



Institute  
and Faculty  
of Actuaries

# SAS ERM – ESSEC CREAR CONFERENCE 2018

## **Making Sense of Cyber Risk**

IFoA GI Asia/International Working Party

Sie Liang Lau



Institute  
and Faculty  
of Actuaries

# Agenda

- 1 About the IFoA GI Asia International Working Party
- 2 Making Sense of Cyber Risk
- 3 Next Steps for the Working Party



Institute  
and Faculty  
of Actuaries

# Agenda

1

## About the IFoA GI Asia International Working Party

2

Making Sense of Cyber Risk

3

Next Steps for the Working Party



Institute  
and Faculty  
of Actuaries

## Who we are



GI Asia/International Working Party created in Q2 2016



The first in Asia for IFoA UK



We have members from UK, AUS, HK, CHN, IND, SIN and MAL



We are from across the broad background from brokers, re/insurers, and working in various functions





Institute  
and Faculty  
of Actuaries

# Working Party Vision

*“Our goal is to reach out to support GI actuaries in the APAC region, to deliberate issues in the region specifically and in turn to support career growth for members in the region more specifically as well as to promote and raise awareness of the profession in the region as a whole, paving way for more such forum for the regions outside UK, and for other actuarial disciplines.”*



Institute  
and Faculty  
of Actuaries

# What is the intention of the working party



To facilitate a market wide research on risks specific for the APAC region



To develop relationships with regulators and local actuarial bodies



To develop initially an understanding of the GI insurance and actuarial issues / hot topics



To identify the perceived relative importance of these issues / hot topics for GI actuaries



To focus on specific topics of interest , common to multiple markets, and to provide fresh light and new understanding



