Institute and Faculty of Actuaries

Cyber Insurance Underwriting and Pricing Considerations

Stavros Martis – KPMG
Phil Mayes - Talbot

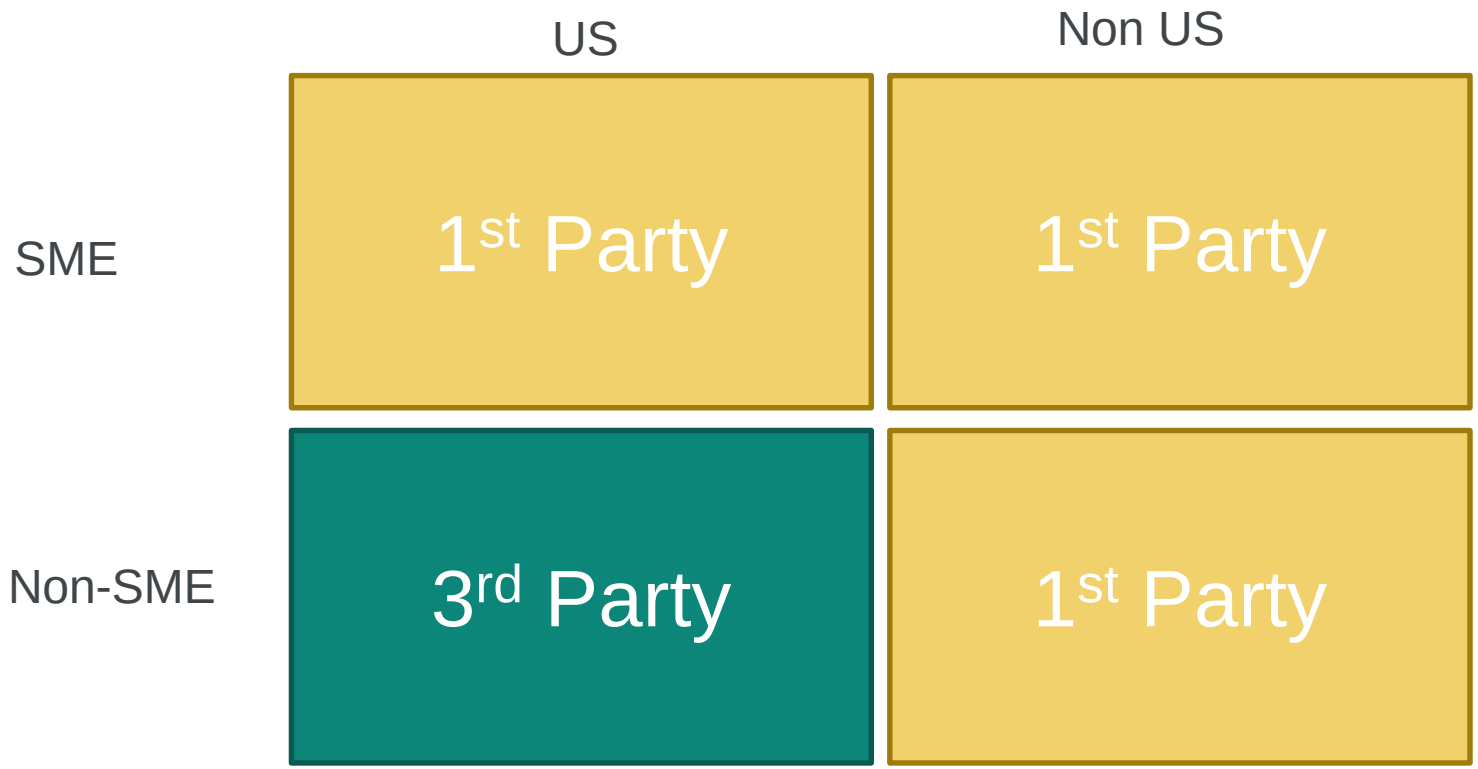
Pricing Seminar
6th June 2017

Institute and Faculty of Actuaries

Underwriting Considerations

The Cyber Landscape

The current coverage landscape may be split into the following areas with coverages across 1st Party and 3rd Party.



