Institute and Faculty of Actuaries

Lessons learnt from the unlikely marriage between Cyber security experts and actuaries in producing a practical approach to cyber modelling

Stavros Martis, KPMG
Ana Chavez, KPMG

22/09/2016

Agenda

1. Overview of the Market

2. Cyber expert's point of view and areas to consider

3. A practical modelling approach

Institute and Faculty of Actuaries

Overview of the market

State of the London Market

- **Cyber Market continues grow**
  - its clear that with new regulation such as GDPR that there is a need for cover beyond the US market.
  - According to The Betterley Report 2015, annual policy premiums are approaching $2.75 billion. Its widely acknowledged as the fastest growing class.
  - According to Allianz 2016 Risk Barometer, cyber incidents are considered the No. 1 emerging risk for the long-term future suggesting the client need is there too.

- **There is a need to differentiate in the market.**
  - Many of the larger players are exploring the incorporation of preventative services into their products (eg Pen Testing, Red Teaming, crisis Mgt.) The main challenge is innovating in this way without raising premium.
  - The other way that insurers are differentiating is by offering higher limits. The most notable example being Munich Re & Beazley offering $100m limit (albeit with a large retention) in April 2016

- **The other high profile topic within cyber insurance is silent coverage** across their existing products. A recent LMA exercise suggested this was most acute in Liability. Lloyd's have issued scenarios to test syndicate exposures' for silent cyber exposure

- **We have seen a number of MGAs** be prominent in this market with Ryan Specialty Group, Scieumus and CFC.

- **Data is likely to be where future players will differentiate.**
  - Many players have looked for technology partnerships with IBM, Symantec, Bitsight etc. Others are building their claims taxonomy to build their own data assets to support with future pricing.

Institute and Faculty of Actuaries

Underwriting and Claims

"Pre-Bind" Assistance on Underwriting

- Questionnaires/Interviews
- On-line assessments
- External penetration assessments (using third party vendors)
- Full reviews
- Or, just do nothing….
- Cost is a key consideration (average premium vs cost of pre-bind assessment)

Why should actuaries care? – If a pre-bind takes place, there could be more data to help with the parameterisation of the models. For example, you could start collecting scores from these assessments and start building relativities.

"Post-Bind" Value-Add Services

- These are additional services that the insurer can offer
  - Pen testing
  - Documentation and process reviews
  - Training
  - Incident response procedures

Again, if these happen, then claims experience should be better than if these do not take place.

On the claims front (incident response), different models are adopted

- Dedicated hotline
- Panel
- Hybrid

What is key here is the time to respond. The longer the response, the larger the ultimate claim cost

Institute and Faculty of Actuaries

Scarcity of Data

- The London Market and Lloyd's have spent a lot of time thinking about data capture.
- This is the obvious first step in creating stable and credible data in the long run
- Various initiatives:
  - Lloyd's
  - Cambridge
  - RMS
  - AIR

- Commonality in collection of **geographic information** on insured companies using ISO country codes such as: US – United States, GB – United Kingdom etc
- **Standard Cyber Peril Codes**, such as: PCY - Cyber security data and privacy breach & PCZ - Cyber security property damage
- Agreement on **key indicators of cyber vulnerability** such as: Enterprise Size as captured by revenue and headcount, Organization Industry or Business
- Aligned **Cyber Coverages** including, but not limited to:
  - Security Breach of Privacy
  - Liability
  - Business Interruption
  - Cyber Extortion
  - Replacement of Lost Data and Software
  - Regulatory fines
  - Physical Damage and Bodily Injury
- Common **cyber risk attributes** including: number and type of records held which could be breached.
- Identifiable **Data Types** at risk include but are not limited to:
  - Credit Card
  - PII (Personally Identifiable Information)
  - PHI (Personal Health Information)
  - IP (Intellectual Property)
- Identification **of cloud service providers**
- Internet **Business Interruption** potential

Coverage

- Variety of coverages and exclusions
- Package vs Standalone
- Affirmative vs Silent

v1.0 Code	Cyber Coverage	% of Products Offering this Cover (Sample of 26)
1	Breach of privacy event	92%
2	Data and software loss	81%
6	Incident response costs	81%
15	Cyber extortion	73%
4	Business interruption	69%
12	Multi-media liabilities (defamation and disparagement)	65%
7	Regulatory and defense coverage	62%
14	Reputational damage	46%
3	Network service failure liabilities	42%
5	Contingent Business Interruption	33%
9	Liability – Technology Errors & Omissions	27%
10	Liability – Professional Services Errors & Omissions	23%
13	Financial theft & fraud	23%
16	Intellectual property (IP) theft	23%
18	Physical asset damage	19%
19	Death and bodily injury	15%
-	Cyber terrorism	12%
11	Liability – Directors & Officers	13%
8	Liability – Product and Operations	8%
17	Environmental damage	4%

