QUANTAR®
INSURANCE RISK ANALYTICS

The Cyber Carrier Market 2020

Presented by : Dr. Phillip King-Wilson, Managing Director,
Quantar Solutions Limited
pkw@quantar.co.uk

May 2020

ORIGIN OF QUANTAR CYBER RISK VALUATION

EUREKO = EXTERNAL PROVIDER: CYBER SOLUTIONS
IP-TAP JERSEY / QUANTAR SOLUTIONS LIMITED

Poland PZU

UK FRIENDS PROVIDENT

The Netherlands achmea

Switzerland Die Mobiliar Versicherungen & Vorsorge

1999 Gothaer Re:
"Our corporate clients want cyber cover; How do we write it?"

Romania & Bulgaria EUREKO SİGORTA

France MAAF

Ireland Friends First

Sweden Länsförsäkringar Skåne

Portugal Millennium bcp

Slovakia Union Poisťovňa

Germany Gothaer

Denmark Topdanmark Forsikring • Pension

Luxembourg COLBERT LIFE LUXEMBOURG

UK F&C

Portugal ATLANTICO BANCO PRIVADO ATLANTICO

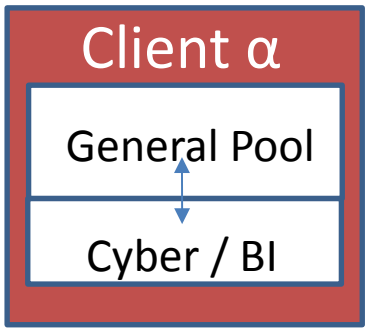
Greece INTERAMERICAN

The Netherlands Interpolis

Germany asstel Direktversicherer der Gothaer

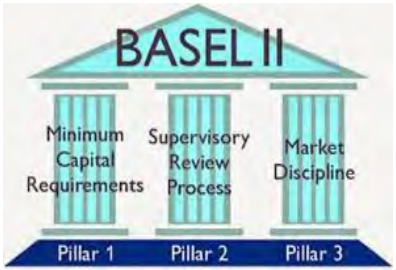
1999: How do we underwrite cyber?

Gothaer re ⇆ Gothaer ⇆ secunet ⇆



2004: How do we quantify I.T. risks for AMA?

BANK FOR INTERNATIONAL SETTLEMENTS ⇆



2009: Which model qualifies us for AMA SCR?

⇆

2002-18: How do we insure against non-compliance?

2019-on: What can we insure against?

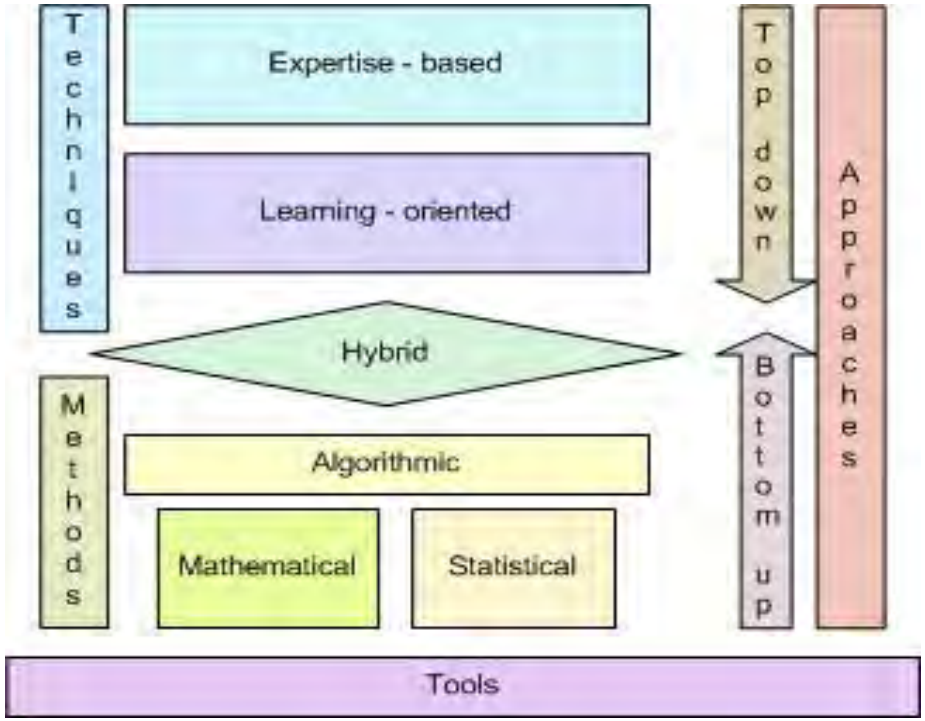
- Extra-territoriality
- OTT, IOT, M2M
- Metadata
- eMarketing

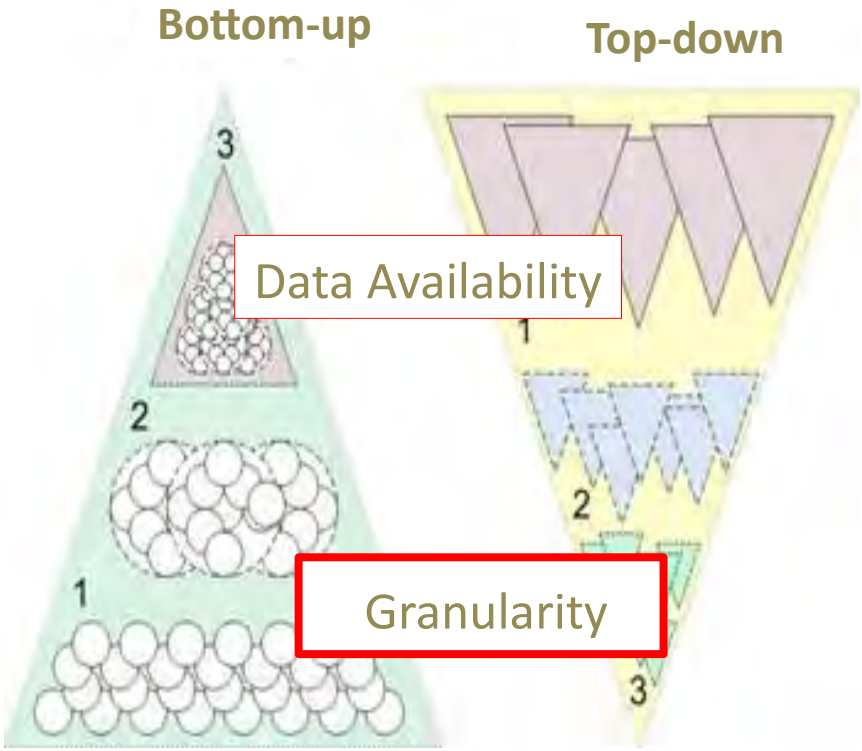
But What is Cyber?

