Symantec.

Where Cyber Security Meets Insurance:
Challenges Presented and Opportunities Created

October 2016

Contents

1 State of Cyber Insurance Market

2 Considerations and Challenges

3 Differences Between Cyber and Other LOBs

Cyber is one of the most attractive opportunities to emerge in the global insurance industry in decades

> “This is the hottest insurance product that has come out in my 40-year career”
>
> **- President, Betterley Risk Consultants**

> “It is very rare in an insurance person's career that a new product not only takes off but provides real benefit and value to the insureds, that's seen as a must-have product.”
>
> **- Paul Bantick, Beazley**

> “Cybersecurity insurance has a very, very bright future for insurers … it fills a gap, a void, that virtually every business in America has”
>
> **- CEO, Insurance Information Institute**

Cyber crime costs **>$400B** per year but **<1%** is covered by insurance today

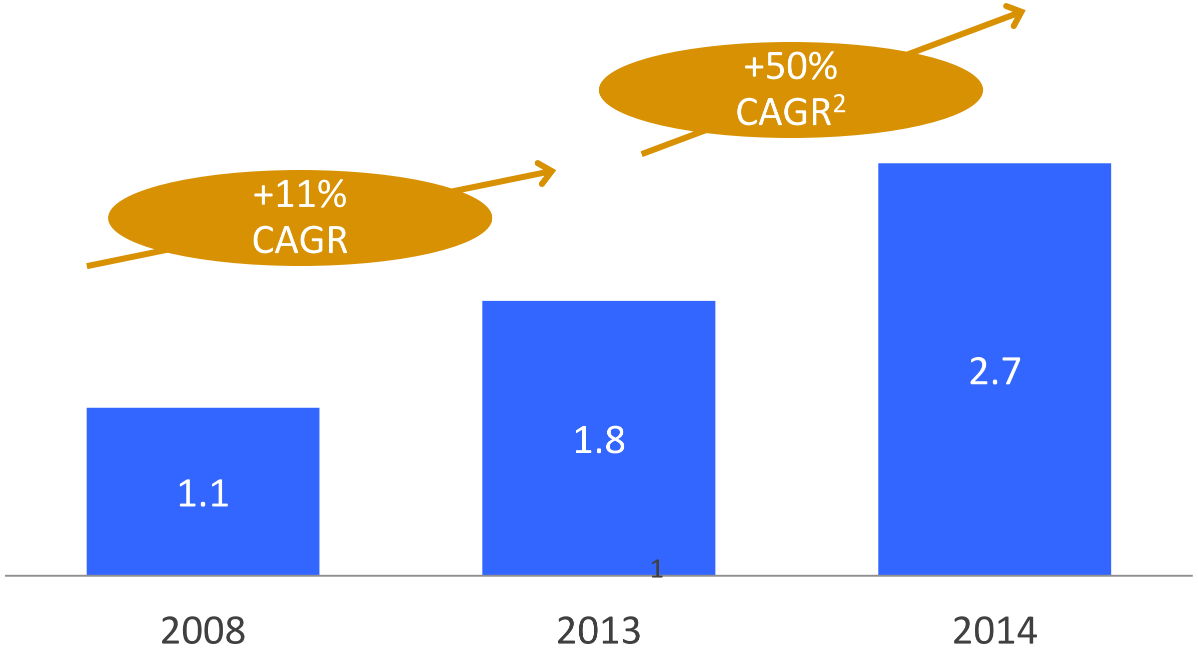
35-50% premium revenue growth per year, expected to grow to **$10-15B+**

>800 $1B+ revenue companies buying cyber insurance in next **3** years

Limited focus on consumer and micro-business to-date

Cyber insurance: $2.7B market experiencing rapid growth and expected to at least triple in size within 5 years

Global cyber insurance market
Gross written premiums (US$B)



- Market dominated by the US
  - 85% US
  - 10% EU (rapid growth expected)
  - 5% Rest of World
- High demand from clients, with annual growth estimates from 2016 onwards ranging from 35-50%
- Industry projected to be between 3-8x the size within 5 years, or $7-20B globally

[1] IBIS estimate of $2B vs $1.8B for UK Government/Marsh report
[2] UK Government/Marsh global estimate of 50%, Betterley report estimate of 35%

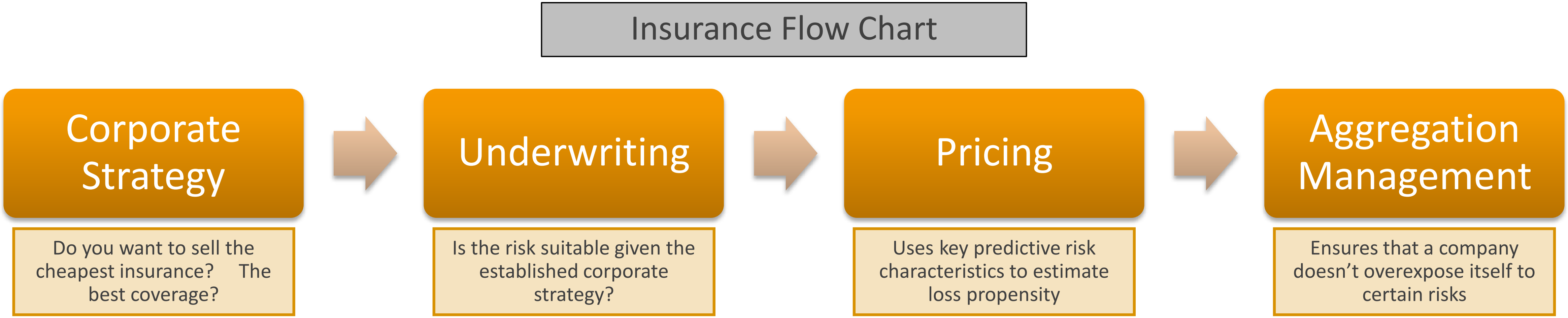
SOURCE: UK Government / Marsh Global Cyber Insurance Report (March 2016); IBIS World (2014); press reports; Allianz (2015); expert interviews

The explosion of IoT is creating a need for a market

What Is At Risk?

- Individual
  - Savings
  - Safety (e.g. compromised car)
  - Reputation (i.e. identity theft)
- Enterprise
  - Assets (e.g. intellectual property, customers list/records, money, physical assets)
  - On-going operations (e.g. website down for e-commerce, ransomware)
  - Reputation
  - Employees’ safety
- Insurance Industry
  - Inability to properly assess/quantify cyber risk
  - Solvency (i.e. individual companies/industry)