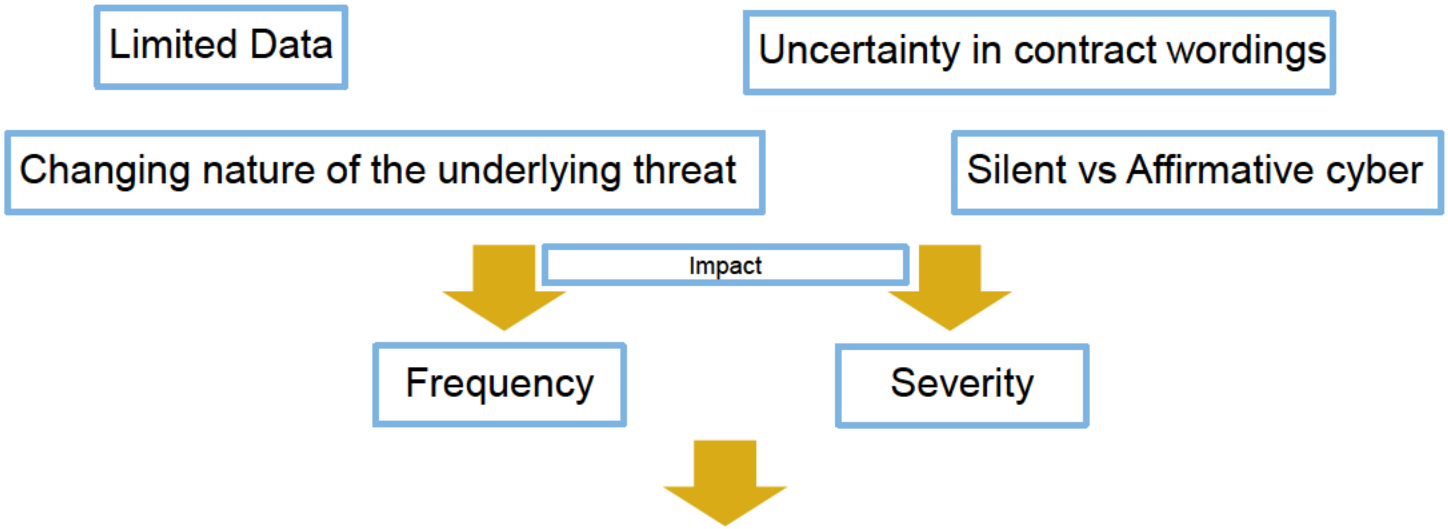
Source: RMS

Data Issues

- We have spent the best part of the year trying to collate data from public other sources.
- There is information out there but there are pitfalls:
  - Publications
    - Inconsistencies between
      - Years (within the same publication)
      - Different reports
    - Definition of
      - Costs
      - “event” or “incident”
    - Population that contributed to the reports
      - Inconsistencies between years
      - USA vs everyone else
      - Sector differences
  - Claims data
      - Sparse
      - Have not observed large events yet
      - Companies are reluctant to publish
      - Sometimes, claims data Include Tech PI claims
  - Already Out of Date?

Traditional Approaches may not work

- Cyber risk is a new risk, which does not lend itself to the use of traditional pricing and reserving approaches



An alternative approach:

- Drop down a couple of layers to look at cyber risk at the Sector/Country/Insured level
- Try to model the risk from ground-up, (starting from the technical characteristics of cyber)
- Talk to cyber experts!

Meeting the Cyber Security Expert….

Institute and Faculty of Actuaries

Meeting the Cyber Security Expert….

- First date went badly…..
- At first glance, this marriage was doomed to fail…..

Institute and Faculty of Actuaries

Meeting the Cyber Security Expert….

- Actuary's view of the cyber experts:

  - Geeks
  - Very focused on the technical side
  - Whilst they do have access to data, they usually do not have a structured way of analysing this data

Meeting the Cyber Security Expert….

Actuary's view of the cyber experts:

- Geeks
- Very focused on the technical side
- Whilst they do have access to data, they usually do not have a structured way of analysing this data

Cyber experts view of the Actuary:

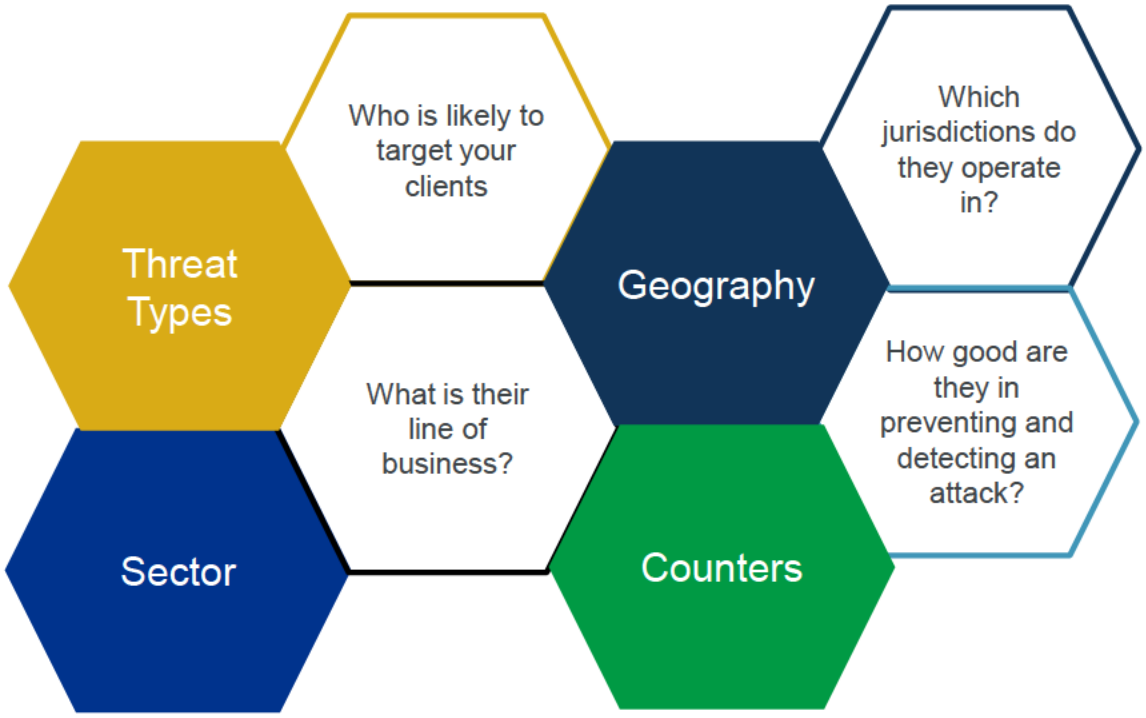
- Geeks
- What on earth are they talking about?
- How can they possibly form views based on barely any data?

Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

Cyber Expert's Point of View

Dimensions to cyber risk



Institute and Faculty of Actuaries

Threat Types

Who would target you, your clients and why?

Organised crime – Global, difficult to trace and prosecute

Motivation: Financial advantage

Impact to business: Financial loss

Competitors – Competition or rivalry

Motivation: Gain business edge

Impact to business: IP theft, reputation damage

The insider – Intentional or unintentional

Motivation: Grudge, financial gain

Impact to business: Distribution or destruction, theft of information, reputation loss

Hacktivism – Hacking inspired by ideology

Motivation: Shifting allegiances – dynamic, unpredictable

Impact to business: Public distribution, reputation loss

State-sponsored – Espionage and sabotage

Motivation: Political advantage, economic advantage, military advantage

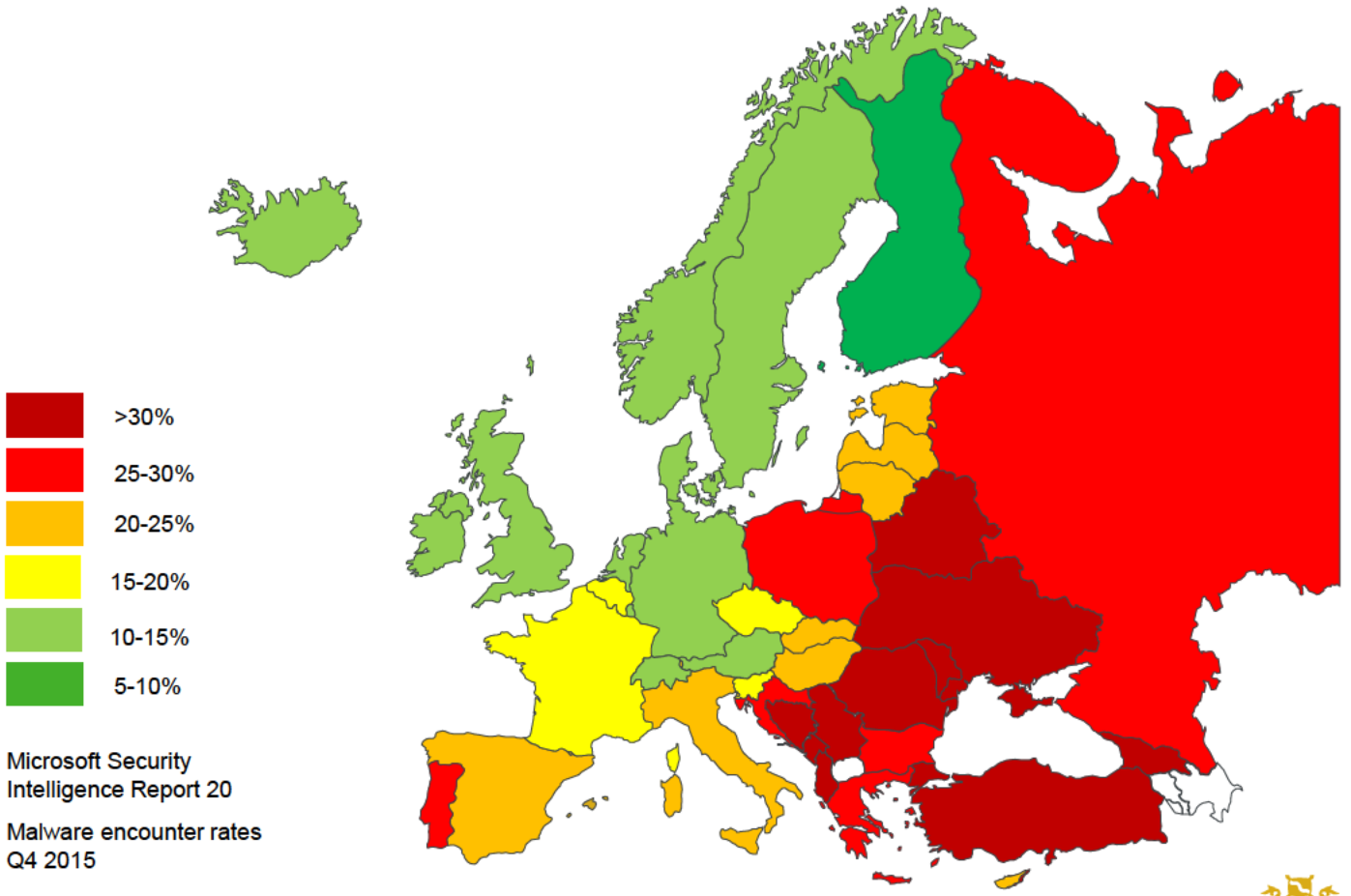
Impact to business: Disruption or destruction, theft of information, reputational loss