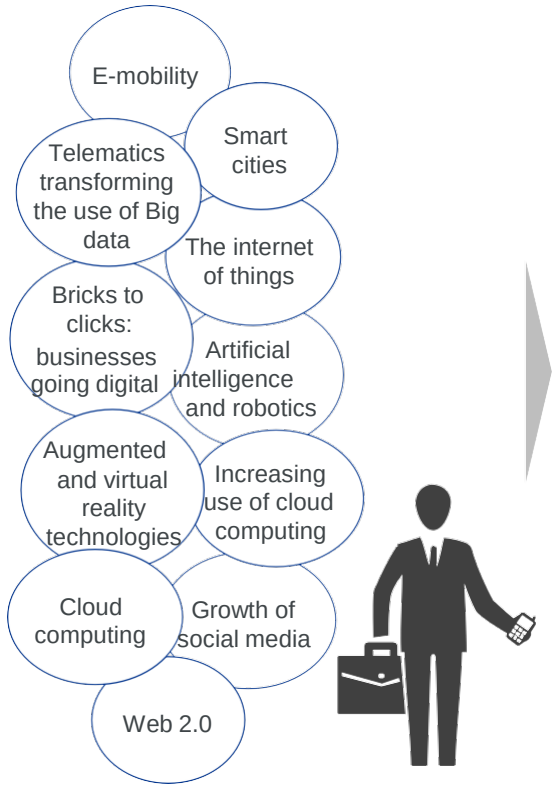
- **1st Party covers:**
- Ransomware
- Cyber extortion
- Network breakdown
- Costs of reconstituting data
- Remediation costs

- **3rd Party covers:**
- Network liability
- Data breach
- Multimedia
- Breach of privacy

Institute and Faculty of Actuaries

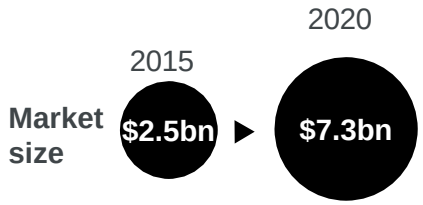
Exposure and Coverage

The current cyber insurance market is predicted to triple in size by 2020, while additional non-traditional loss areas may present significant growth opportunities in medium-long term.

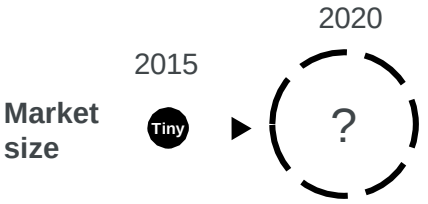


1	**Privacy Breach**	• Merchant data theft • Privacy breach liability • Remediation costs • Regulatory penalties
2	**Cyber Crime & Fraud**	• Identity theft liability • Transactional fraud in electronic payments
3	**Extortion**	• Cyber extortion
4	**Data & Software Loss**	• Data loss and reconstitution
5	**Network Security Liability**	• Transmission of a virus to a third party
6	**Business Interruption**	• Loss of profits due to network failure or interruption
7	**Theft of IP**	• Litigation costs for IP disputes • Theft of intellectual property
8	**Cyber Physical Damage**	• Cyber terrorism • Broader physical damage of assets resulting from a cyber attack
9	**Reputational Harm**	• Reputational harm following cyber events
10	**Multimedia**	• Media and Copyright Infringement Liability • Defamation • Piracy and misappropriation of idea

Current segment focus:



Medium – long term propositions:



Sources: (1) Juniper Research, 'Cybercrime and the internet of threats', 2015

Institute and Faculty of Actuaries

Sources of Cyber Risk

Traditional insurance classes will need to increasingly pick up a variety of cyber perils which will require new capabilities and skillsets.

The Internet of Things

With increasingly interconnected physical devices, vehicles, buildings, electronics, software, data and other objects, many products are increasingly exposed to cyber risk.

Home insurance:

Criminals intercept some of the smart-home radio signals and replay them to open a property's doors and commit a robbery, or hackers attack a system and disable heating systems.

Property Insurance:

Smart warehouse's thermostats are hacked, causing significant increase or decrease in temperature, leading to major loss of products.

Alternatively, sprinkler system is hacked, causing physical damage.