Challenges to Writing Cyber Insurance



Insurance Flow Chart

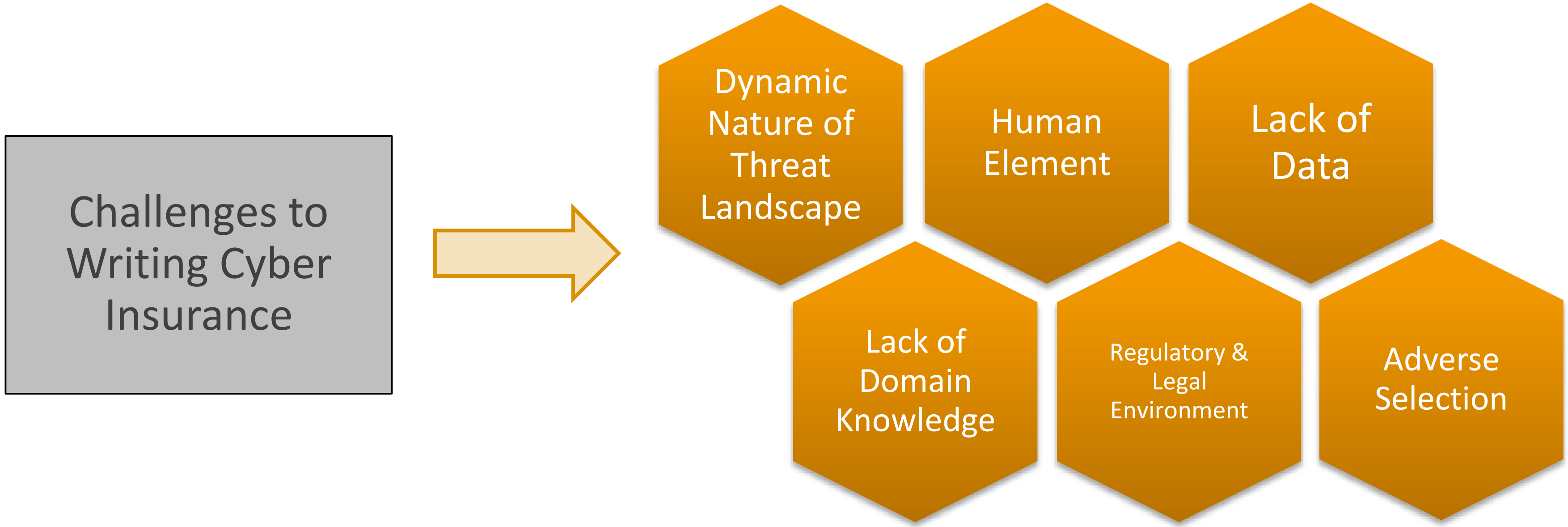
Corporate Strategy → Underwriting → Pricing → Aggregation Management

Corporate Strategy: Do you want to sell the cheapest insurance? The best coverage?

Underwriting: Is the risk suitable given the established corporate strategy?

Pricing: Uses key predictive risk characteristics to estimate loss propensity

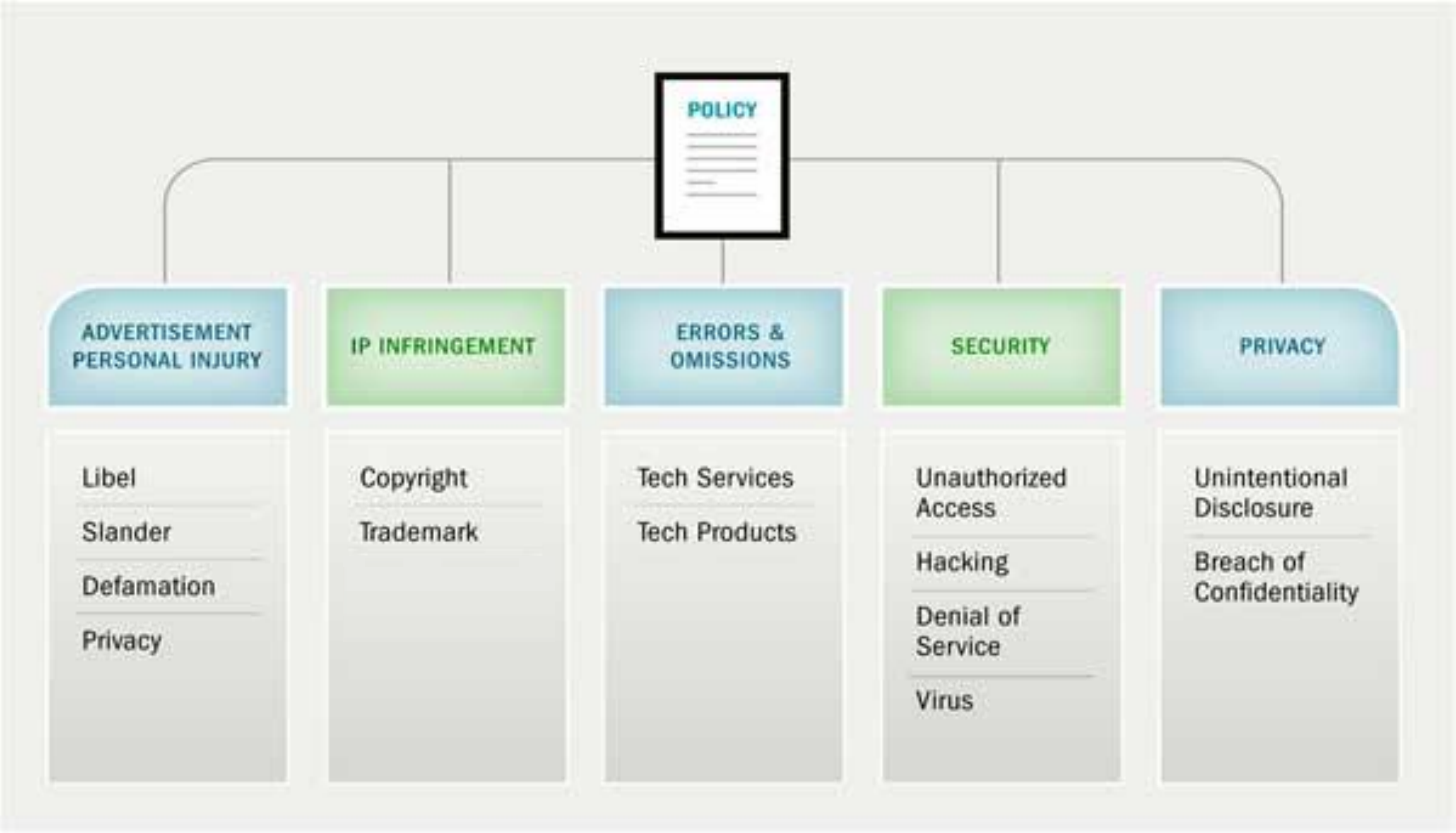
Aggregation Management: Ensures that a company doesn't overexpose itself to certain risks



Challenges to Writing Cyber Insurance →

- Dynamic Nature of Threat Landscape
- Human Element
- Lack of Data
- Lack of Domain Knowledge
- Regulatory & Legal Environment
- Adverse Selection

What does Cyber Insurance Cover?

