Panel Discussion on Making Sense of Cyber Risk

IFoA GI Asia/International Working Party

Peter Cashin (Partner, Kennedy's Law)
Allan Learoyd (SVP, Casualty Underwriting, Peak Re)
Chiew Yee Ng (Actuary, KPMG)

ASHK 3rd General Insurance Seminar
Friday, 19 October 2018

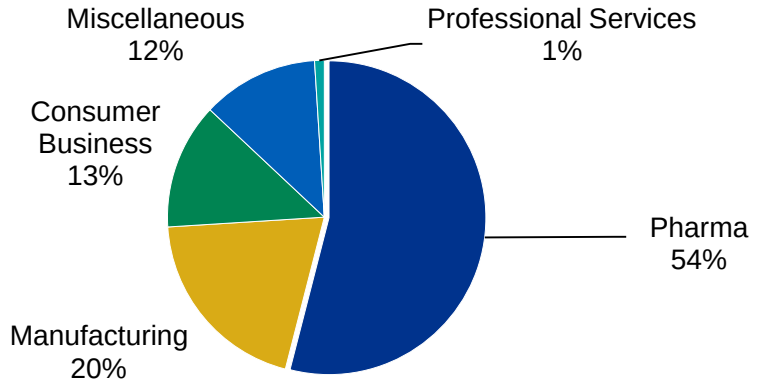
ACTUARIAL SOCIETY of HONG KONG 香港精算學會


MAERSK
MAERSK
SEALAND

The first major cyber catastrophe: NotPetya (June 2017)

- **NotPetya was:** A state-sponsored cyber attack on a Ukrainian accounting software firm. Designed to infect users and spread through corporate networks, corrupting equipment and deleting data.
- **What made this a catastrophic event?** NotPetya spread quickly, disrupting multinationals such as Maersk, FedEx and Merck
  - In various industries
  - Across geographical borders
  - Causing insured losses across multiple lines of business
- Many companies affected did not have standalone cyber cover. Pharmaceutical giant Merck was one of the exceptions.

NotPetya Projected Insured Losses by Sector



Source: PCS, A Verisk Business

Institute and Faculty of Actuaries

‘Silent cyber’ – cyber exposures within traditional P&C

- Traditional P&C insurance policies may not implicitly include/exclude cyber perils.
- Predominant driver of ‘silent cyber’ losses from the NotPetya event were Property business interruption losses – though some financial lines (E&O, kidnap and ransom) were also triggered.
- **Challenges**: customer demand for clarity of coverage, unknown exposures for insurers, increasing regulatory pressure

> “ The insured losses from NotPetya are estimated at **USD 3 billion**, with **~90% of the loss coming from silent cover**.
>
> *PCS Global Cyber Industry Loss Index estimate as at September 2018*

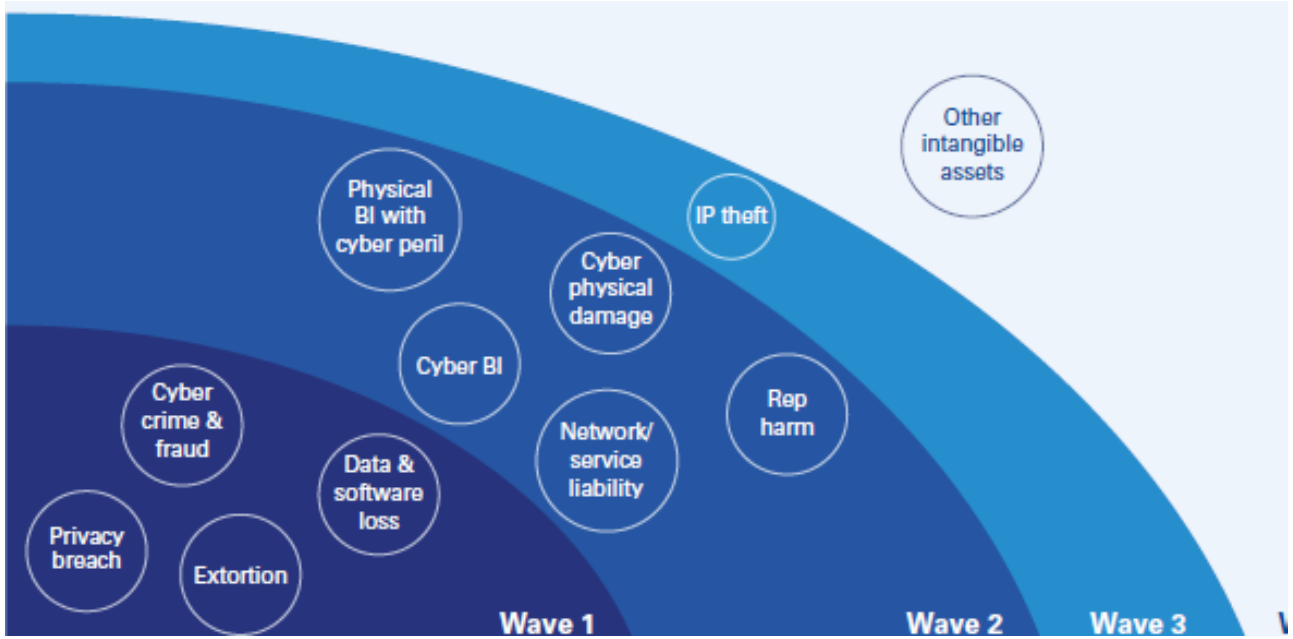
- **In which LOBs are ‘silent’ exposures material, given the exclusions / wordings in place?**
- **What can we do as an industry to address the risks arising from silent cover?**