Institute  
and Faculty  
of Actuaries

## Who are you?

### IFoA The Actuaries' Code

1. Integrity
2. Competence and Care
3. Impartiality
4. Compliance
5. Communication

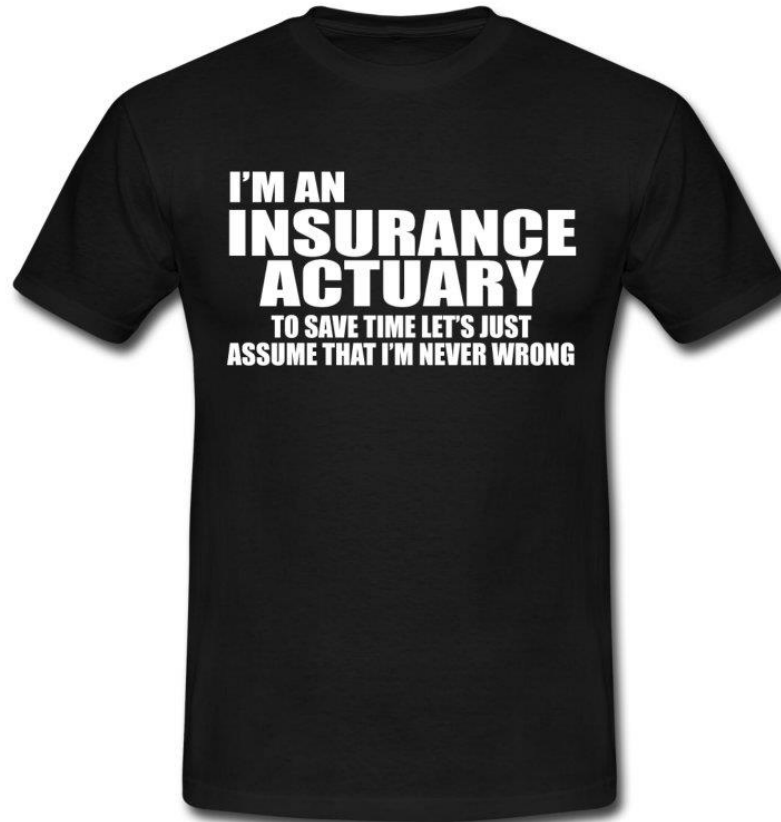
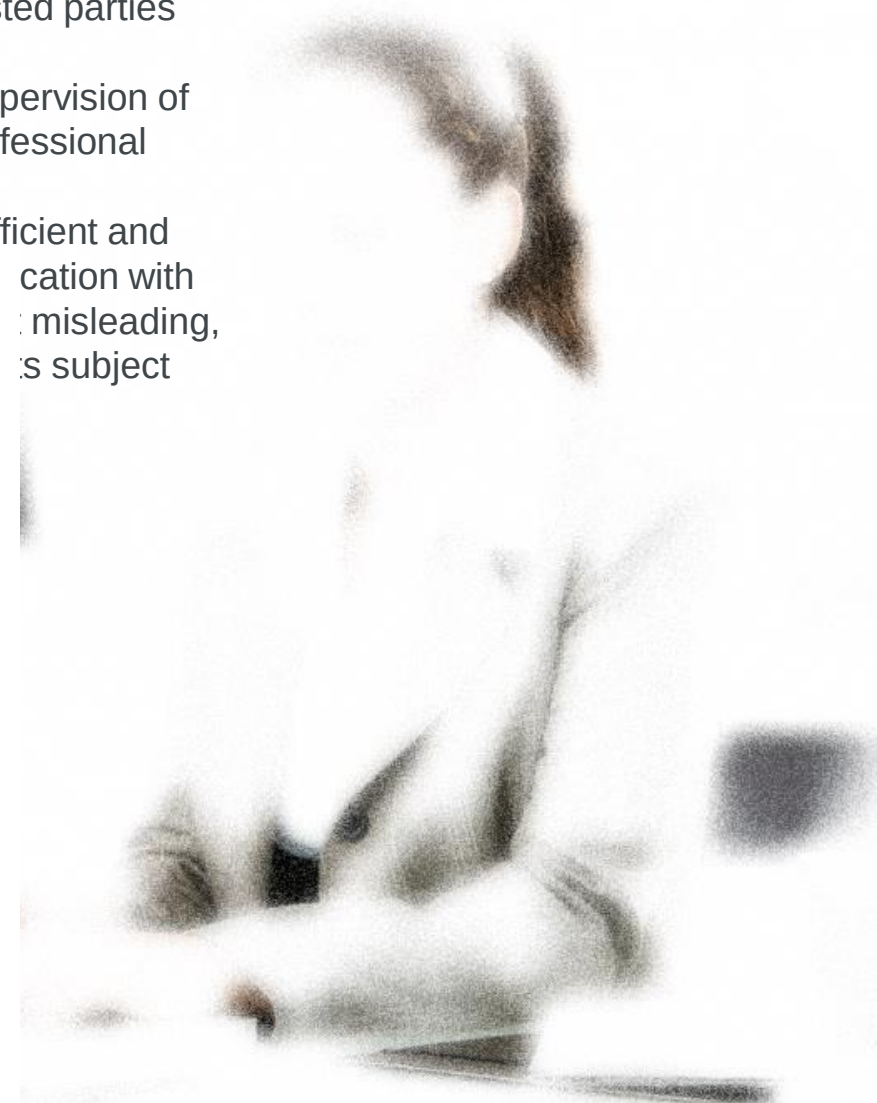
*Responsibility is on all of us to ensure we understand and communicate risk*

2.2 Members will not act unless:

- a) they have an appropriate level of relevant knowledge and skill; or
- b) they are acting on the advice of an individual who has the appropriate level of relevant knowledge and skill and all interested parties are aware that this is the case; or
- c) they are acting under the direct supervision of another member who is taking professional responsibility for that work.