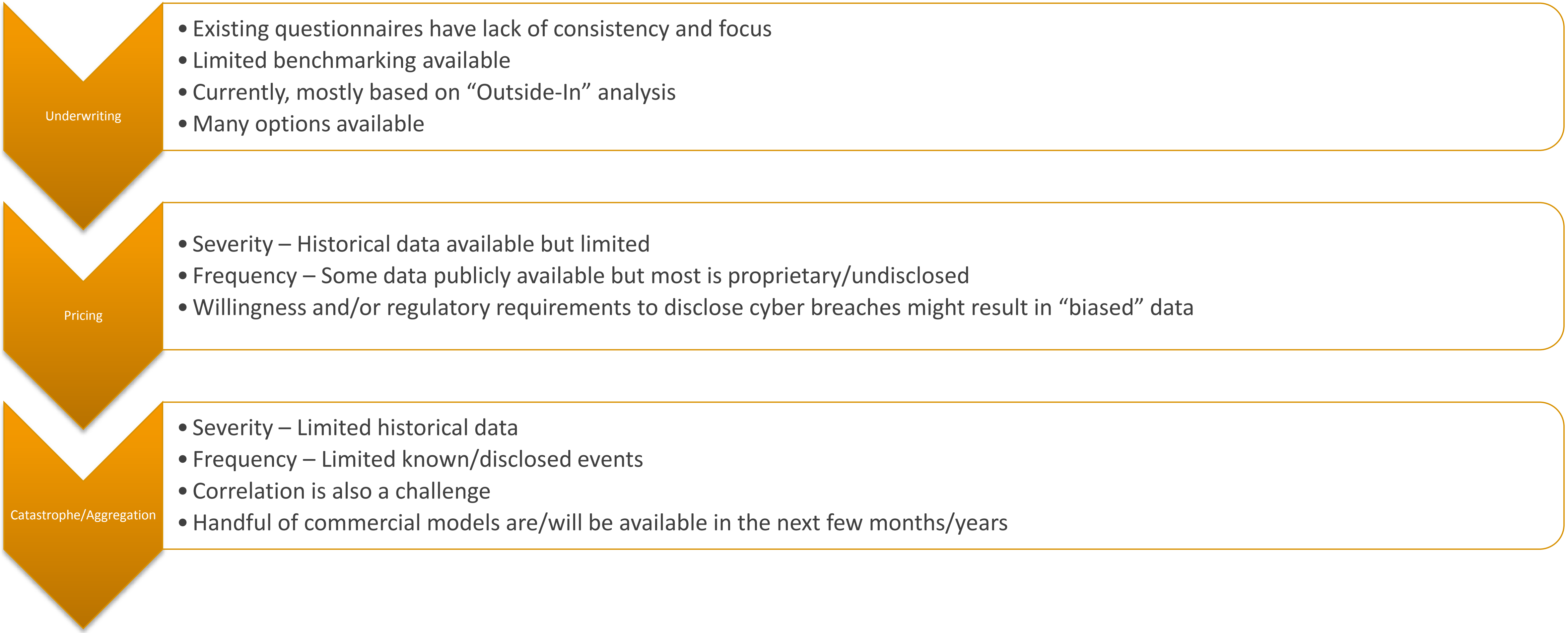


POLICY

ADVERTISEMENT PERSONAL INJURY	IP INFRINGEMENT	ERRORS & OMISSIONS	SECURITY	PRIVACY
Libel Slander Defamation Privacy	Copyright Trademark	Tech Services Tech Products	Unauthorized Access Hacking Denial of Service Virus	Unintentional Disclosure Breach of Confidentiality

©2008 Carpenter Moore, a NASDAQ OMX Company

Tools and Models – Similar to other types of insurance



Underwriting

- Existing questionnaires have lack of consistency and focus
- Limited benchmarking available
- Currently, mostly based on “Outside-In” analysis
- Many options available

Pricing

- Severity – Historical data available but limited
- Frequency – Some data publicly available but most is proprietary/undisclosed
- Willingness and/or regulatory requirements to disclose cyber breaches might result in “biased” data

Catastrophe/Aggregation

- Severity – Limited historical data
- Frequency – Limited known/disclosed events
- Correlation is also a challenge
- Handful of commercial models are/will be available in the next few months/years

Tools and Models – Underwriting

Questionnaire

- Should focus on quality over quantity
- Need for monitoring: Good risk one day, good risk everyday … not the case!

“Outside-In” analysis

- Security posture based on publicly available information
- Provides good information but accuracy is not unanimous (and focus is not given to physical security)
- “Inside-out” provides valuable information

Availability

- Multiple options available for tools based on “outside-in” analysis
- Work being done to include “inside-out” and benchmarking

Tools and Models – Pricing

Demographics

- Industry
- Size (e.g. employee count, # end-point devices, # financial transactions)
- Location(s)
- Public or private

Financials

- Revenue
- Surplus / Equity
- “Asset value” at risk (e.g. # of PHI, PII, PCI records stored)

Security Posture / Technology

- Categories of software used
- Encryption practices
- User behavior (e.g. downloads, websites visited)

Tools and Models – Aggregation/Catastrophe

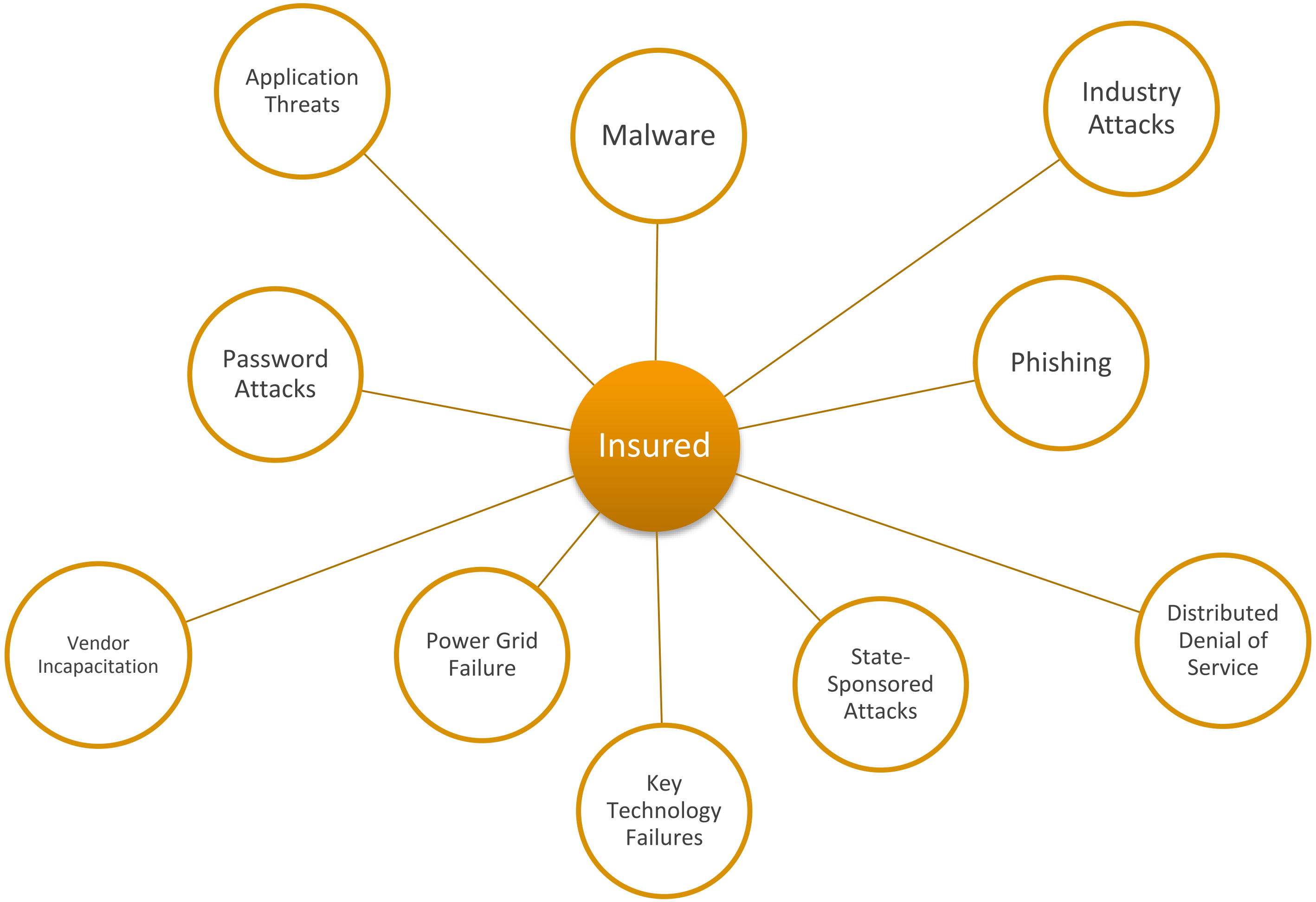
- Definition of “catastrophe”
- Risk identification is a challenge (i.e. what could go wrong?)
- Impact on portfolio (i.e. quantification)
  - Deterministic – How bad can it get?
  - Stochastic – Where’s the data?
- Understand exposure
  - “Stand-alone” cyber policies
  - Terms and conditions in non-cyber policies