Institute and Faculty of Actuaries

Affirmative Cover: Demand and Supply

- **Demand**: limited take up of standalone cyber cover.
- **Supply:** Standalone policies and extensions/packages.
  - Strong growth but divergent products…
- **Coverage** provided for losses to digital assets, for:
  - **First party costs**: Data/software recovery, crisis response, notification costs, ransom, cyber crime, business interruption?
  - **Third party costs:** liability for data breach, fines

Moving beyond 'basic' cyber cover…



Source: KPMG, Embracing the cyber insurance opportunity

- **Why don't more companies buy cyber cover, especially in Asia? What needs to change?**
- **How do 'value-add' offerings such as cyber incident response impact claims experience?**

Institute and Faculty of Actuaries

Development of the cyber insurance market

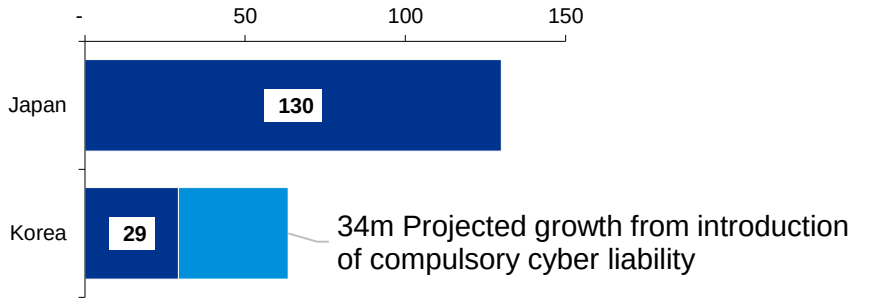
- **US market (USD 1.8 billion) is 90% of global premiums**
  - Chubb is the biggest writer in 2017
  - Loss ratio has improved to 32.4% (from 40s)
  - Despite 2017 events, both claim frequency and severity seem to have reduced

- **Asia (USD 100+m) : Little traction outside of Japan/Korea**

  Recent events (though no large insured losses):
  - Singhealth hack July 2018: 1.5 million records stolen
  - Taiwan Semiconductor Manufacturing Co (Aug 2018) virus outbreak: ~USD 170m in lost revenue

> “ Cyber is **three times more expensive than General Liability**, and six times more expensive than Property”. **Acquisition costs** for cyber products are at an estimated 40%”.
>
> *2018 London cyber insurance conference panel*