Property Insurance:

Operational technology is hacked to change product ingredients or manufacturing designs, causing liability or product recall.

Alternatively, waterworks are hacked, causing flooding and physical damage.

Motor Insurance:

Terrorists could hack into the communication system between vehicles to send false signals and cause widespread fatalities to passengers.

Energy Insurance:

Criminals hack a drilling system, make it overheat and cause fire.

Alternatively, a hacker accesses an internal oil-rig system, attaches a virus to outgoing e-mails, infecting computer networks on-shore.

Aviation Insurance:

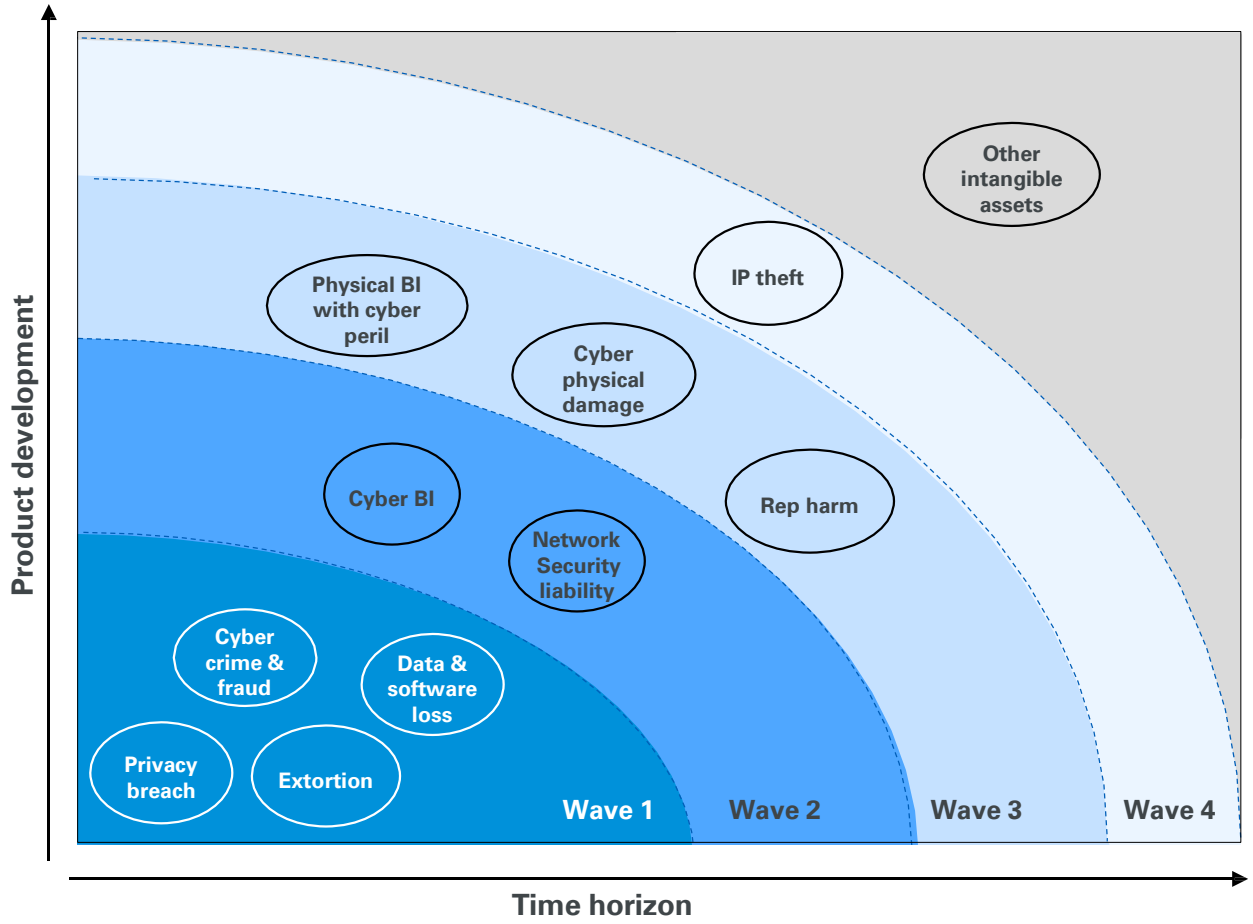
Hackers access an in- flight entertainment system and steal personal passenger information.