	Includes	Insurable?
Business Interruption	✓	✓
Regulatory Compliance*	✓	✗
D&O	✓	✓
E&O	✓	✓
Enterprise Risk Management	✓	✓
Governance	✓	✗
Third Party Liability	✓	✓
Breach Response	✓	✓
Brand & Reputation	✓	✓
Extortion	✓	✓
Asset Theft/Damage	✓	✓

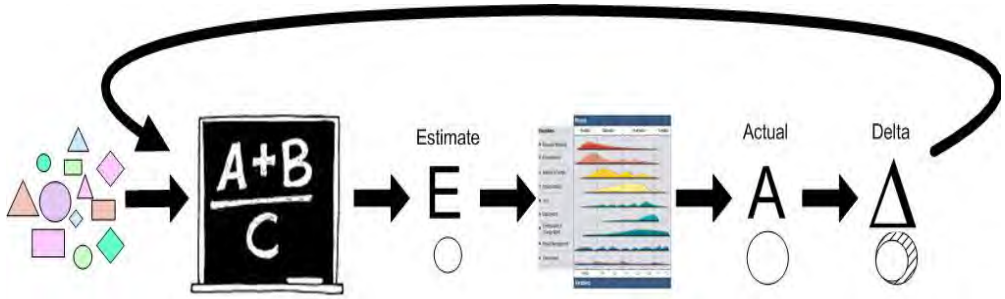
* Per-territory dependent

Two Approaches to Quantification & Valuation of Cyber Risks

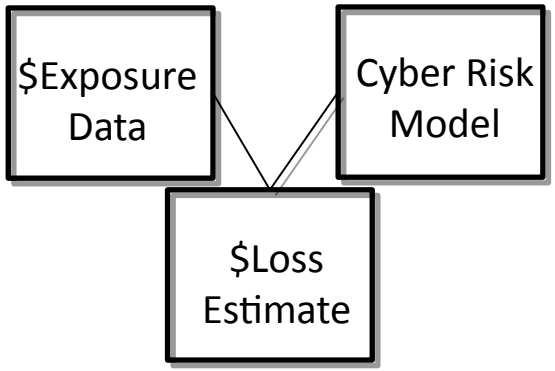




Current: Data Accumulation + Algorithmic Modelling + Comparison Against Actual



Current Basic Cyber Carrier Model



PRIMARY ISSUES FOR CYBER CARRIERS

Capacity

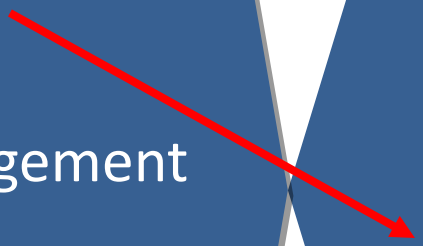
Pricing

Aggregation

Claims Management

Silent Cyber

Speed to Market of Evolving Technologies



What Data is Required?

Use High-Level Data & Modelling?

Degree of Granularity Required?

Is Peering a Reality?

Model Appropriateness?

Model From Effect Data or Causal Data?

"autopsy risk management"

UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for Risk Studies

TOP-DOWN RISK CARRIER PROPOSED SHARED MODEL 2016-18

CYBER INSURANCE EXPOSURE DATA SCHEMA V1.0

Advisen, AIR, AM Best, AON Benfield, AXIS Capital, Barbican Insurance Group, Guy Carpenter, Hiscox, JLT Specialty, Lloyds Emerging Risks, Lloyds Market, MS Amlin PLC, Munich Re, QBE, Reinsurance Assoc. of America, SCOR, Sompo Canopius Re, Renaissance Re, RMS, Talbot Underwriting, Tokio Marine, Willis, XL Catlin

1. Accumulation Focus

This initial development of the data schema will focus **on the data required for managing exposure accumulations**, rather than other areas of decision support, such as underwriting individual accounts, risk selection and pricing decisions.

- data requested by insurers for risk selection and pricing purposes varies widely and is regarded as competitive-advantage expertise.

4. Adopting a Categorization of Cyber-Induced Losses

- we may need to extend and improve granularity of the scheme, particularly for cyber liability-related loss coverages.