Institute and Faculty of Actuaries

Ruthless and Rationale Entrepreneurs

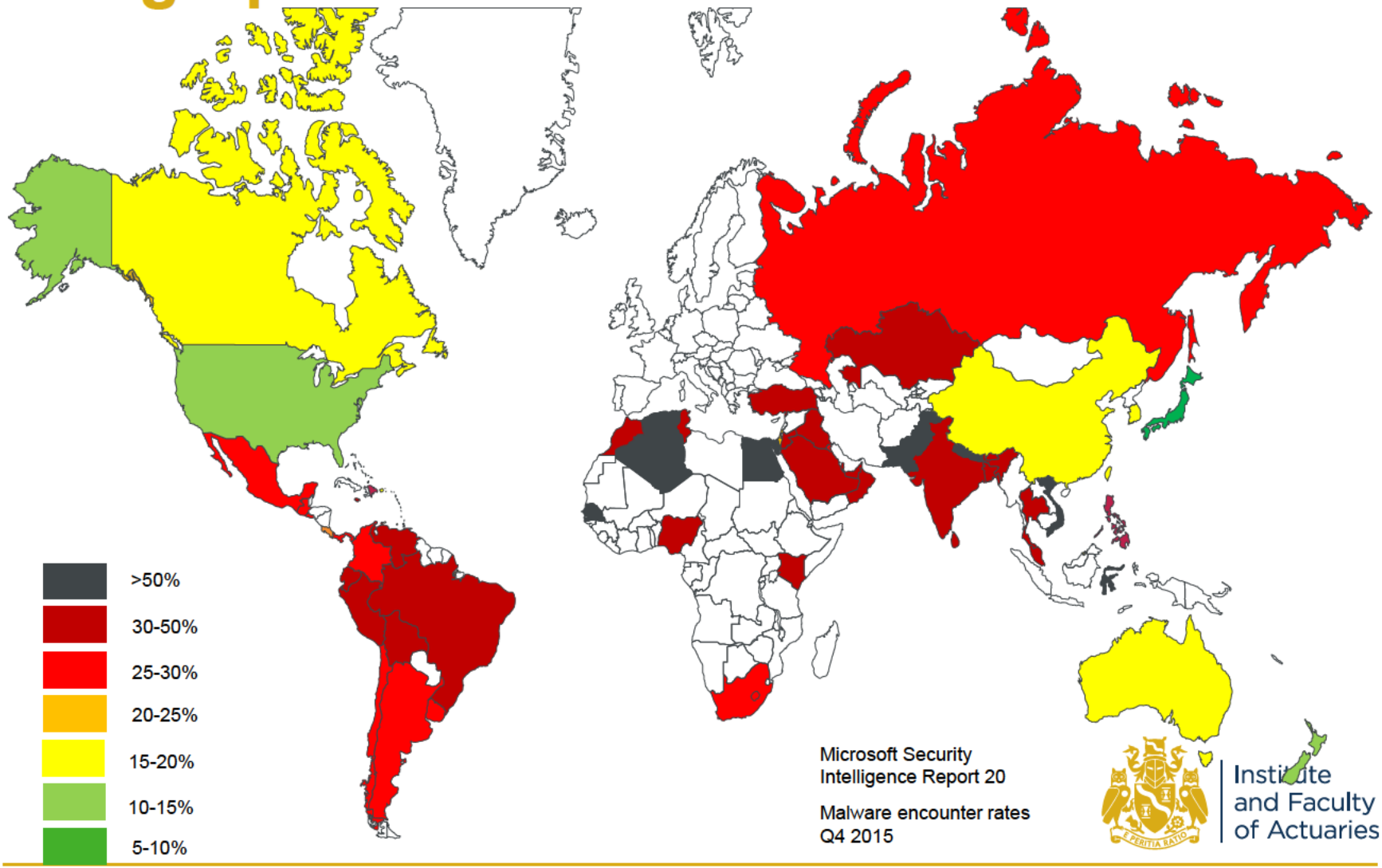
Institute and Faculty of Actuaries

Geographic Distribution - Europe



Institute and Faculty of Actuaries

Geographic Distribution – Rest of World



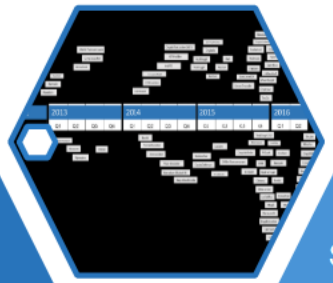
Microsoft Security Intelligence Report 20

Malware encounter rates Q4 2015

Institute and Faculty of Actuaries

Ransomware

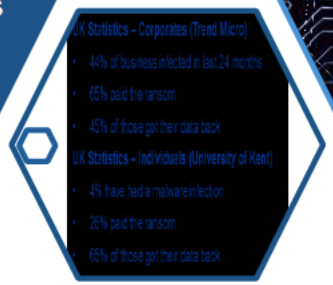
Major growth in range of groups and tools since Oct 2015



44% of business hit in last 24 months

Most pay up

Small ransoms often only 1 bitcoin



Particular threat to hospitals

Large scale extortion attacks

COMMODITY

Institute and Faculty of Actuaries

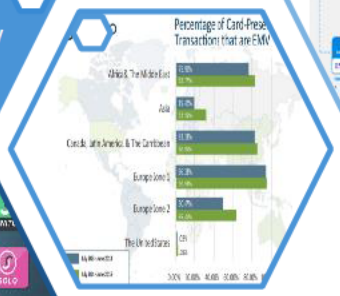
Payment card attacks

EFTPOS remains a concern – although awareness has risen post Target

Roll-out of EMV (Chip and Pin) is helping – now US has shifted liability

Fraud levels remain stubbornly high (30-100bps)