Which coverages are triggered? Lack of standardization clouds the issue.

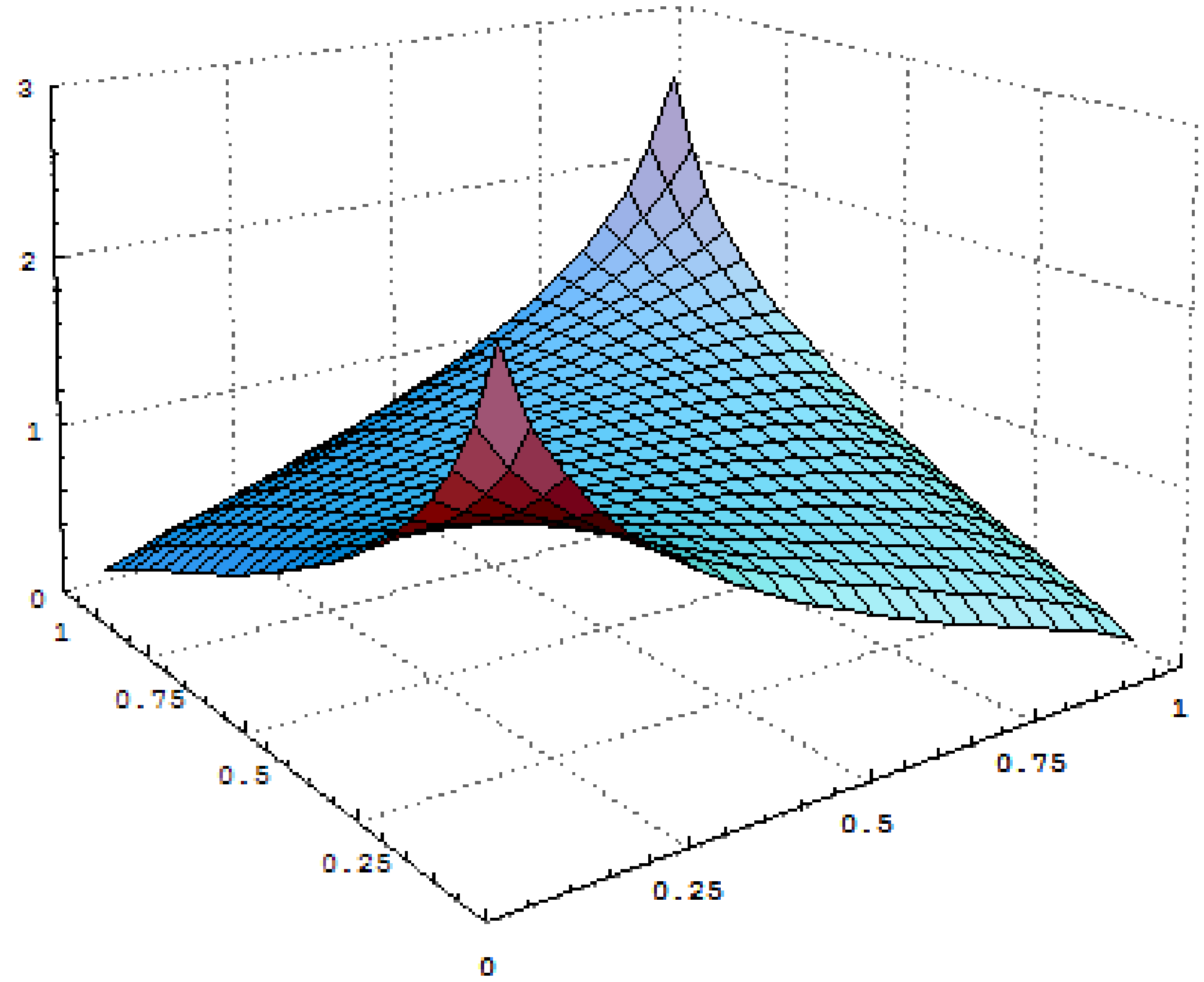
What about silent coverage?

	Property & Casualty									Life & Health	
Event	Affirmative Cyber	Property	Auto	Workers Compensation	Directors & Officers	Errors & Omissions	Business Owners	General Liability	Marine	Life	Accident & Health
Attack Scenario 1	x	x		x			x	x		x	x
Attack Scenario 2	x		x	x				x		x	x
Attack Scenario 3	x						x	x		x	x
Attack Scenario 4	x						x	x			
Attack Scenario 5	x						x	x			
Attack Scenario 6	x						x	x			
Attack Scenario 7	x						x	x			
Attack Scenario 8	x						x	x			

Insureds Must Protect Against a Diverse Range of Attacks



Events may very well be correlated



We need data! How does regulation come into play?

Regulation to be aware of:

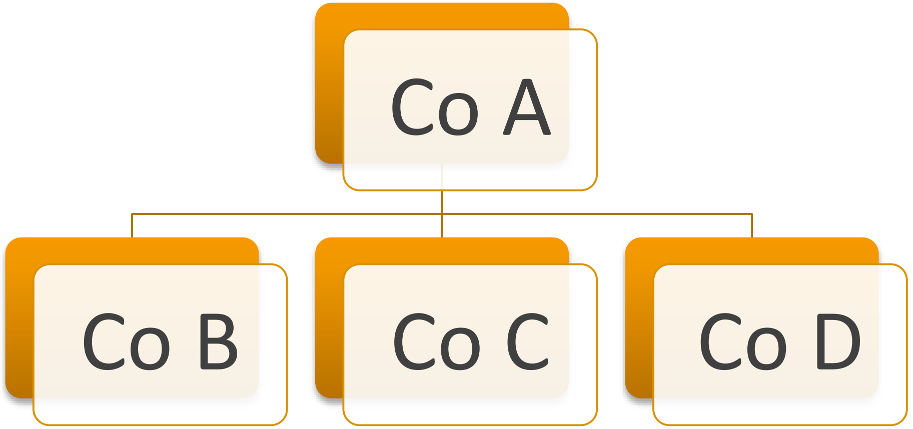
- EUGDPR regulation
- Insurance brokerage regulations (vs. marketing partnerships)
- Consumer regulation
- State vs. Federal Regulation

What is regulated?