Alternatively, a terrorist uses a smartphone app to access a plane's steering system and causes a crash.

Institute and Faculty of Actuaries

New opportunities are emerging in cyber insurance

Development of cyber insurance may follow several waves, gradually expanding from core propositions focusing on digital assets to new products covering other types of assets and even some non-cyber perils



Wave 1 – enhancing core propositions with strong crisis management services.

Wave 2 – improving risk modelling and coverage.

Wave 3 – expanding to other assets with cyber triggers.

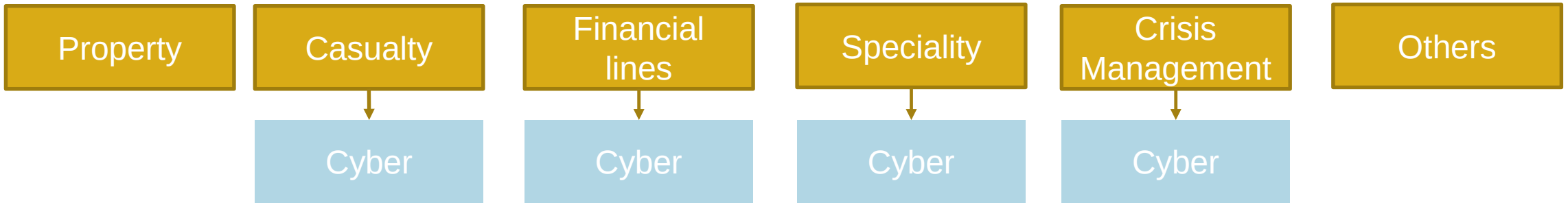
Wave 4 - innovating to develop products to address market gaps.

Wave 5 – considering to expand scope to cover other intangible assets with non-cyber perils.

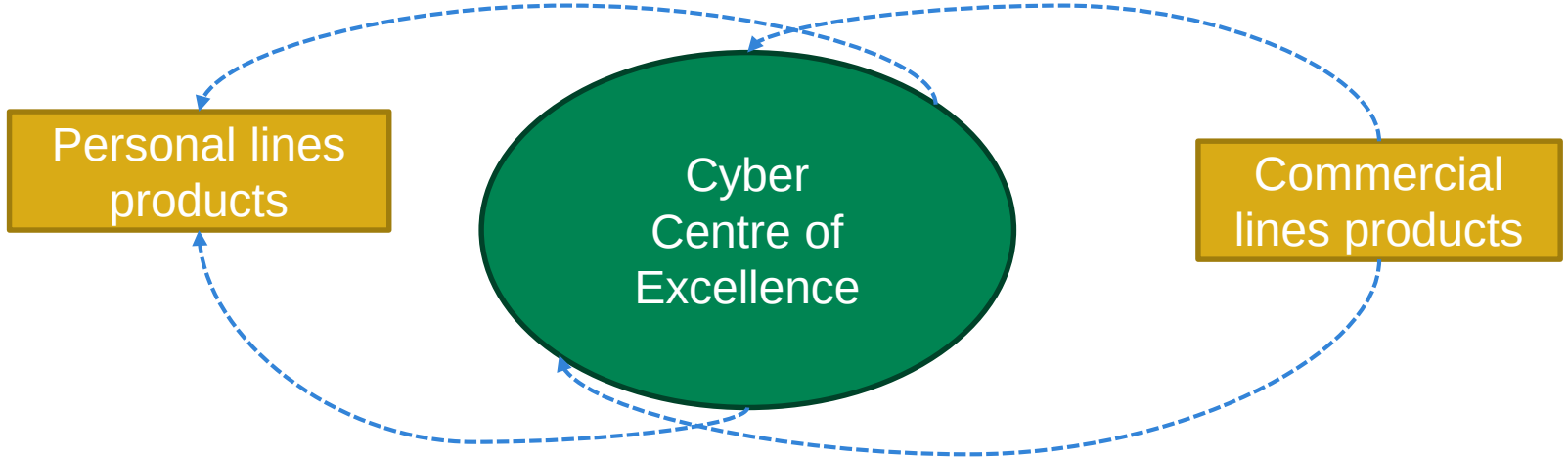
Institute and Faculty of Actuaries

Insurance Company Organisational Design

- Today's Insurance company



- Tomorrow's Insurance Company



Institute and Faculty of Actuaries

What does the future look like?