6.1.5 Cyber Security Assessment

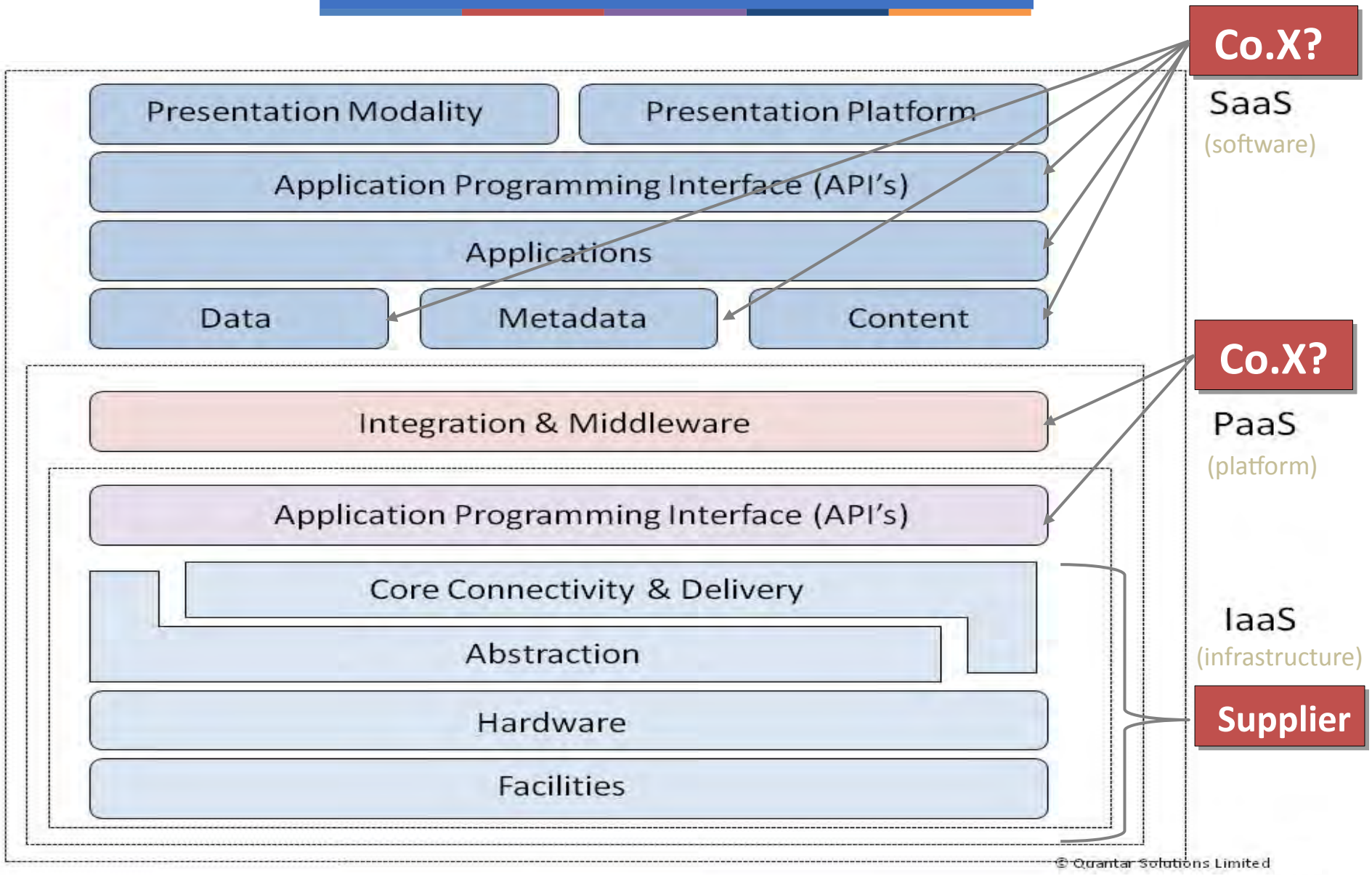
- The cyber security score should be defined in a supporting document for the counterparty in terms of ***the percentile of the total number of enterprises in that jurisdiction that are expected to qualify for that score***, ranked by quality of cyber security. For example, "A security score of XX means that this enterprise is in the top 10% of enterprises in the United States, ***ranked by quality of cyber security***."

Example of Basic Modelling Cyber Top-Down Issues: Entity Uses Cloud? Y/N?

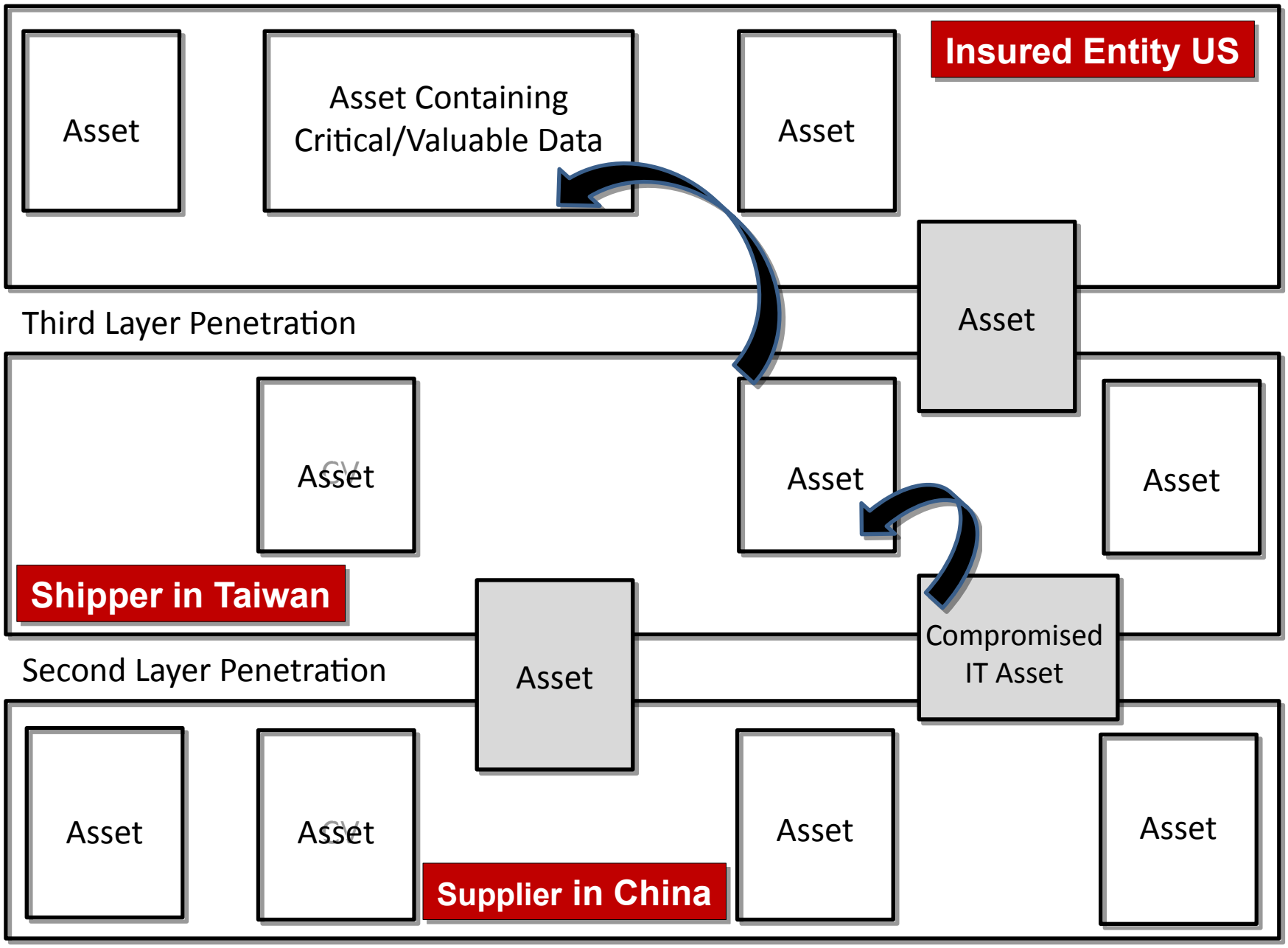
18 Processes x 18 Variables = 6,402,373,705,728,000 permutations