5.3 Members will take such steps as are sufficient and

cation with  
misleading,  
subject





Institute  
and Faculty  
of Actuaries

# Agenda

- 1 About the IFoA GI Asia International Working Party
- 2 Making Sense of Cyber Risk**
- 3 Next Steps for the Working Party

# Agenda – Making Sense of Cyber Risk

- 1** Setting the scene
- 2 Silent cover vs. Affirmative cover
- 3 Development of cyber products and regulations in The West & Asia
- 4 Quantifying cyber risk / Managing aggregations
- 5 What's next? Future research areas



Institute  
and Faculty  
of Actuaries

# The Risk Landscape: Aon Global Risk Survey 2017



Institute  
and Faculty  
of Actuaries

# Setting the scene - steady rise in cyber threats

“ Until recently, the general (re)insurance market **treated cyber as a product**.

There was a belief that cyber exposure could be avoided if it was not written on an affirmative basis. **This approach is slowly changing.**

Increasingly, cyber is viewed as **a distinct peril**, as risk carriers realise that it cannot be avoided ”

*Capsicum Re Cyber white paper, May 2018*

- **WannaCry ransomware attack, May 2017** encrypts files on computers running the Microsoft Windows, blocking access then demanding a ransom payment in bitcoin. Affected 400,000 machines in 150 countries, including UK's National Healthcare system and Spain's Telefonica. Total economic losses associated with WannaCry are estimated at \$8bn, with half-a-billion dollars attributed to direct costs and indirect business disruption, according to AIG.
- **NotPetya, June 2017** - state sponsored attack that ground the operations of shipping firm Maersk in Ukraine to a halt in 60 minutes as every single piece of its IT equipment was infected – forced to reinstall 4000 servers and 45000 PCs, millions of dollars damages. Impact spread far beyond Ukraine. US pharmaceutical Merck filed a large property claim.
- **Operation Cloud Hopper** - attacks were levelled against managed IT service providers, which were used to access clients target's corporate assets and trade secrets.
- **Roaming Mantis malware** that steals user information, giving the hacker full control over compromised Android devices. Initially targeting Asia – now spreading globally.



Institute  
and Faculty  
of Actuaries

# Agenda – Making Sense of Cyber Risk

- 1 Setting the scene
- 2 Silent cover vs. Affirmative cover**
- 3 Development of cyber products and regulations in The West & Asia
- 4 Quantifying cyber risk / Managing aggregations
- 5 What's next? Future research areas



Institute  
and Faculty  
of Actuaries

# Types of cyber cover - Silent cover

“ **NotPetya** had negatively impacted 3Q results, including an unfavorable **revenue impact** of approximately **\$135 million from lost sales** and approximately **\$175 million in costs**. This will be repeated in Q4. ”

*Merck CFO, 3Q2017 earnings call*

This led to a claim on Merck's property policies

- ‘Non-affirmative’ or ‘Silent’ cyber cover is emerging as the critical area of concern.
- It refers to potential cyber exposures within traditional property and liability insurance policies, as well as MAT & motor, which may not implicitly include or exclude cyber risks.
- Cyber losses are materialising with increasing frequency across traditional property/casualty covers.
- There is uncertainty whether losses caused by a cyber event will be covered under traditional insurance covers.
- As an example, NotPetya disrupted US pharmaceutical giant Merck's production lines - leading to a claim on its property policies. Financial impacts were feared to be as high as USD1 - 1.5bn, though insurance settlement likely up to USD 275m
- ‘Silent’ cyber risks are material



Institute  
and Faculty  
of Actuaries

# Types of cyber cover - Silent cover

## The key challenges:

- Ambiguity for the insured
- Unknown exposure for the insurer - cyber catastrophic losses can transcend class, geography, and industry, exacerbating the challenge. Traditional aggregation methodologies do not apply.
- Regulatory pressures on contract certainty and clarity of cover
- Customer demand for clarity of coverage

## What can/should the industry do?

- Clear wording or exclusion clauses – in consideration of customer interests and increasing regulatory pressure. However many of these clauses have yet to be tested in court of law.
- Example: Marine cyber exclusion (The Institute Cyber Attack Exclusion Clause CL 380)



Institute  
and Faculty  
of Actuaries

# Types of cyber cover - Affirmative Cover

## Demand:

- Buyers still getting used to the concept of needing to purchase standalone cyber cover (especially SMEs).
- The business case to purchase cyber cover is complicated by the large differences in types of cover available, non-standardized wordings.
- Several larger-scale cyber events, and increasing maturity / in the market leading to clearer exclusions of cyber coverage from existing Property / Liability / Marine policies could increase demand for cyber products.