- Pricing/Rating Variables
- Solvency
- Profit & Contingencies
- Breach Reporting Requirements

How we should define a catastrophe/aggregation event is unclear

VS.



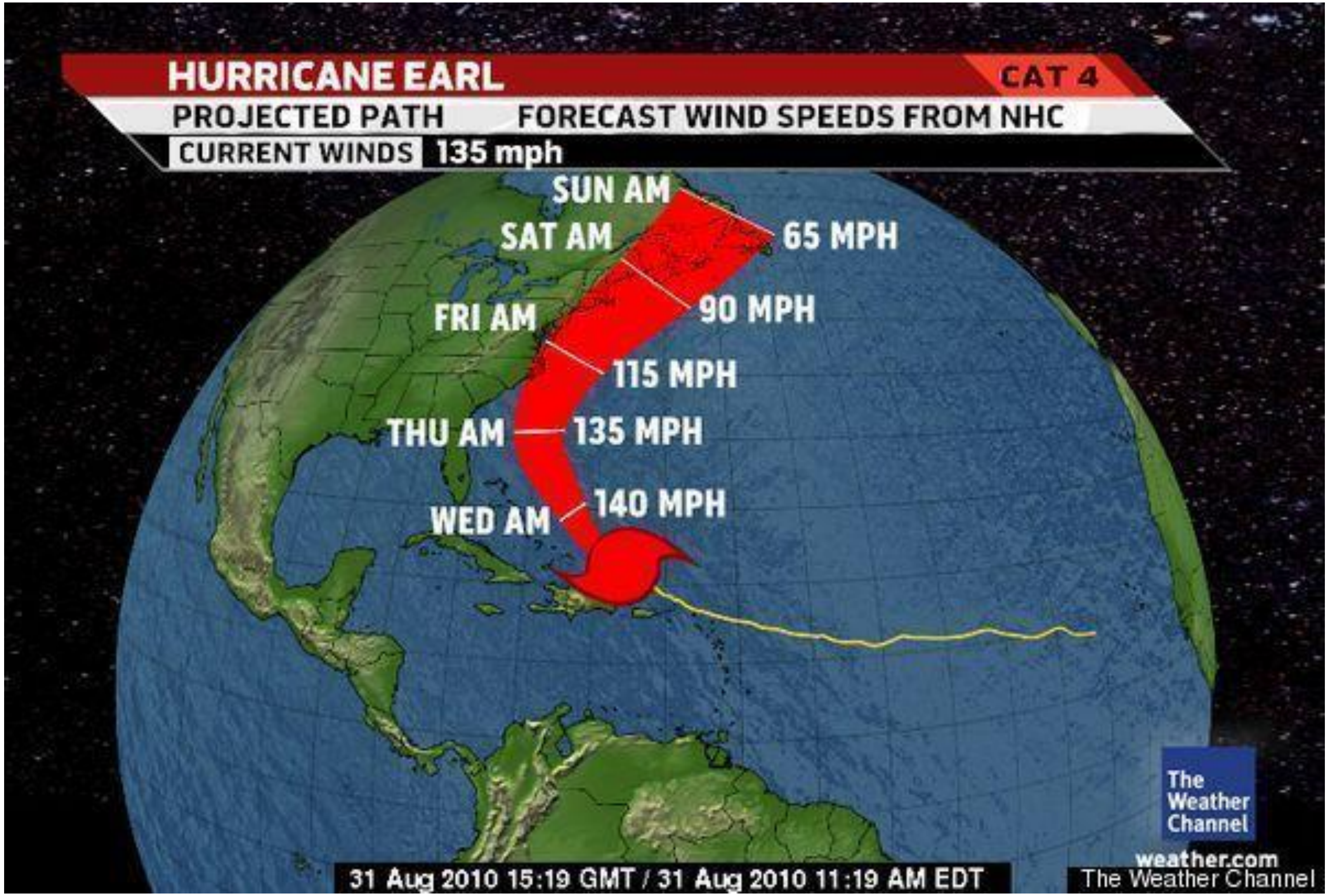
Co A

Co B

Co C

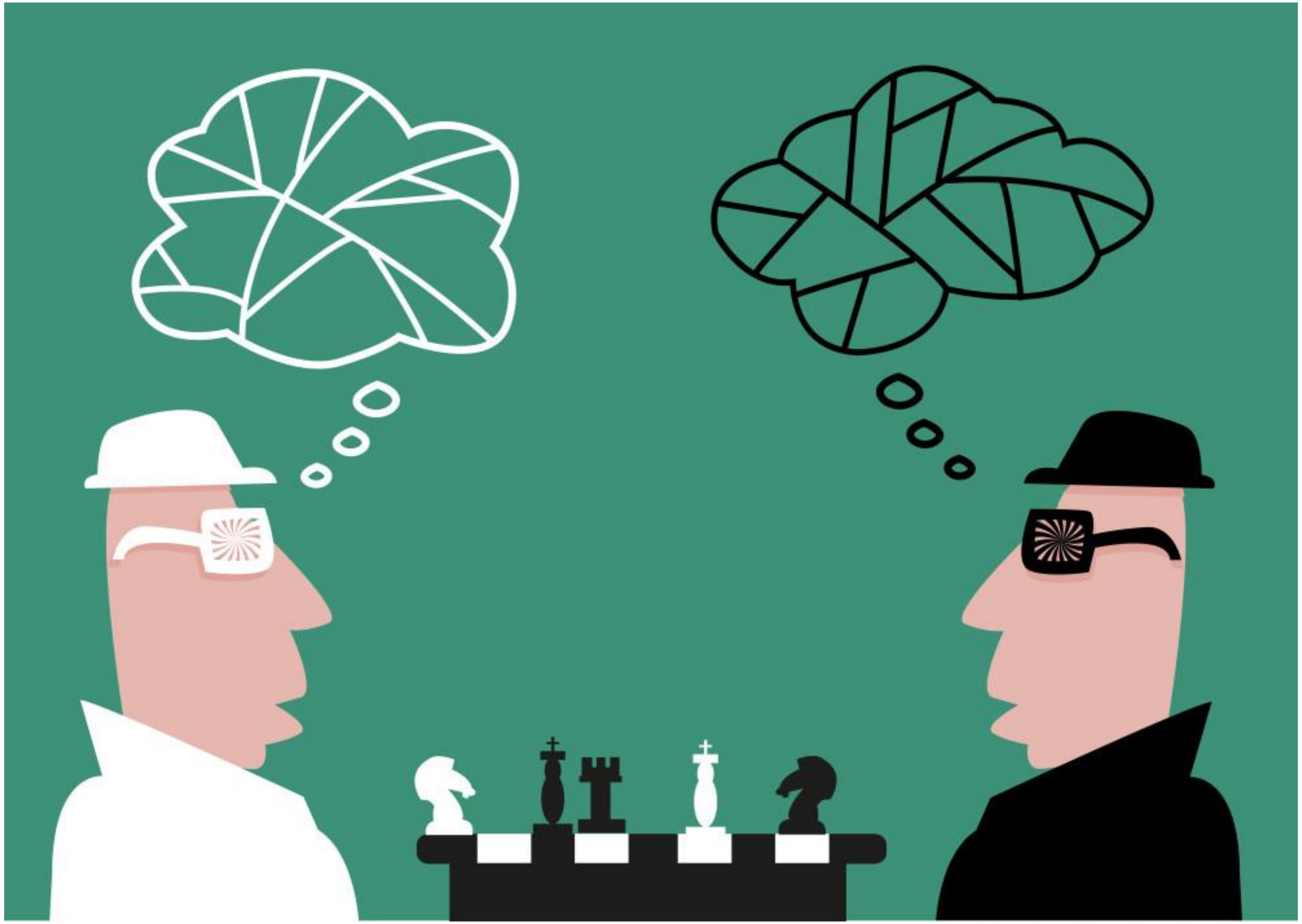
Co D