Which Provider?	API's? – Library V Proprietary	Data Centre Security?
Data Centre Location? – Regs/Latency	Type of Hypervisor?	Data Centre Power Supplier?
Contract Terms? – SLA	Application Run?	Data Centre Backup Provider?
Contract Terms? – Legal /Governing Law	OS Run?	Shared Hardware?
Cloud Topology?	Data Encrypted – Method/Provider?	Shared Software?
Data Routing by User?	Hardware Provider if Metal?	Hybrid Topology? – Pub/Priv

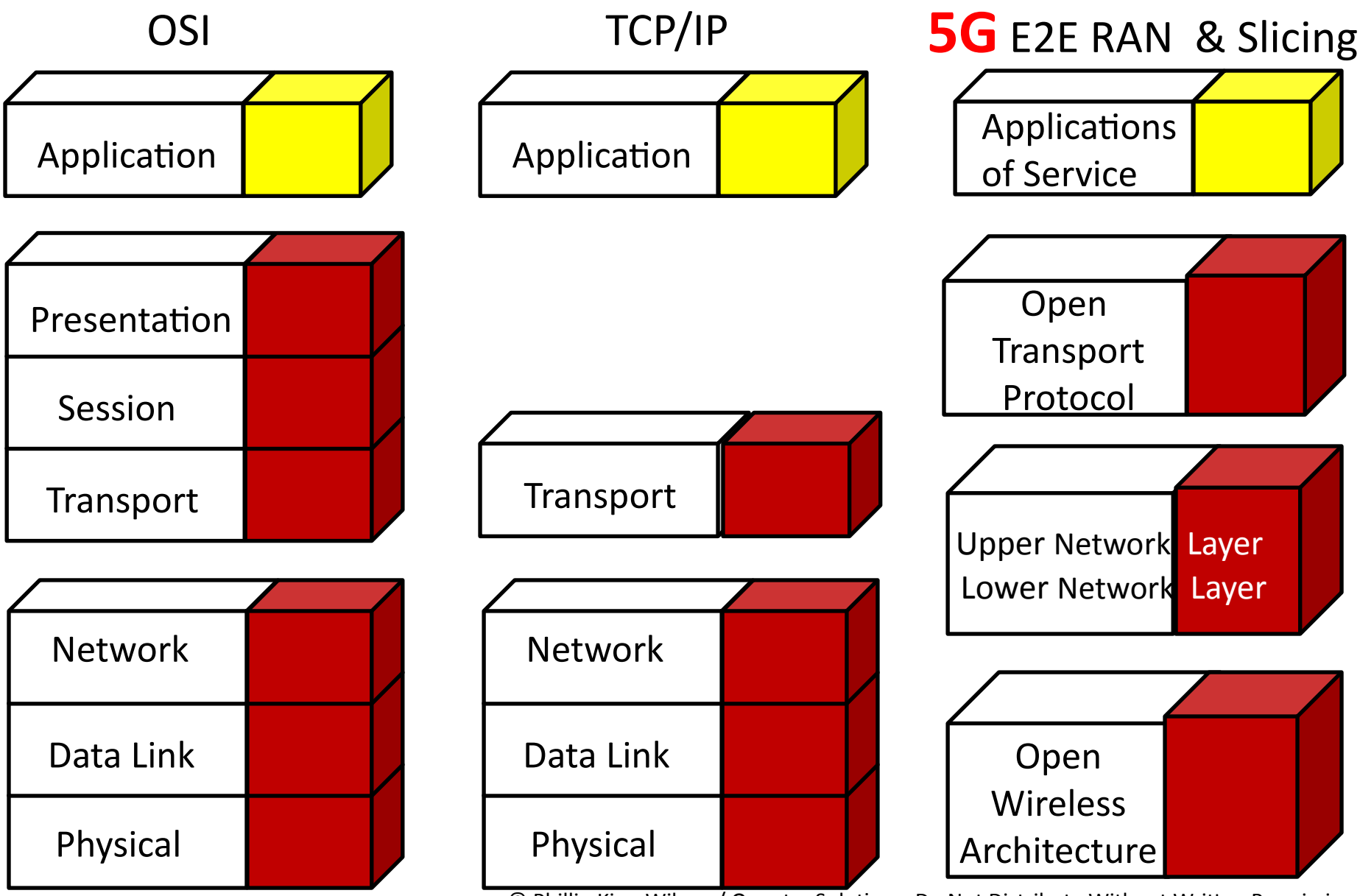
Cloud Data & Liability Issues



Operational Variables e.g. Supply Chain – Causality?