“ Cyber is **three times more expensive than General Liability**, and six times more expensive than Property ”

*Inga Beale, Lloyds*



Institute  
and Faculty  
of Actuaries

# Types of cyber cover - Affirmative Cover

## Supply:

- Affirmative cyber cover – cyber risk is explicitly evaluated, priced, and underwritten as a standalone risk. Also available as extension to general liability policies.
- Cyber insurance market is growing quickly. Level of maturity is growing though products are still very divergent across providers.
- Coverage provided for:
  - Perils: Data breaches, hacker attacks, (contingent) business interruption
  - Types of cover: Financial indemnity, peace-of-mind cover (recovery costs to get businesses back up and running)
- Role of cyber insurers in enhancing policyholder's cyber risk management practices

“Current **acquisition costs** for cyber products are high, at an estimated 40%”. There is potential for online distribution or aggregators to lower this cost

*2018 London cyber insurance conference panel*



Institute  
and Faculty  
of Actuaries

# Agenda – Making Sense of Cyber Risk

- 1 Setting the scene
- 2 Silent cover vs. Affirmative cover
- 3 Development of cyber products and regulations in The West & Asia**
- 4 Quantifying cyber risk / Managing aggregations
- 5 What's next? Future research areas



Institute  
and Faculty  
of Actuaries

# Regulations Relating to Cyber Security

- UK: GDPR expected to drive frequency/severity of cyber claims
- Asia: Segmented levels of regulation that are evolving