Traditional view of geography as a predictive variable

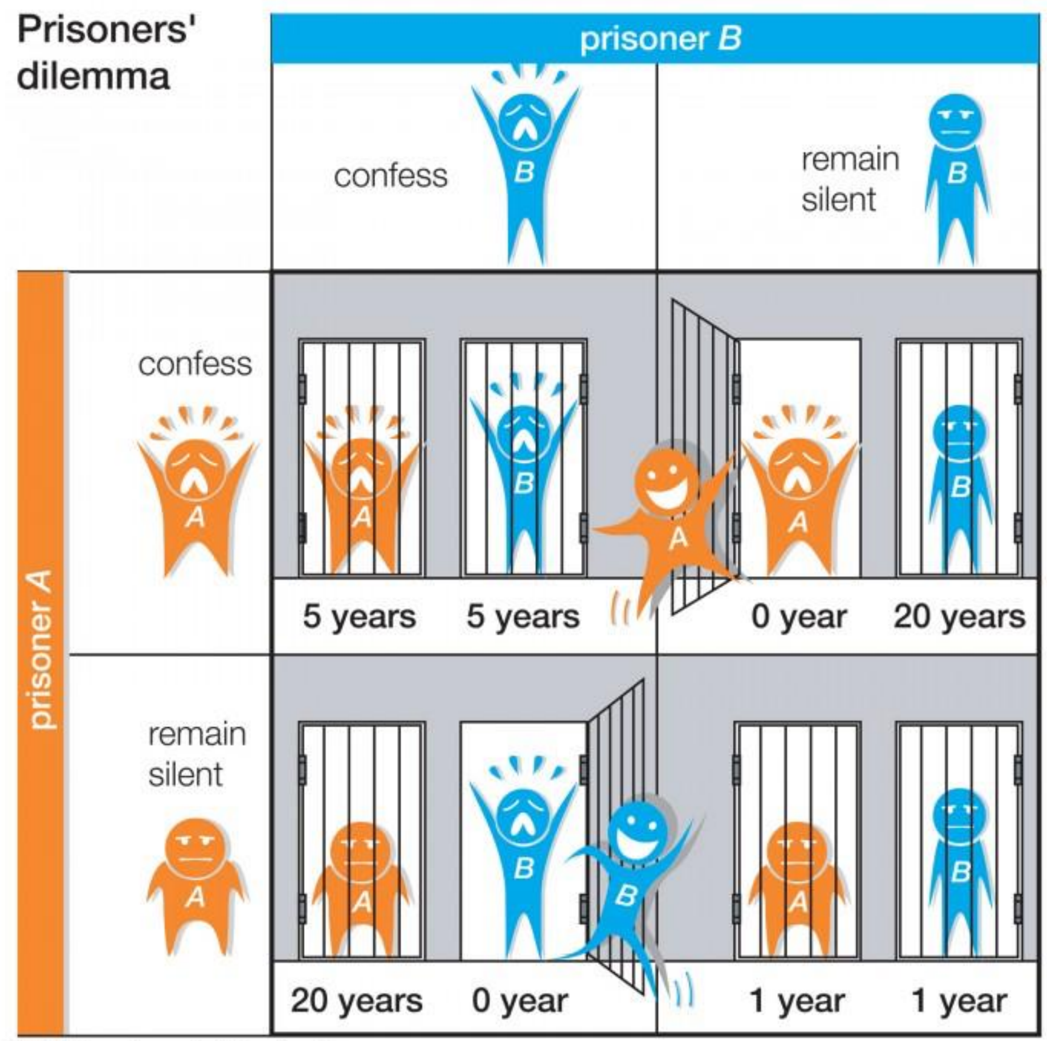


In a connected world, “geography” now takes on a new form…

Cyber Insurance contains a human element



What is Game Theory?



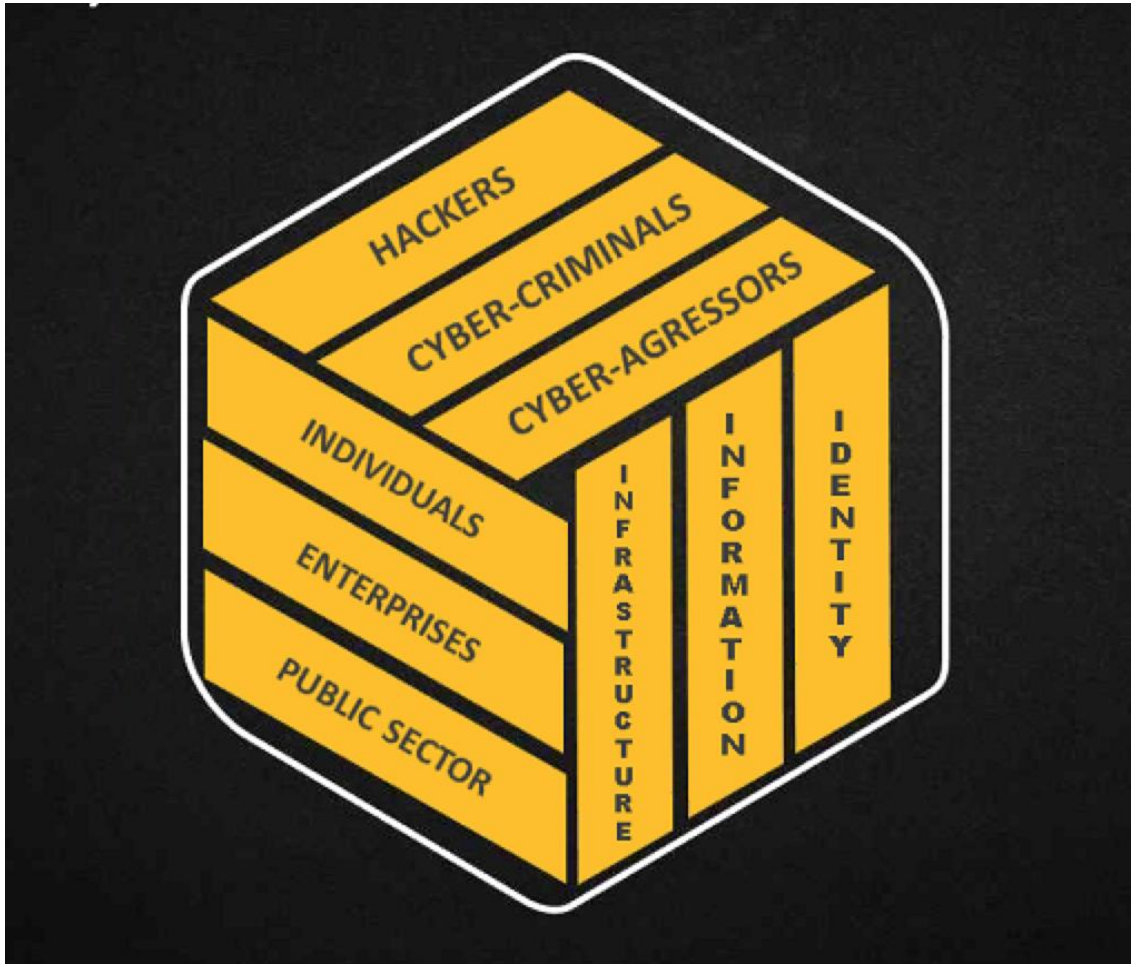
© 2010 Encyclopædia Britannica, Inc.