Transport Issues



Carriers: “No Threat Data”

First Known System Attack	First Known Network Penetration Attack	First Known Ransomware Attack
1963	1988	1989
PHREAKING	Automated Worm Attack	AIDS/PC Cyborg
WAR DIALING	MORRIS WORM	TROJAN
HARVARD TELEPHONE SYSTEM	4BSD/SUN 3	DOS
DEC PDP-1	Unix sendmail/finger rsh/rexec	Autoexec.bat
(monoculture targeting)	(monoculture targeting)	(monoculture targeting)

Carriers: “No Threat Data”

First Known Polymorphic Virus Attack

1990

Anti-Virus Avoidance Attack

1260

DOS

.Com Infector

(monoculture targeting)

First Mainstream Software Security Products

1999

Anti-Hacking

Microsoft

Windows 98

100’s Patched in Year 1 – multiple hacks

(monoculture targeting)

First Known High Profile Botnet Use

2000

Credit Card Number Theft

Spam Botnet Attack

ISP Bandwidth Use

Earthlink ISP

(single target)

Carriers: “No Threat Data”

First Known High Profile DNS Attack

2001

Domain Redirects

DNS Attack

DNS

Microsoft DNS

(monoculture targeting)

First Known Reference to Data Exfiltration

2002

IP Theft

EXFILTRATION

MS Office 2000

Office VB Scripts

(monoculture targeting)

First Known Programmable Logic Controller Attack

2005

IP Theft

STUXNET

SCADA/PLC

Zero Day Exploits/
Siemens Step7

(monoculture targeting)

Carriers: “No Threat Data”

First Known High Profile Social Engineering Attack

2013

Political/
Stock Market

Social Engineered
Twitter Access

Twitter

Associated Press
Password

(individual target)

First Known Crypto Currency Payments for Ransomware Attacks

2013

Fake News/
Stock Market

CryptoLocker

Windows OS

eMail Attachment

(monoculture targeting)