Complex liability model



Card not present frauds are biggest growth area

But beware unlimited cash outs – banks can be a weak link

TAILORED

Institute and Faculty of Actuaries

Broader industry attacks

Criminals now looking beyond financial sector

CEO and business email compromise fraud now rampant

FBI warn received fraud reports totalling $3.1 Billion

Recent example of $44 million fraud

Attacks now tailored to firms, their business and their employees

LinkedIn

Sophisticated social engineering

Networks of call centres

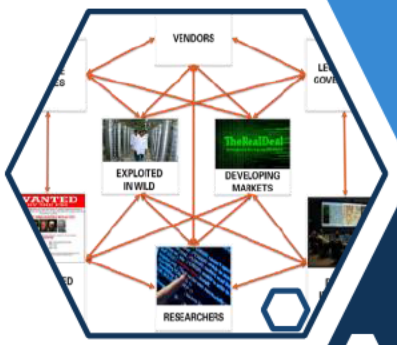
TAILORED

Institute and Faculty of Actuaries

Persistent and targeted attacks

SWIFT attacks followed

Attempted $951M fraud at Bank of Bangladesh



$81M successfully transferred to Philippine casinos

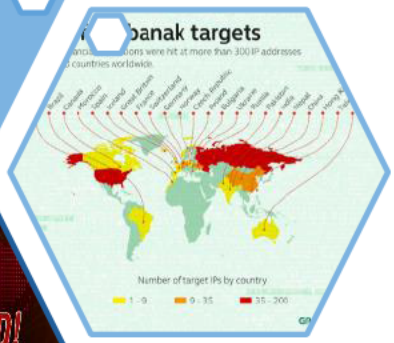
Other SWIFT attacks followed

Weak links?

Speculation over criminal and State links and flow down of techniques

Carbanak signalled a new type of attack

Persistent and stealthy



HIGH END

Institute and Faculty of Actuaries

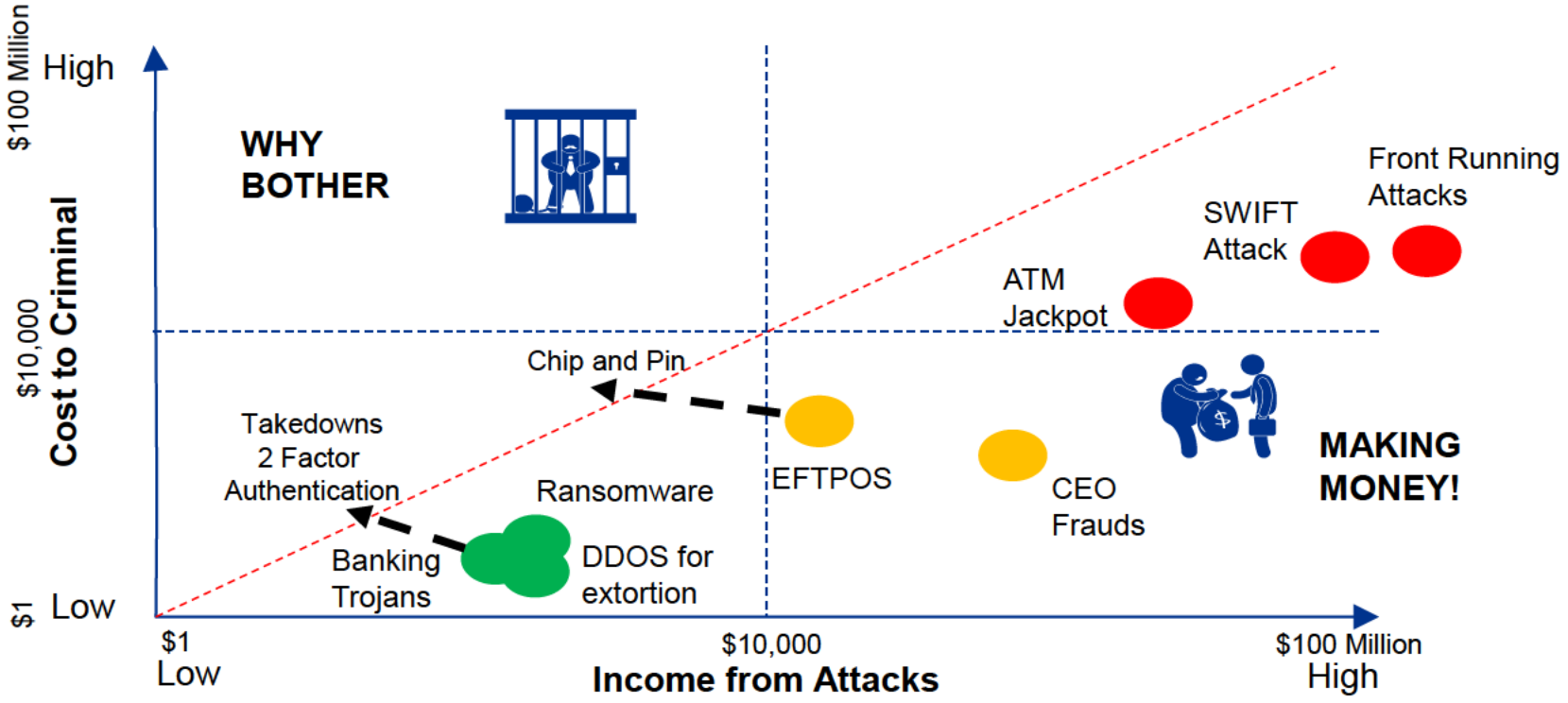
Sector Characteristics

Different attack patterns and severity profiles

- Utilities
- Transport
- Media & Telecommunications
- Arts & Entertainment
- Agriculture
- Non Profit
- Health
- Education
- Construction
- Manufacturing
- Mining
- Hospitality
- Retail
- Government
- Banking & Finance
- Defence