Cyber Premiums in Asia (USD m), 2016



Source: Japan External Trade Organisation (2016), Axco

Institute and Faculty of Actuaries

Data protection & cybersecurity regulations on the rise

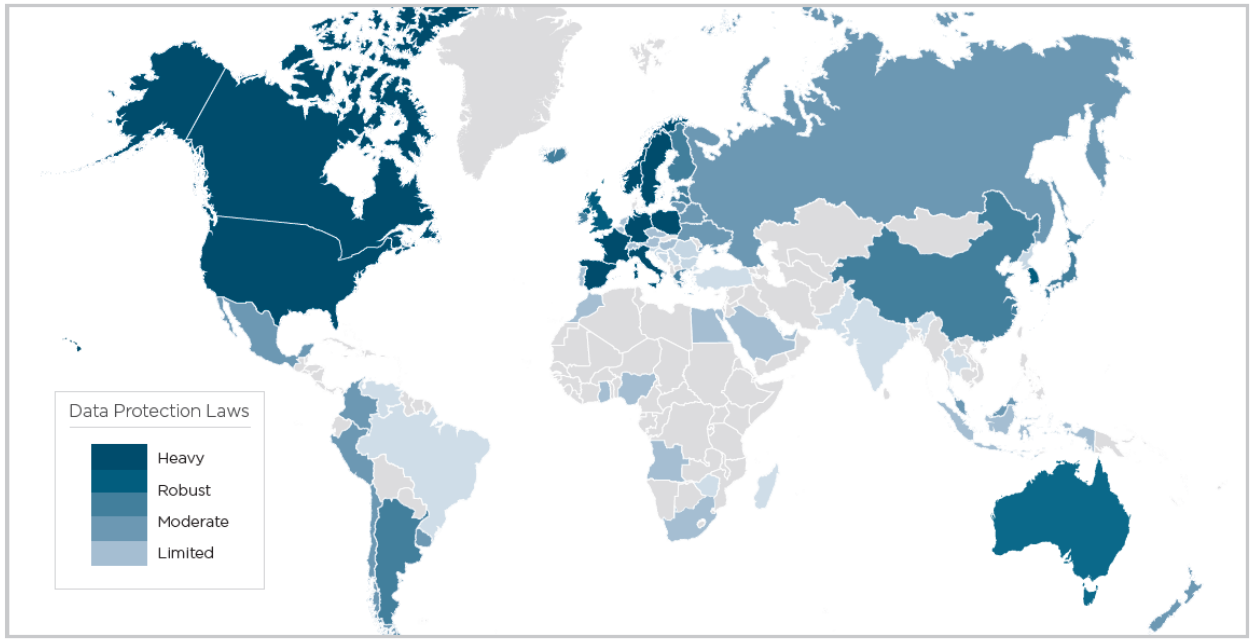


Figure 2: World Map of Data Privacy Regulation (Source: DLA Piper)

Extracted from RMS Cyber Risk Outlook 20180305

- UK: GDPR expected to drive frequency/severity of cyber claims
- Singapore: MAS Cybersecurity Bill, Personal Data Protection Act 2014, currently consulting on legally-binding cyber hygiene requirements for Fis
- Hong Kong: Personal Data (Privacy) Ordinance 2016
- Korea: compulsory cyber liability insurance introduced in 2016
- China: Cybersecurity Law 2017
- Malaysia: National Cyber Security Act, Personal Data Protection Act 2010
- Australia: Various laws from Australia Privacy Commissioner and APRA

- **What are the implications of the rise in cyber hygiene regulations / guidelines?**
- **Can/should compliance with regulations be used as a condition of coverage, or rating factor?**

Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

Discussion

- **In which LOBs are 'silent' exposures material, given the exclusions / wordings in place?**
- **What can we do as an industry to address the risks arising from silent cover?**
- **Why don't more companies buy cyber cover, especially in Asia? What needs to change?**
- **How do 'value-add' offerings such as cyber incident response impact claims experience?**
- **What are the implications of the rise in cyber hygiene regulations / guidelines, including for insurers and other financial institutions?**
- **Can/should compliance with regulations be used as a condition of coverage, or rating factor?**

Discussions with our panelists and practitioners in HK/Greater China including (re)insurance underwriters and cybersecurity experts have informed the thinking in this session. The working party would like to express our sincere appreciation for their contributions. We also thank PCS, a Verisk business for providing insights on the NotPetya loss.

IFoA GI Asia International Working Party members; Sie Liang Lau (Chair, UK), Nam Nguyen (UK), Michael Crouch (Aus), Cynthia Liu (HK), Chiew Yee Ng (HK), Cheu Teck Leo (HK), Sherwin Li (China), Paul Wee (MY), Nicholas Chee (MY), Ming Kien Lee (MY), Brad Weir (SG), Jim Attwood (SG), Mehul Dave (SG), Ishita Bhatia (SG), Sarthak Mahajan (IN), Megha Agarwal (IN)


50
ANNIVERSARY
ACTUARIAL SOCIETY
of
HONG KONG