First Known Hijacked NSA Exploit Attack Use

2016

Financial Ransom

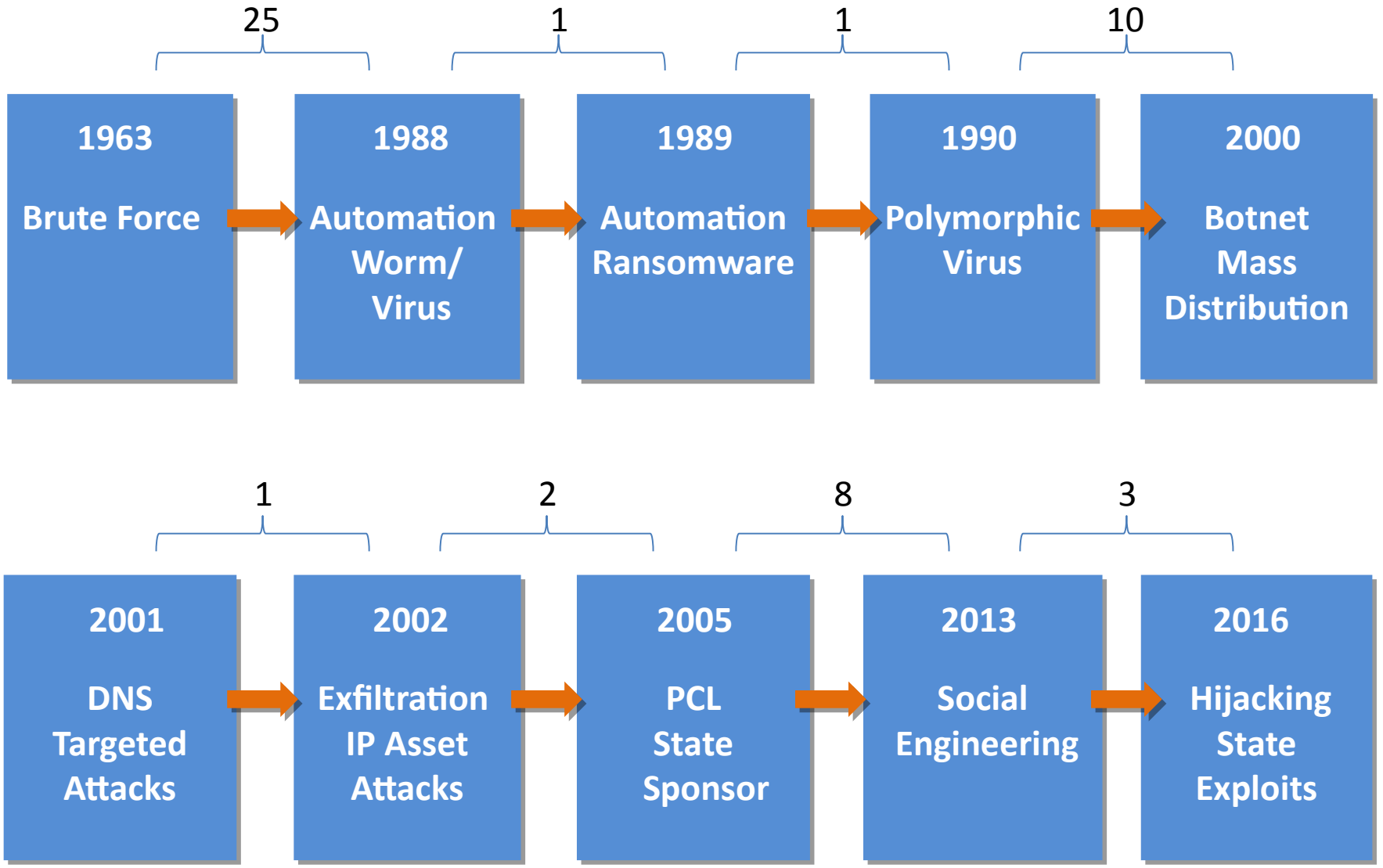
Wannacry/Petya

MS Windows

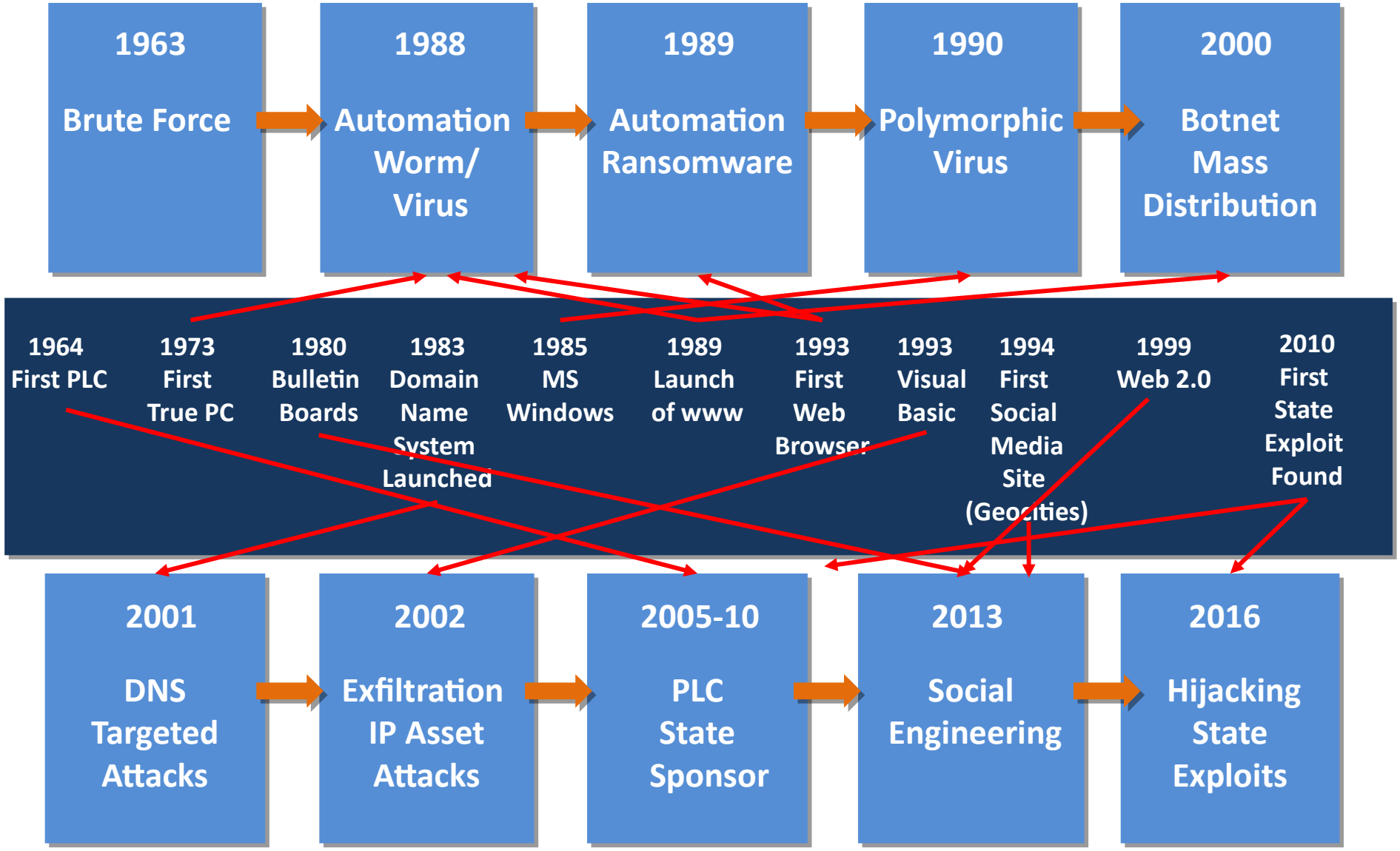
Master Boot Record

(single target)