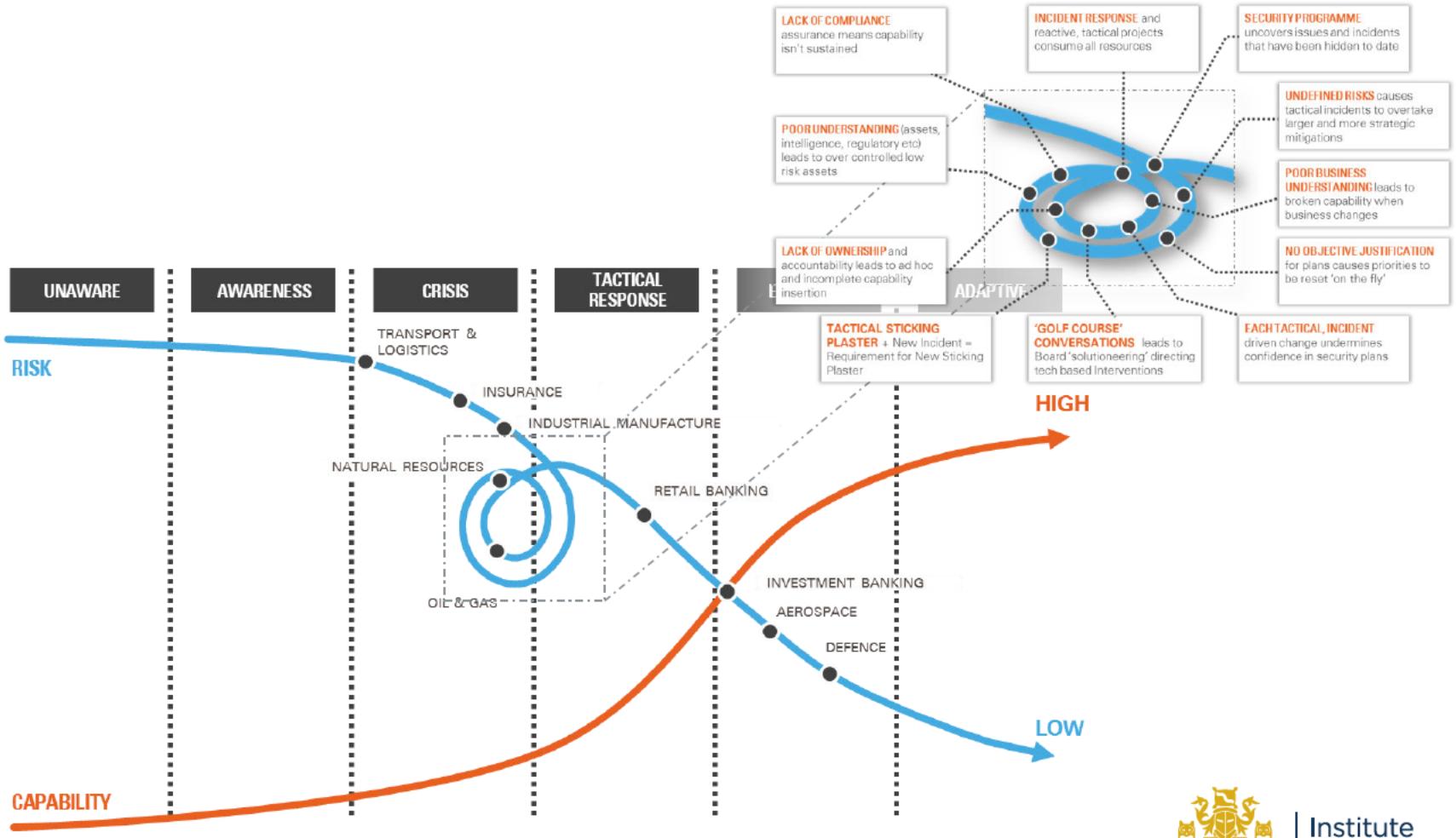
Institute and Faculty of Actuaries

Return on Investment



Institute and Faculty of Actuaries

The Threat Keeps Changing….



