Institute and Faculty of Actuaries

Cyber & Terror Reserving Considerations

Stavros Martis – KPMG
Dr Christos Mitas – RMS

Reserving Seminar
20th June 2017

Institute and Faculty of Actuaries

The Cyber Landscape

Expertise Sponsorship Thought leadership Progress Community Sessional Meetings Education Working parties Volunteering Research Shaping the future Networking Professional support Enterprise and risk Learned society Opportunity International profile Journals Supportin

What is the Cyber Landscape?

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

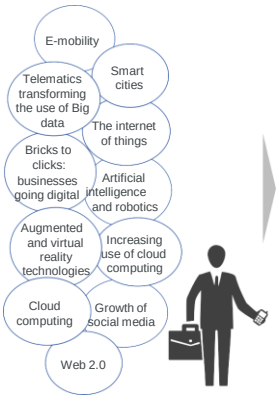
	US	Non US
SME	1st Party	1st Party
Non-SME	3rd Party	1st Party

- **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

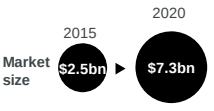
What Does Cyber Insurance Actually Cover?

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:



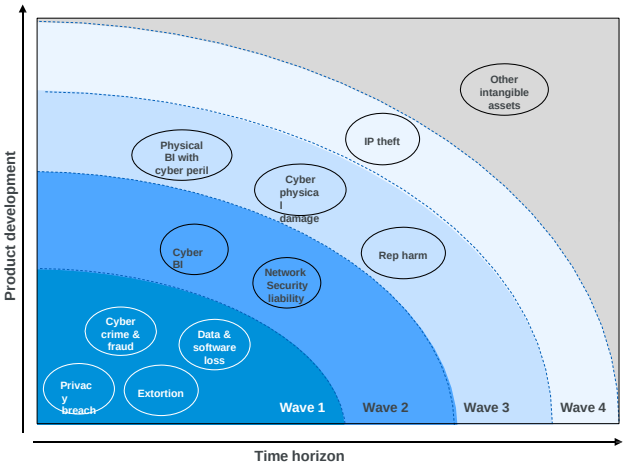
Medium – long term propositions:

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

Institute and Faculty of Actuaries

Can I rely on Historical Data?

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

6

Cyber – How is it priced?

Initial Risk Assessment	Underwriting Judgement	Claims

• **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.
	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
		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

• Questionnaires/Interviews • On-line assessments • External penetration assessments (using 3rd party vendors) • Full reviews	**Underwriter's judgement and skill** • Assess data • Map exposures to coverage offered by policy • Large vs SME • View on accumulation	

• 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)
	Pricing Process	• Limited data on new coverages
		• Issues with historical data

Institute and Faculty of Actuaries

9

How much Reliance Can I Place on Cyber Data?

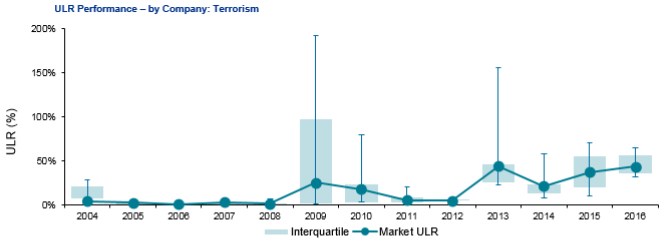
- Data schemas are generally US-focused
  - Available data is predominantly from the US therefore not necessarily relevant for other territories
- Common Issues:
  - ***By publication:***
    - Inconsistencies between years (within the same publication)
    - Inconsistencies across different reports
    - 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***

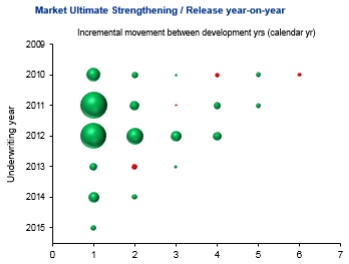
Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

The Terrorism Landscape

How has the Terrorism Class Performed?





Institute and Faculty of Actuaries

Terrorism – How is the Landscape Changing?