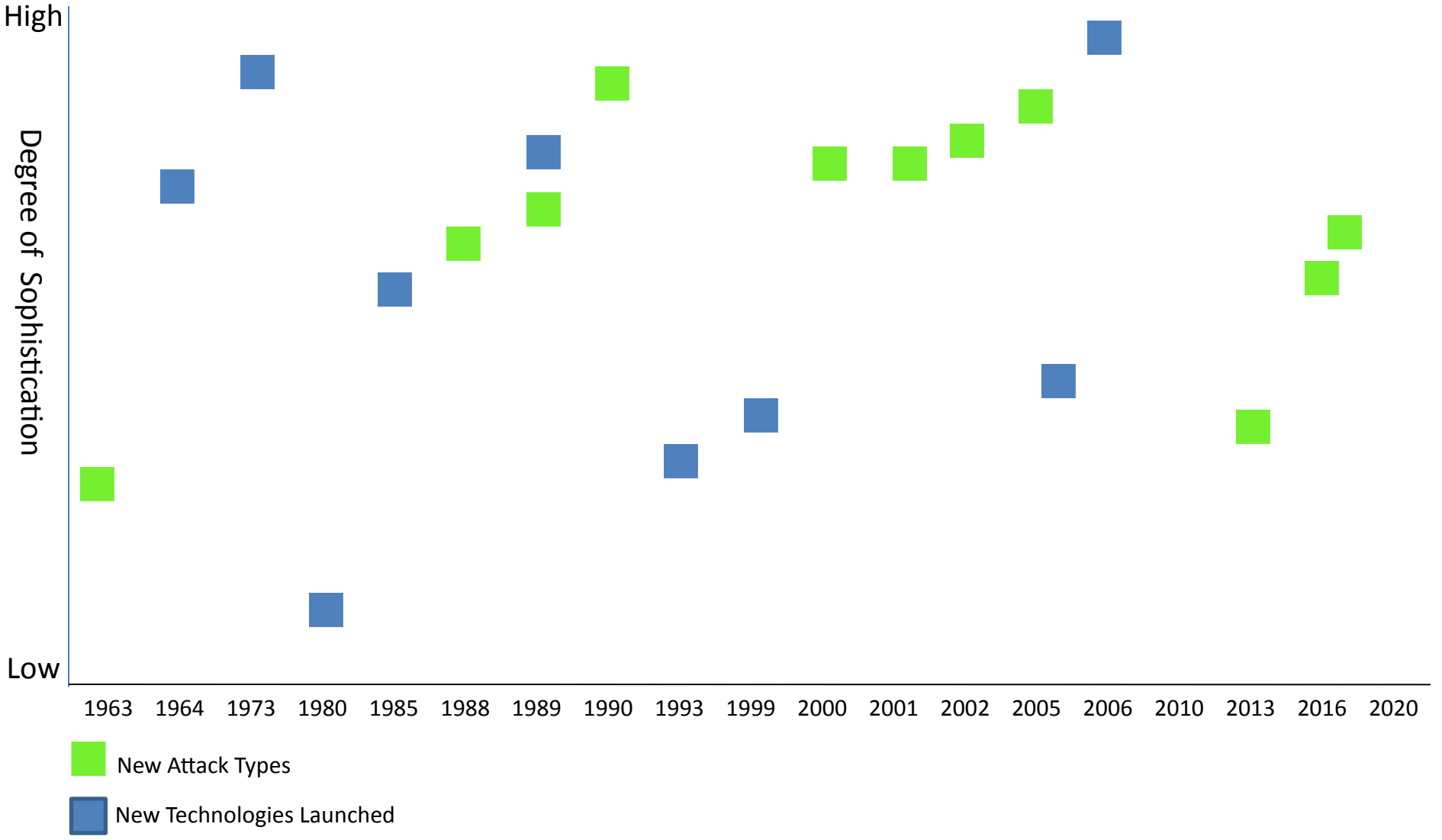
Threat Evolution Periods



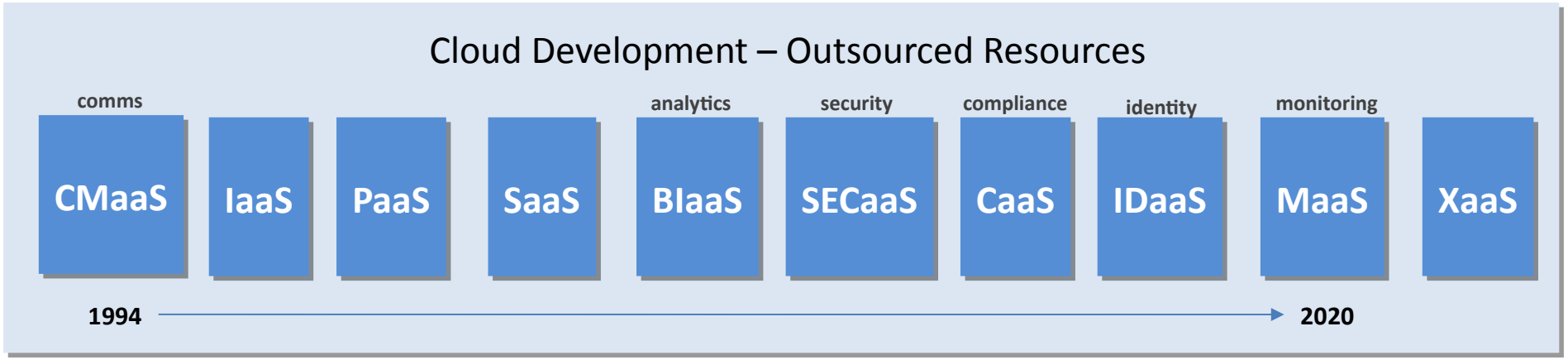
IT Versus Threat Evolution

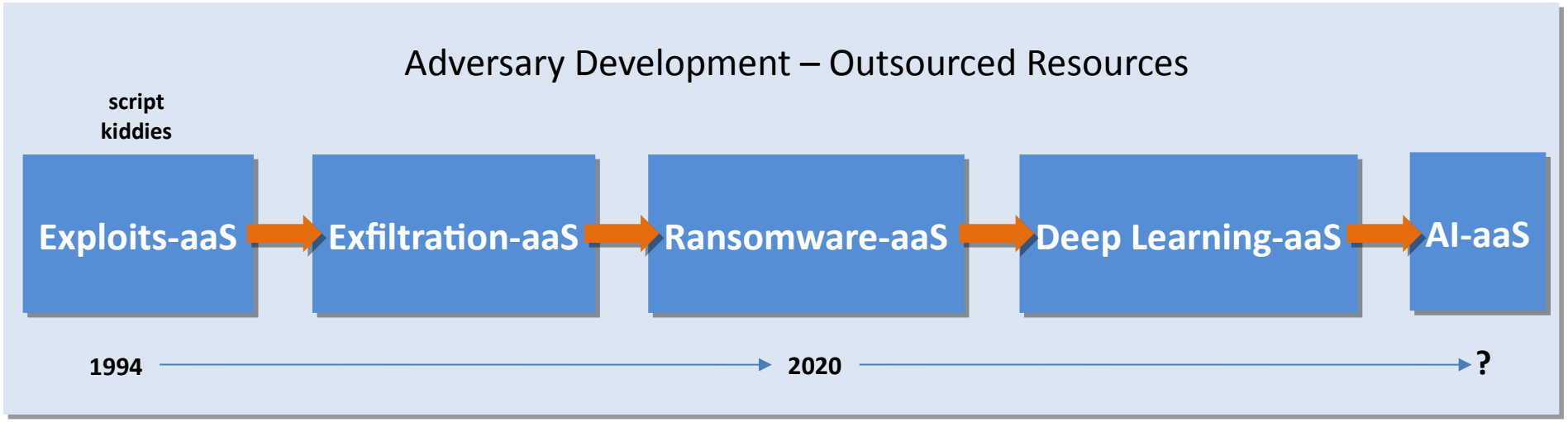


IT Versus Threat Pattern Y/N?



Cloud Versus Threat Evolution





M-L / D-L / AI

Characteristics	Attacker Impact	Defender Impact
Diverse Culture Targeting	+	+
Polymorphic Evolution	+	+
Genetic Mutation	+	-
Uncertain Impact	+	-
Uncertain Control	+	-
Uncertain Life	+	-
r/K selection theory growth rate	+	-
Data Theft	+	-
Data Destruction	+	-
Data Alteration	+	-
Vulnerable to Attack	?	?

Bottom-Up Valuation Methodology

RiskLens 2011

Cyber risk valuation for CISO's

PIVOTPOINT RISK ANALYTICS 2014

Cyber risk valuation

Bay Dynamics 2001 2014 (relaunched)

Behavioural analytics, valuation for security

Public Data Aggregation + Underwriting Platform

GUIDEWIRE CYENCE 2014

Cyber risk valuation for P&C non-cyber market; integrating into Guidewire

corax 2013

Data collection & analysis

CARPE DATA 2016

Data analytics: underwriting support

Security & Insurance Bundling

2017 Coalition

Cyber security & insurance bundling

PALADIN Cyber 2017

Cyber security & insurance bundling

at bay 2016

SME Cyber security & insurance bundling

Global Cyber Risk Valuation Companies : Patent Protected?

Company	Model	Patents	Filed
CyberCube	CAT risk Models	None	--
CARPE DATA	Predictive Scoring/Indices	None	--
RiskLens finjan	Factor Analysis	None	--
corax	Bayesian Belief Network	US10333963B2 US 102776207	2016
cyberpoint PIVOTPOINT	Bayesian Belief Network	US9537884	2016
Bay Dynamics	Behavioural Analytics Security	US 9390082 US9171055 US9330091 US9081830 US 9183269 US8965836	2011
GUIDEWIRE CYENCE	Data Listening/ Diversity Analysis	US9699209B2 US14585051 US10050989B2	2014

ITSEC Personnel Skills Gap

58% of CISOs - problem of not having expert cyber staff: Human security configuration key to cyber risk management

Missing Cyber Security Skilled Personnel

2013	1 Million
2018	3 Million
2021	3.5 Million