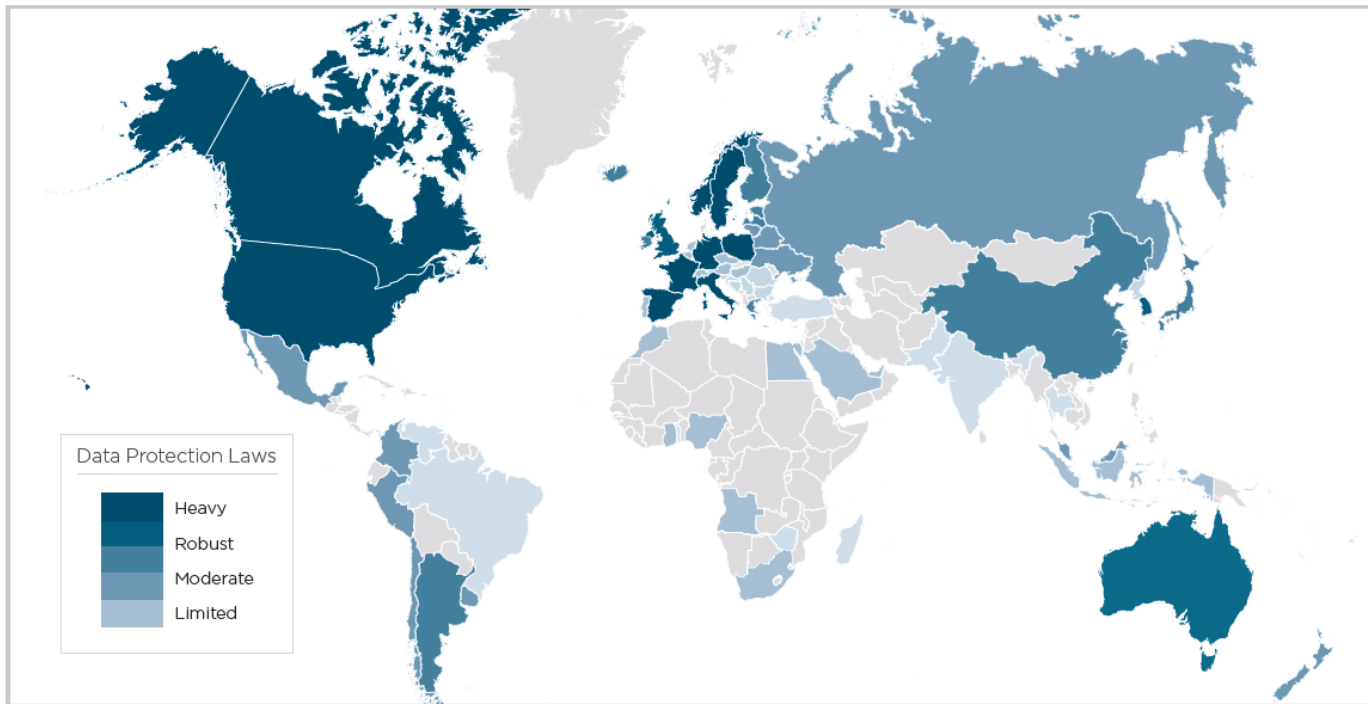


Figure 2: World Map of Data Privacy Regulation (Source: DLA Piper)

Extracted from RMS Cyber Risk Outlook 20180305

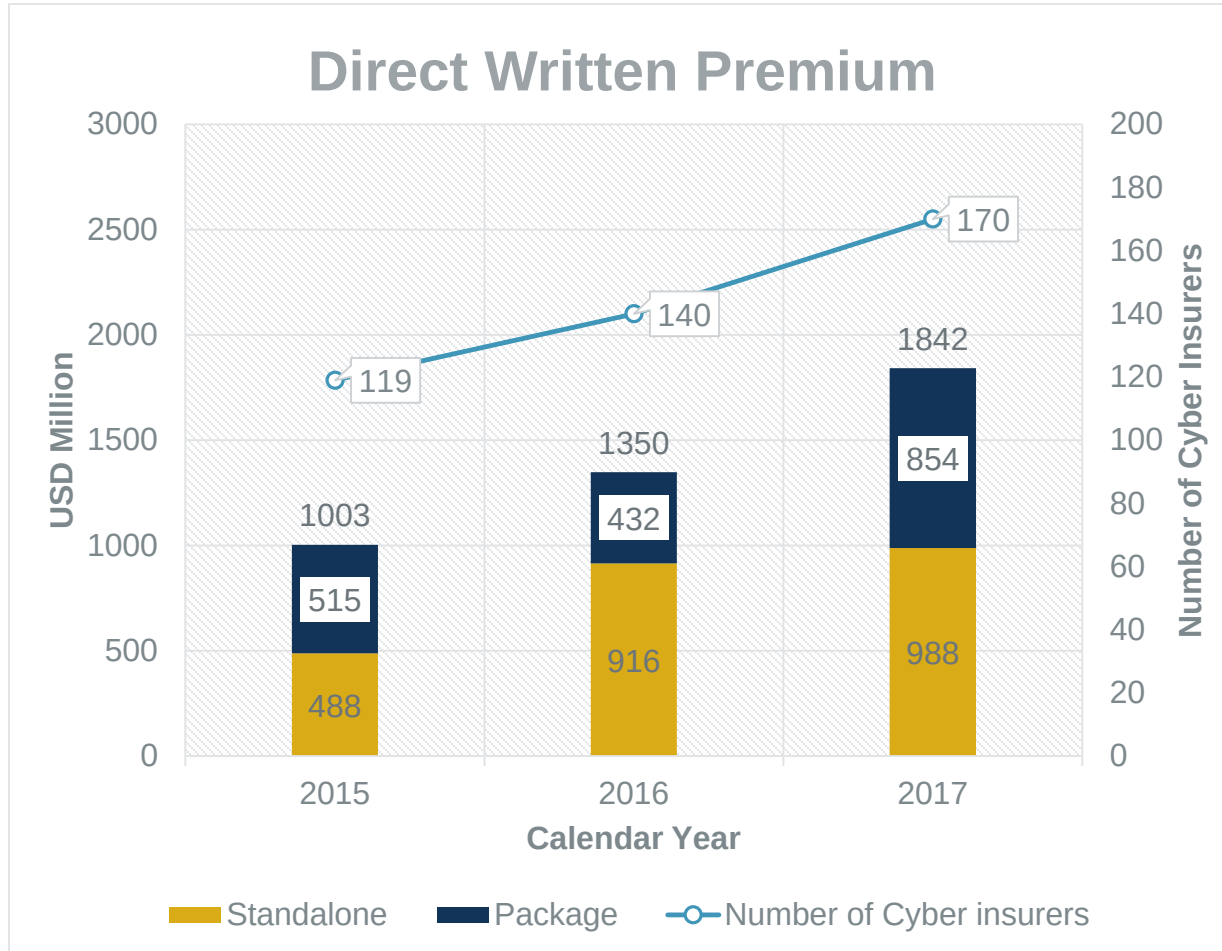
- Singapore: MAS Cybersecurity Bill, Personal Data Protection Act 2014
- China: Cybersecurity Law 2017
- Hong Kong: Personal Data (Privacy) Ordinance 2016
- Malaysia: National Cyber Security Act, Personal Data Protection Act 2010
- Australia: Various laws from Australia Privacy Commissioner and APRA