- Terrorism remains a persistent global threat
  - Although large scale attack frequency has subsided
- Re/insurers trying to understand risk of large scale attacks, the risk is not random:
  - Logistical burdens are high
  - Funding requirements are substantial
  - Targeting preferences are constrained
- Chemical/Biological/Radiological/Nuclear (CBRN) risk is a renewed concern

Institute and Faculty of Actuaries

What are the latest on the dynamics of Terrorism risk?

- The terrorist threat transforms according to evolving security
  - "Terrorism risk is the risk of failure of counter-terrorism" (Dr Gordon Woo)
- Target substitution operates at all spatial scales of the threat landscape.
- Counterterrorism organizations can optimize finite resources by randomizing the locations of their forces

Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

Tail Risk & Accumulation

Why Would Reserving Actuaries Care?

- Cat Loads
- ENIDs
- IELR
- Margins (IFRS and Solvency II)

Institute and Faculty of Actuaries

Cyber Tail Risk – What is happening?

- Systemic nature of Cyber Risk is now generally accepted
  - WannaCry
  - ShadowBrokers
  - SWIFT
  - Dyn DDoS attack (IoT)
  - Cloud Service Providers growth
- Regulations
  - US regulations on disclosure of 'breach of privacy' largely responsible for insurance market growth
    - Operating from 2005-2006 onwards
    - Now covering 47 States
  - EU legislation expected in May 2018 – GDPR
    - Notification in 72 hours
    - Max fines of €20M or 4% of annual global turnover
  - Australia & Asia are following suit
- Cyber-physical systems are becoming more prone to systemic cyber attacks
  - Energy; Property; Marine; Industrial Facilities

Institute and Faculty of Actuaries

Cyber Tail Risk – How can it be quantified?

- Accumulation management
  - Cyber exposure schemas
  - Extreme but plausible scenaria
  - Affirmative & cyber-physical
- Catastrophe modelling
  - Human behaviour
  - Interdependent dynamics
  - Needs understanding of:
    - Threat actors
    - IT and human vulnerability
    - Assets at risk
    - Regulatory environment

Institute and Faculty of Actuaries

Terrorism Tail Risk – Latest Developments?

- Terrorism is difficult to insure
  - Areas of high risk are areas of high exposure
  - Loss outcome uncertainty is high
  - Event footprints are small
  - Risk landscape is unpredictable
- But, much better data today to model terrorism
  - 140,000+ historical attacks worldwide are cataloged
  - Hundreds of known large-scale plots
  - Dozens of threat groups
  - An increasing amount of transparency into counterterrorism specifics
  - Better data → better models
    - More potential for insurance product innovation

Institute and Faculty of Actuaries

Terrorism Tail Risk – How is it modelled?

- Accumulations
  - Top accumulations in building, radius, post code, or underwriting zone
  - Capital allocation
- Scenaria
  - Stress testing
  - Regulatory requirements
- Cat modelling
  - Top events in a portfolio
  - Relative risk between accounts and portfolios

Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

Wrap-Up

Expertise Sponsorship Thought leadership Progress Community Sessional Meetings Education Working parties Volunteering Research Shaping the future Networking Professional support Enterprise and risk Learned society Opportunity International profile Journals Supportin

Cyber vs Terrorism

Similarities

- Systemic risks
  - Fat tails; Large loss uncertainty
- Rapidly changing dynamics
  - And highly interdependent
- Based on human behaviour
  - Threat & Defence actors
- Potential for attritional losses
- Difficult to model in detail, so:
  - Accumulations
  - Scenaria

Differences

- As we observe with other threats, terrorism moves to cyber-space
  - 'Software is eating the world'
- Digital assets are exponentially increasing
  - More cyber risk; less physical terrorism risk; more cyber-terrorism risk
- International norms & cooperation
  - Much better in terrorism than cyber

Institute and Faculty of Actuaries

Conclusion

Historical Patterns - Use with care	Moving to High frequency/Low severity?
IELRs - Need to get closer to pricing models	Closer link to pricing – Independent Estimate?
Changing nature of threat – Data Obsolete	More frequent updates to models

ENIDs, Cat Loads & Margin – Subjective estimation. Models exists

Institute and Faculty of Actuaries

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 presenters.

Institute and Faculty of Actuaries