	Today	Future Vision
Team Structure	• Silos of teams due to limited scope of cyber coverage	• Standalone cyber departments • Cyber Centre of Excellence
Policy Coverage	• Limited coverage, with **too much focus on privacy breach** • Limited coverage beyond privacy breach • Limited Use of Preventative service	• Extended service offering • Increased policy coverage • Greater use of preventative services
Data	• Lack of confidence in modelling capability due to data limitations • Lack of cyber modelling capabilities	• Partnerships with external specialised providers • Niche cyber underwriting teams.

Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

Pricing Considerations

Underwriting and Claims Considerations

Initial Risk Assessment

- **Process needs to be quick and not intrusive**
- **Difference between SME vs Large**
- **SME risks** can be managed via a finite number of questions in most cases.
- **Large risks** require a larger set of questions**.**

- Questionnaires/Interviews
- On-line assessments
- External penetration assessments (using 3rd party vendors)
- Full reviews

- Data is available
- Able to create a view on a client's capabilities:
  - Documentation and process reviews
  - Training
  - Incident response procedures
  - Systems
- But limitations could exist (e.g. outside-in view only)

Underwriting Judgement

Challenges of Initial Risk Assessment

- Reliance of 3rd party data
- Data only provides a snapshot
- Insufficient data
- Previous step does not absolve responsibility of underwriter

Underwriter's judgement and skill

- Assess data
- Map exposures to coverage offered by policy
- Large vs SME
- View on accumulation

Claims

What does the customer need?

- SME
  - Dedicated hotline
  - Incident response/Crisis Management, NOT indemnity
- Large Corporates
  - In house teams to deal with initial response
  - Need expert support
  - Some indemnity element