Institute and Faculty of Actuaries

Institute
and Faculty
of Actuaries

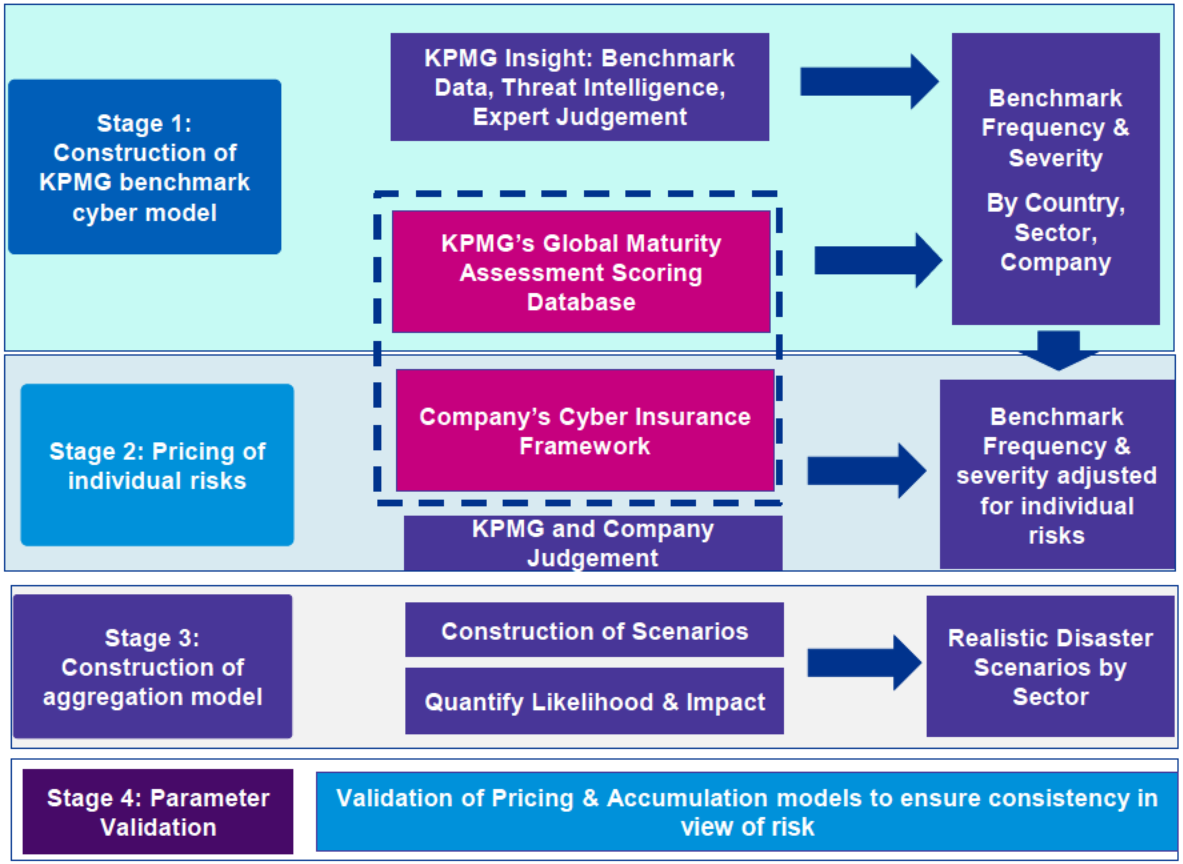
Modelling Approaches

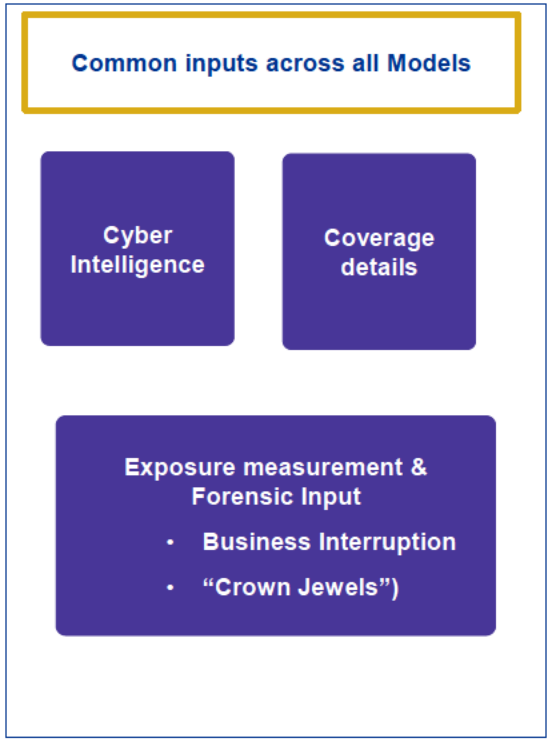
A Variety of Approaches

- Bespoke quantitative and/or qualitative solutions (Primary Insurers/MGAs)
- "Cat models" to assist with accumulation/aggregation management
  - Brokers
    - AON
    - WTW
    - Marsh
  - Modelling Firms
    - AIR
    - RMS