Institute  
and Faculty  
of Actuaries

# Products in the Market

## Case Study: US Cyber Market



Extracted from US NAIC statutory filings on 4 June 2018 (Aon Benfield Analytics)

### Observations:

- Chubb is the biggest writer in 2017
- Premiums grew approximately 37% to USD 1.84 billion
- A growing number of insurers' participation (170)
- Loss ratio has improved to 32.4% (from 40s)
- Despite 2017 events, both claim frequency and severity seem to have reduced



Institute  
and Faculty  
of Actuaries

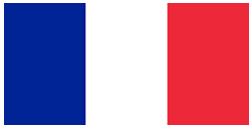
# EMEA-Country Cyber Map



- Number of Cyber product offering insurers/syndicates: >50
- Segments of supply: industrial/SME/private
- Market wording - no
- Lloyds Market premium 600-700m worldwide + Non-Lloyds premium (size?)



- Number of Cyber product offering insurers: 23 (10 Globals / MN + 13 medium and small insurers)
- Segments of supply: 12 industrial / 16 SME / 6 private
- Market Wording : yes – from the Insurance association GDV
- Market premium 2017: € 80-100m



- Number of Cyber product offering insurers: 11
- Segments of supply: >6 industrial/ <6 SME
- Market wording: no
- Market premium: >€50m



- Number of Cyber product offering insurers: >11
- Segments of supply: industrial/ SME/ private
- Market wording: no
- Market premium: industrial >1m/ SME + private €2-3m



- Number of Cyber product offering insurers: 10-15
- Segments supply: industrial /SME
- Market wording: no
- Market premium: €10-15m

Facts and figures (often based on estimates) collected from the underwriters



Institute  
and Faculty  
of Actuaries

# Products in the Market

## Case Study: Malaysia

- Only larger and multinational companies offer cyber covers
- Demand mainly from large conglomerates, public listed companies as well as branches and subsidiaries of multinational companies
- Typically low policy limit eg \$20m to \$100m



# Products in the Market

## Case Study: Malaysia

Typical Cover:

- Business interruption loss
- Data loss and restoration costs
- Incident response and investigation costs
- Liability settlement and defence costs
- Regulatory defence and penalties
- Cyber extortion expenses and extortion monies

Plus additional crisis management service



Institute  
and Faculty  
of Actuaries

# Products in the Market

## Case Study: Malaysia

Typical Exclusions:

- Bodily injury
- Property damage and hardware
- Malicious intent of representatives
- Unauthorised or wrongful collection of personal data
- Failure in power, internet, telecommunications and other infrastructure
- Natural catastrophe
- Theft or loss of unencrypted laptops and mobiles