Cube Taxonomy Framework

Attackers

Targets

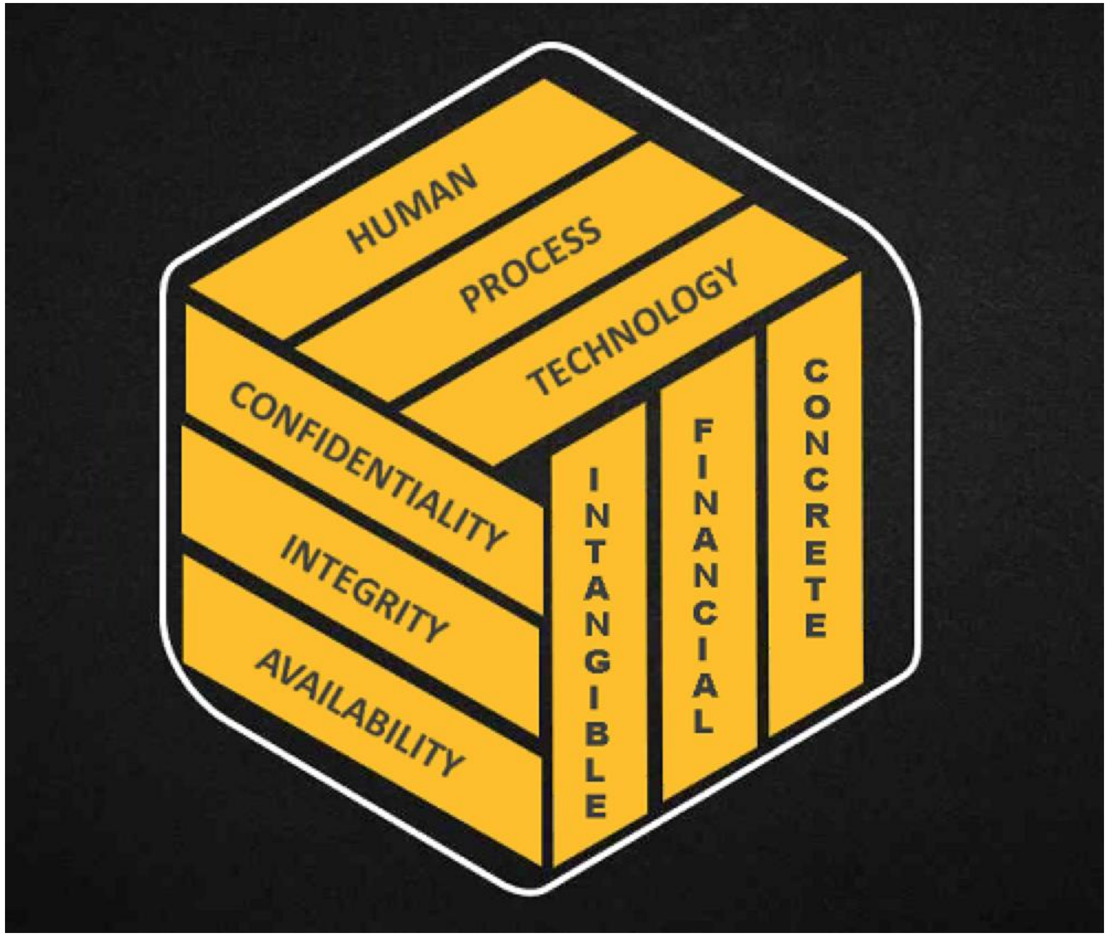
Objectives



Cube Taxonomy Framework (Continued)