KPMG Cyber Modelling Approach

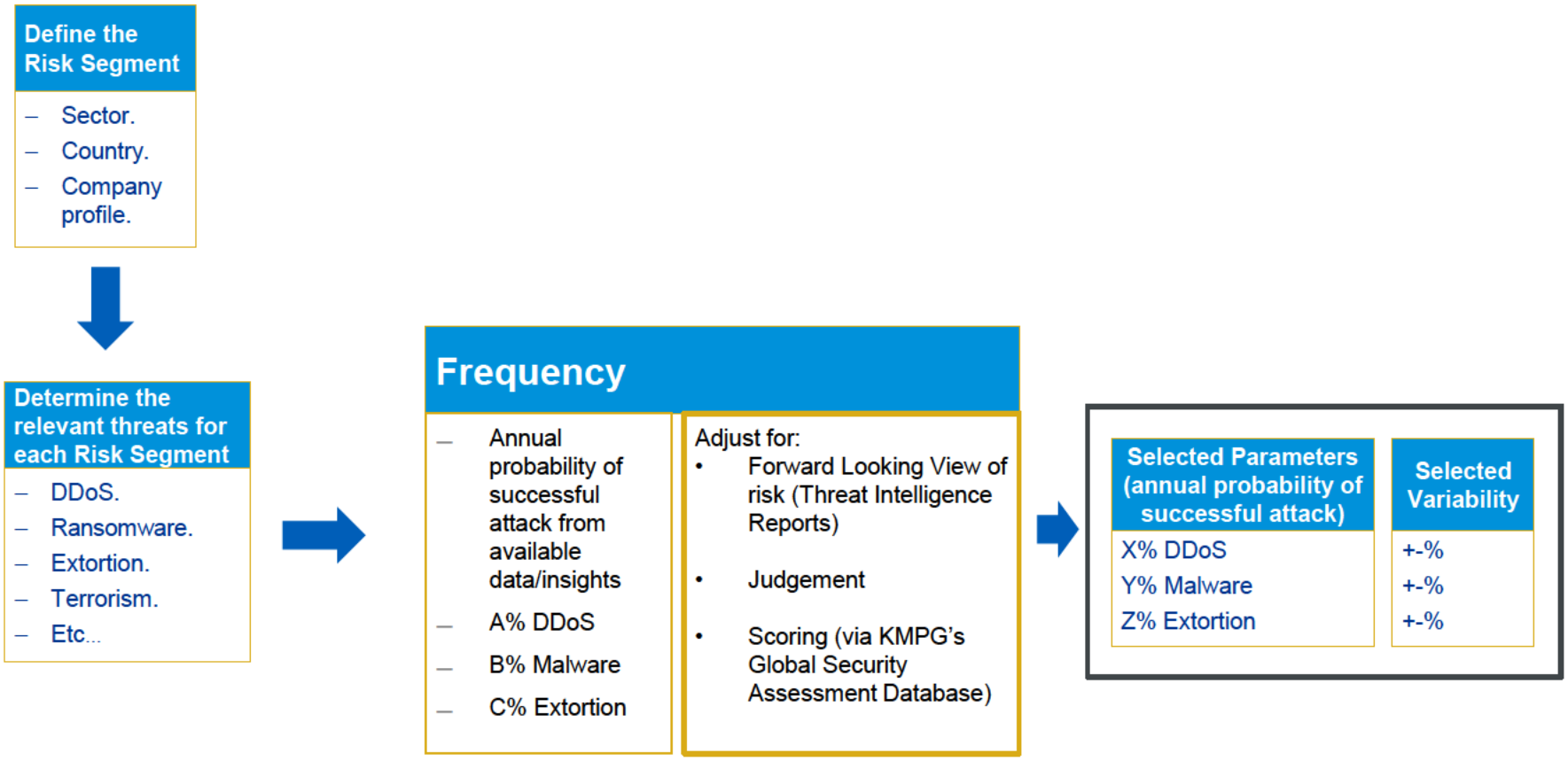
- We work with clients to develop bespoke cyber models.
- Our key strength and focus is on the parameterisation of models (either for pricing or accumulation management purposes)





Institute and Faculty of Actuaries

KPMG Benchmark Cyber Model Output - Example



Institute and Faculty of Actuaries

KPMG Benchmark Cyber Model Output – Example (Cont.)

Define the Risk Segment

- Sector.
- Country.
- Company profile.

Determine the relevant threats for each Risk Segment

- DDoS.
- Ransomware.
- Extortion.
- Terrorism.
- Etc...

Severity

- Look at what the immediate effect is on the company
- Collect information that is a proxy for this effect

Create "model points" from each of the relevant threats to estimate costs split by heads of damage:

- Breach costs
- Fines
- Liability
- Etc…

Selected Parameters		Selected Variability
DDoS	$ $ $	+-%
Malware	$ $	+-%
Extortion	$ $ $	+-%

Institute and Faculty of Actuaries

KPMG Benchmark Cyber Model Output – Example (Cont.)

Selected Parameters (annual probability of successful attack)	Selected Variability
X% DDoS	+-%
Y% Malware	+-%
Z% Extortion	+-%

Selected Parameters	Selected Variability
DDoS $ $ $	+-%
Malware $ $	+-%
Extortion $ $ $	+-%

Simulation

- Individual Risk Pricing
- Validation of reserving IELRS
- Capital Modelling

Institute and Faculty of Actuaries

Example of Extreme Event Analysis

Probability of Compromising general IT infrastructure	×	Rising Trend in attacks	×	Probability of destructive attack	×	Probability of Breaking into OT environment	×	Adjustment factor to allow for entry via other routes
This is based on market statistics and reflects the recorded successful attacks on the general IT infrastructure of a company.		Increasing trend in attacks over the past 12-24 months. This factor allows for this trend to continue in the next 12 months, and derived using expert insight and experience		This step is to reflect the fact that only a subset of the observed attacks relate to a malicious attack.		Attacks on the Operational Technology systems, which control key assets, are the most significant.		Attacks can also happen via third party vendors who act as subcontractors. This risk is increased if systems are centralised.
A%	×	B%	×	C%	×	D%	×	E%
							=	Frequency

Type of loss	Impact ($000s)
Property	615
Loss of life	30
Repair costs and patches for IT and OT systems	5
Own company's business interruption costs	13,850
Environmental impact plus third party business interruption	20,000
Clean-up costs	11,200
Regulatory fines	1,000
D&O claims	5,000
Total	**51,700**

Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

Conclusion

Conclusion

- Variety of underwriting approaches
- Data is an issue but there is a starting point
- Forming a forward looking view is key. Cyber threats are evolving fast.
- Different modelling approaches are being developed
- The insight from cyber security experts is available and we should embrace them

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