- Limited data on new coverages
- Issues with historical data

Pricing Process

Institute and Faculty of Actuaries

Regulatory Issues

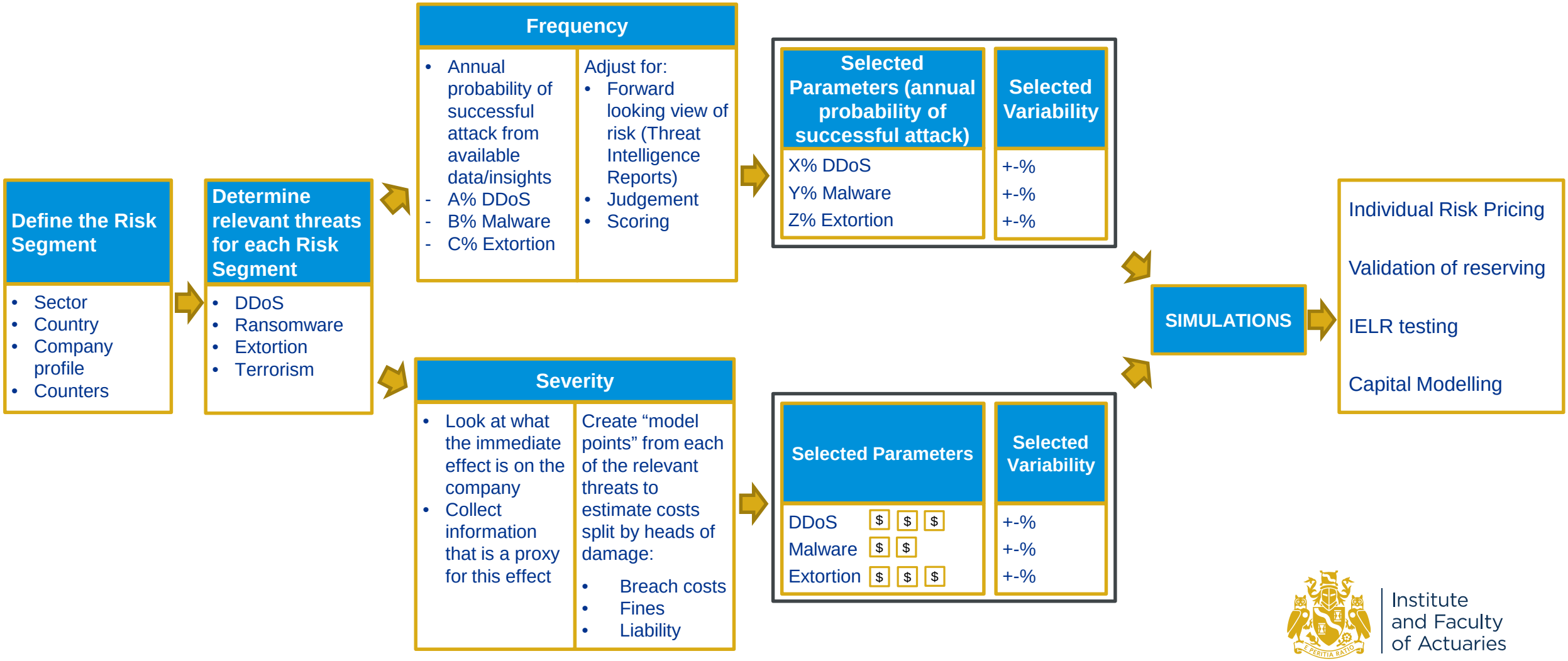
- Data Breach
  - The loss or possible unauthorised revealing of (Sensitive) Personal Data (E.U.), PII/SPII/(e)PHI (U.S.), or any data relating to individuals that is controlled by legislation anywhere in the world.
  - Definitions
    Personal Data
    PII (Personally Identifiable Information)
    PHI (HIPAA) (Personal Health Info)
  - General Data Protection Regulation (E.U.)
- PRIVACY IS NOT DATA BREACH!
- It is not possible to contract out of the statutory legislation relating to data Controllers/Owners, although robust contractual terms will substantially mitigate the exposure
- It is the breach of legislation anywhere in the world and will be triggered by the COLLECTION, RETENTION, PROCESSING AND DESTRUCTION of personal / sensitive data.
- Restrictive legislation is not restricted to the US and EU.
  Australia, South Africa, Singapore, Brazil & China are introducing stricter privacy bills and Indonesia debating probable implementation

Data Issues

- Data schemas are generally US-focused
- Available data is predominantly from the US therefore not necessarily relevant for other territories
- Common Issues:
  - ***By publication:***
    - Inconsistencies between years (within the same publication)
    - Inconsistencies across different reports
    - Varying definitions (e.g. costs / event / incident)
    - Population that contributed to the reports show inconsistencies between years, territories (US vs others) and sector
  - ***Claims data issues such as:***
    - Sparse with very few large events recorded
    - Lack of transparency as companies do not publish data
    - Segregation is not sometimes clear (Tech E&O vs breach response claims)
  - ***Potentially already out of date***

Institute and Faculty of Actuaries

Frequency – Severity Approach



Institute and Faculty of Actuaries

Accumulation

- Models are in their infancy – Outputs are likely to change (potentially materially) as risk is better understood

- Reinsurance cover is cheap at the moment – The problem has shifted to reinsurers (for now)

- How do you monitor aggregation? By:
  - System?
  - Geography?
  - Sector?

- Scenarios are widely used – But are they useful/appropriate?

Institute and Faculty of Actuaries

Implications on Pricing

Data

- Lack of volumes
- Better quality/breadth is required
- Consistency across products
- Increased availability of information
- Types of data will evolve over time as knowledge of risks emerges

Modelling

- Types of parameters used in models
- Need to frequently update models
- Scenario analysis to assess impact on pricing
- Scenarios are the starting point

Governance

- Accumulation tools still being developed
- Validation of scenarios
- Monitor how models are developed and used
- How cyber is underwritten: Centralised vs silos

Institute and Faculty of Actuaries

Conclusion

- Coverages vary across US and Non-US and are predominately 1st party with growth expected for 3rd party coverages
- Sources of cyber risk present across a number of products
- Insurance company organisation design will change in future
- Underwriting approaches vary depending on the size of the risk
- Data is an issue with improvements in quality and consistency required
- Forming a forward looking view is key as Cyber threats are evolving fast

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