Institute  
and Faculty  
of Actuaries

# Agenda – Making Sense of Cyber Risk

- 1 Setting the scene
- 2 Silent cover vs. Affirmative cover
- 3 Development of cyber products and regulations in The West & Asia
- 4 Quantifying cyber risk / Managing aggregations**
- 5 What's next? Future research areas



Institute  
and Faculty  
of Actuaries

# Known claims to reinsurers (to date)

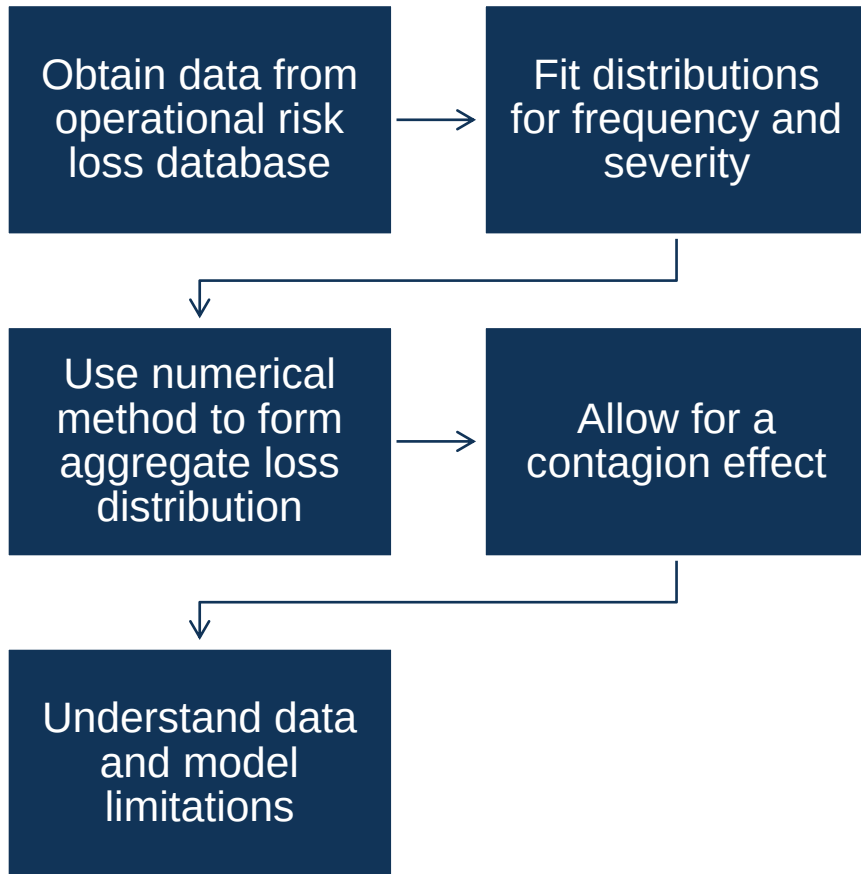
| Claim               | TARGET     | HOME DEPOT | SONY       | EXPERIAN   | MERCK      | MONDELEZ |
|---------------------|------------|------------|------------|------------|------------|----------|
| Date                | 19/12/2013 | 02/09/2014 | 24/11/2014 | 24/09/2015 | 27/07/2017 |          |
| Cyber Limit         | NIL        | NIL        | NIL        | NIL        | Yes        | Yes      |
| Status              | Closed     | Closed     | Open       | Open       | Open       | Open     |
| Gross Loss Estimate | USD 175 m  | USD 247 m  | USD 87 m   | USD 52 m   | USD 1 b    | USD 50 m |

**Target , Home Depot, Sony, Experian are data breaches which resulted from different events. The two last losses Merck and Mondelez were caused by the same Virus and appear to be for the reinsurance Market the two first losses caused by the same event. Not Petya caused disruption of thousand companies around the world.**



# Quantifying Cyber Risks

## Theoretical Approach



- Frequency – Severity Model (similar to models used to quantify operational risks at banks or to price insurance contracts).
- For further details see IMF Working Paper WP/18/143 Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment.
- This approach is suitable for large insurance groups writing cyber covers and also financial institutions where cyber exposure is high.