US	1 Million
Asia/Pacific	2 Million
EU	400 000

US States	
MA	9000
NY-NJ-CT	20 000
PHL	10 000
AZ	7000
SD	8450

Probable Outcome

Risk Carriers:

1	**Cyber: High Risk, Less Than 1% of P&C Revenues**	Drop Pure Cyber
2	**Legal:** Data protection laws; Cannot Insure Against Breaking Laws: US; UK; EU; India; China; Malaysia; Singapore + Future Expansion.	Policy Exclusions
3	**Coverage:** Risk of Forced Payout as Per Covid-19.	Policy Exclusions
4	**Silent Cyber:** Retro Risk Too High.	Drop Pure Cyber + Policy Exclusions
5	**ART/ILS:** Limited Risk Transfer Potential; Risk Too High; Limited Revenue Prospect Against Cost & Complexity.	Leave to Capital Markets to Develop at Present
6	**Captives & Sidecars:** Limited Capacity; Low Revenues; Needs Bottom Up Models for Capital Adequacy.	Develop/Test for Limited Exposures
7	**ILW:** Same Aggregation & Peering Issues As Others; Non-Quantifiable Portfolio Exposure.	Too High Risk to be Worthwhile
8	**Data:** Asymmetry Will Not be Overcome; Lack of Uberrimae fidei by Corporates; Disclosure Impact on Reputation & Share Value	Policy Exclusions & Warranty Terms

Litigation Model Offered by NPE

DEFENDANT OPTION 1: File an IPR (costs per patent assertion)

In-house legal review of patent assertions	$200 -250 000
IPR filing costs	$15 000
IPR legal costs	$300 – 600 000
Totals Minimum	$515 000
Number of patents 7	3,605,000.00

DEFENDANT OPTION 2: Wait and defend patent claim in court

Defending assertion	$1 – 4 000 000

DEFENDANT OPTION 3: Pay licensing fee

Licensing cost -all current & future patents	$200 000

Quantar Income 1st Tranche Infringers	
Corax + SSIC + Cyberpoint + Risklens + Cyence + Arx Nimbus + Evolver + Cybercube.....etc	20 X $200 000
Commission payment to legal entities	52%
Net Totals for 20 Licenses	$1,920,000

Release Software Free on Github to Kill Category Post Licence Payments

QUANTAR®
INSURANCE RISK ANALYTICS

END

Presented by : Dr. Phillip King-Wilson, Managing Director, Quantar Solutions Limited

May 2020