costs**

- Network interruption
 - Investigation
 - Legal representation
 - Fines
 - Public Relations
 - Notification & monitoring
 - Data reconstitution & forensics

- 3rd party liability**

- Personal & corporate data
 - Outsourcer liability
 - Data security
 - Defence costs

SHOW ME HOW CYBER INSURANCE WORKS

CASE STUDY: HOTEL CYBER BREACH



- Situation:
 - *A hotel was informed by their credit card processor that a number of credit cards used at their U.S. locations were fraudulently used elsewhere. Credit cards were potentially compromised from payment terminals at businesses within the hotel.*

SHOW ME HOW CYBER INSURANCE WORKS

CASE STUDY: HOTEL CYBER BREACH



- **Under this scenario the client incurred costs through:**
 - **Mitigation** - *Taking the appropriate course of action to identify the extent of the hack as well as containing it, then they incurred crisis management expenses in order to rapidly contact their customer base and outline their action plan.*
 - **Notification costs** – *The client incurred costs where they had to submit formal notifications to the respective affected persons.*
 - **Payment Card Industry assessment** – *The client was investigated by the Card Association and incurred a pecuniary fine.*
 - **Reputation** – *The breach was high profile and the client needed efficient and effective advice and action to mitigate damage to its reputation.*
 - **Third party damages** – *The client was exposed to third party damages from their customers due to the loss of data, breach of privacy and resultant settlement of damages.*

SHOW ME HOW CYBER INSURANCE WORKS

CASE STUDY: HOTEL CYBER BREACH



■ **How the policy responded:**

- **3rd Party Liability** - *Access to legal advice / other services and payment of judgments or settlements which the Insured is legally liable.*
- **Data Crisis Response** - *Access to advice / other services of legal or communications advisor(s) on how to handle an actual or suspected security breach or hacking event.*
- **Notification & Monitoring** - *Costs and expenses to disclose / notify a security breach or hacking event to the affected Individuals (includes identity theft education and credit monitoring costs).*
- **Payment Card Industry (PCI) Assessments** – *payment of written demand received from the Card Association for a pecuniary fine or penalty*
- **Pro-active Forensic Services** - *Costs and expenses to determine if a security breach or hacking event is occurring / has occurred, why it occurred, and how to prevent or reduce the security breach/hacking event in the future.*
- **Repair of the Company's & Individual(s)' Reputation(s)** - *Costs and expenses for PR consultants to help reduce damage, after an alleged or actual security breach or hacking event.*



THANK YOU & QUESTIONS

FOR MORE INFORMATION,
PLEASE CONTACT ANY OF
OUR OFFICES AND ASK FOR
THE FINANCIAL LINES
GROUP (FLG) OR JUST
SEND US AN EMAIL:

✉ **FLG@jltasia.com**

Alternatively, please visit our
website at www.jltasia.com