Vulnerability

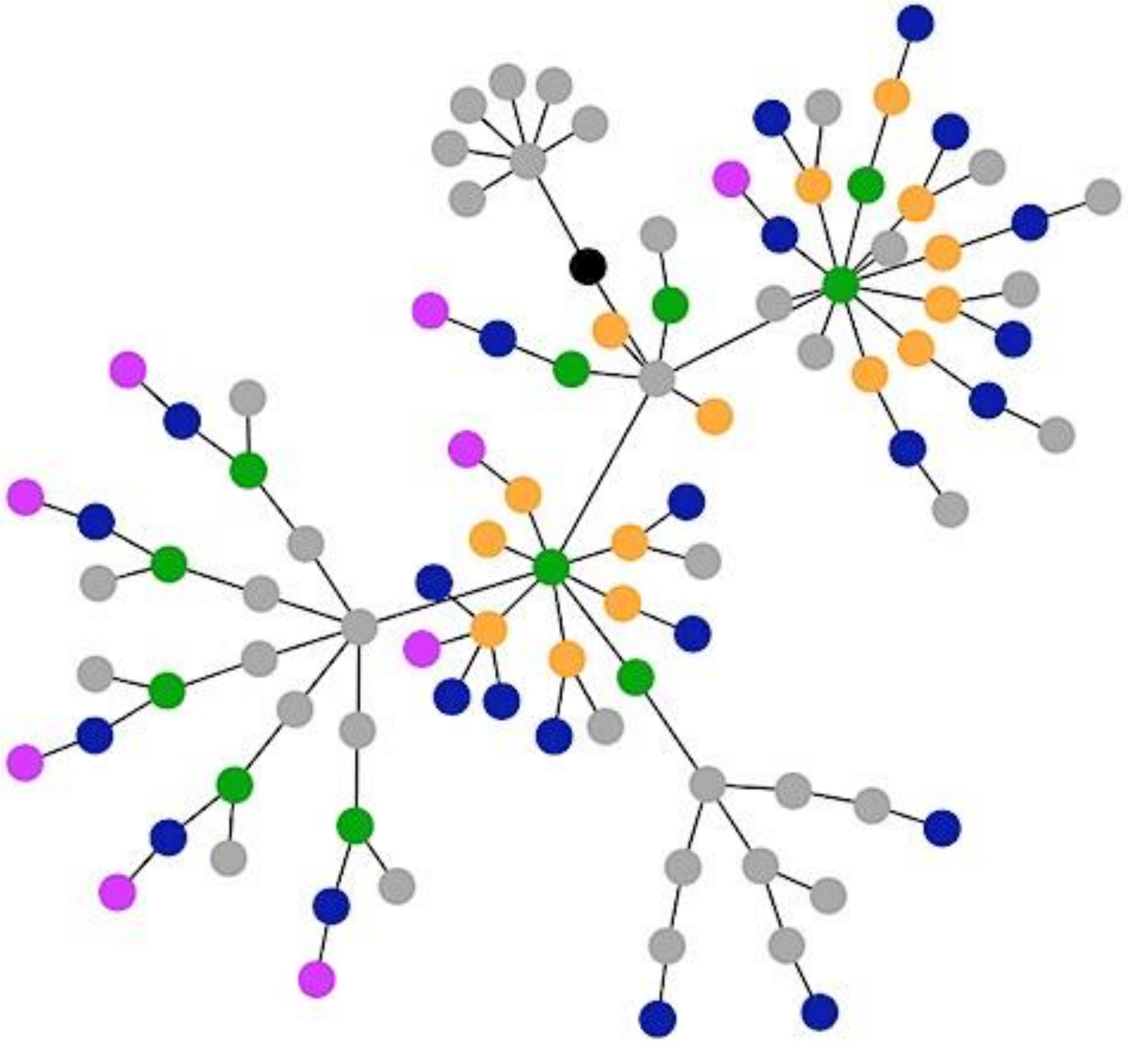
Impact



Consequences

What is your security posture?

An insurer must pay attention to insured relationships



Consumer cyber insurance – open questions in a new market

Example consumer coverage

- Phishing fraud
- Online reputation repair
- Virus removal
- Theft of devices
- Counseling for online bullying/abduction
- Identity theft

Questions being asked by insurers

- Are consumers sufficiently covered by existing policies/endorsements?
- Is there a market for more comprehensive standalone policies that bundle these together?
- What are the barriers to these policies?
- Is there a role for services provision within these policies?

Micro-business cyber insurance – open questions in a new market

Scope

- Single person owner-operators?
- 1-10 person small businesses without IT staff?

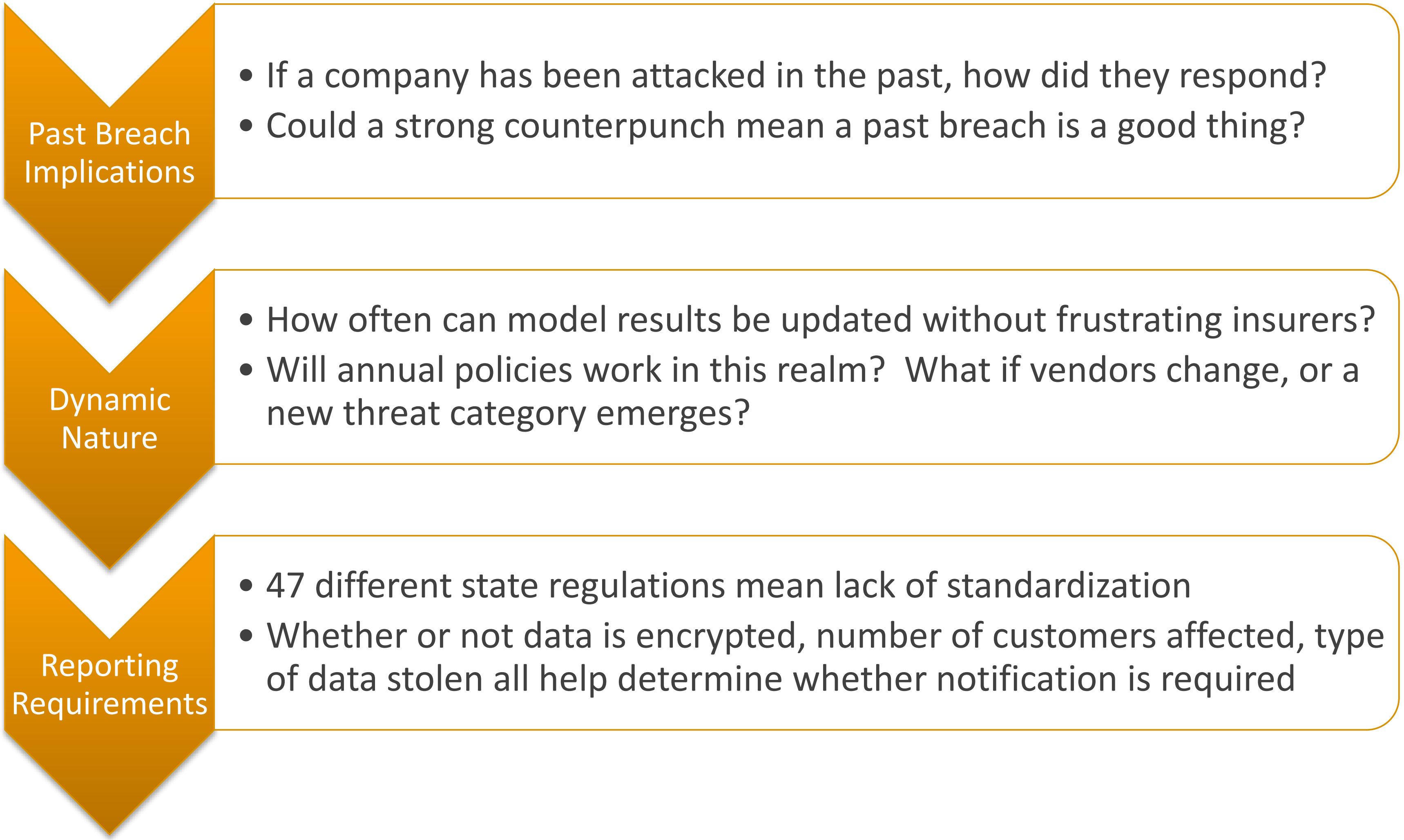
Coverage

- Data privacy policies? (incident response, breach notification, third party liability)
- Business interruption? (lost revenue)

Questions being asked by insurers

- Are small businesses sufficiently covered under existing business policies (e.g., “business owners policies”, policy endorsements)?
- Is there a market for standalone micro-business policies? If so, how should distribution for these policies work (presumably broker channel is cost prohibitive)?
- Operationally, how do mid-market policies need to be adapted for these micro-businesses (e.g., any underwriting, claims triage, incident response)?

Other Challenges and Considerations



Past Breach Implications

- If a company has been attacked in the past, how did they respond?
- Could a strong counterpunch mean a past breach is a good thing?

Dynamic Nature

- How often can model results be updated without frustrating insurers?
- Will annual policies work in this realm? What if vendors change, or a new threat category emerges?

Reporting Requirements

- 47 different state regulations mean lack of standardization
- Whether or not data is encrypted, number of customers affected, type of data stolen all help determine whether notification is required

Thank you!

SYMANTEC PROPRIETARY/CONFIDENTIAL – INTERNAL USE ONLY