# Quantifying Cyber Risk

## Pragmatic Approach

- Most organisations do not have the resources or sophistication to quantify cyber risks to a granular detail
- Proprietary approaches from risk related service providers eg brokers and consultants are widely available
- Top down approach can be utilized – market scenarios, with consideration for insurers' market share
- Fit for purpose for industries where cyber exposure is not significant and not industry specific



# Agenda – Making Sense of Cyber Risk

- 1 Setting the scene
- 2 Silent cover vs. Affirmative cover
- 3 Development of cyber products and regulations in The West & Asia
- 4 Quantifying cyber risk / Managing aggregations
- 5 What's next? Future research areas**



Institute  
and Faculty  
of Actuaries

# What's next? Future research areas

When considering the impact of potential cyber exposures, underwriters need to focus on three things:

1. Frequency – To what extent do cyber incidents make losses more frequent?
2. Severity – To what extent do cyber incidents make losses more severe?
3. Systemic – To what extent do cyber incidents present a systemic risk?



# What's next? Future research areas

Our initial research raises more questions than answers – not a bad thing!

Combination of professional expertise required to consider:

- Commercials – product wordings, coverage, exclusions
- Pricing and aggregation – development of stochastic scenario modelling
- Cooperation on data gathering

Asian-specific context / data could be useful, though given the nature of cyber risk, Asian markets are in a better position to leverage developments in London/US markets, as compared to other perils /LOBs.



Institute  
and Faculty  
of Actuaries



Institute  
and Faculty  
of Actuaries

# Agenda

1 About the IFoA GI Asia International Working Party

2 Making Sense of Cyber Risk

**3 Next Steps for the Working Party**

# What are the Next Steps for Working Party

- We want to hear from local practitioners
  - Work with Actuarial Societies on local, regional challenges
  - Key issues within local markets
  - Data challenges
  - Any other areas
- How will the working party aim to engage
  - Survey
  - One-on-one
  - Continuous Feedback
  - Industry events



Institute  
and Faculty  
of Actuaries

## Further Related Areas of Interests for Local Practitioners

- Following a presentation by the GI Asia International Working Party earlier this year in Singapore, we have received various queries and feedback. This has demonstrated significant interests from local practitioners with regard to cyber risk modelling.
- One main theme is the credibility of model results, in light of lack of data /events for modelling such risk, generally we are unsure how often a model would give an accurate tail event and how they can trust model outputs given that results change every year.
- Another theme that was raised is the prospect of Big Data and Machine Learning to aid cyber risk modelling, in view of lack of economic losses in the region.



# Who we are

## Members

- Sie Liang LAU (Chair, UK); slau@scor.com
- Nam NGUYEN (UK)
- Michael CROUCH (Australia)
- Sherwin (Xiao Xuan) LI (China)
- Brad WEIR (Singapore)
- Paul WEE (Malaysia)
- Nicholas YEO (Malaysia)
- Megha AGARWAL (India)
- Sarthak MAHAJAN (India)
- Lyon CHEU (Hong Kong)
- Chiew Yee NG (Hong Kong)
- Cynthia LIU (Hong Kong)

## UK GI Board Chair

- Martin NOBLE; martin.noble@uk.zurich.com

## Executive Staff

- Marie LEE (Singapore); marie.lee@actuaries.org.uk
- Sharon CUMBERBATCH (UK); sharon.cumberbatch@actuaries.org.uk



Institute  
and Faculty  
of Actuaries

# Questions

# Comments

Expressions of individual views by members of the Institute and Faculty of Actuaries and its staff are encouraged.

The views expressed in this presentation are those of the presenter.



Institute  
and Faculty  
of Actuaries