PTBA:
Risk Selection In Cyber Insurance

Dr Raveem Ismail

&

Ari Chatterjee, ACAS

Ari www.linkedin.com/in/ari-chatterjee-28518aa

STATISTICAL INDIAN INSTITUTE
भिन्नेष्वैक्यस्य दर्शनम्
UNITY IN DIVERSITY

GE Insurance Solutions

FLAGSTONE RE

hannover re®

Raveem www.linkedin.com/in/raveem

UNIVERSITY OF OXFORD

EA

AON BENFIELD

VALIDUS

Ariel Re

FRACTAL INDUSTRIES

Why Cyber Insurance, Why Now?

An **emerging risk**, with **evolving products**,
and still developing **cyber insurance risk transfer chain**

Polarising

Dearth of technical research relevant to cyber insurance

Mountains of data, often freely available

What Is PTBA?

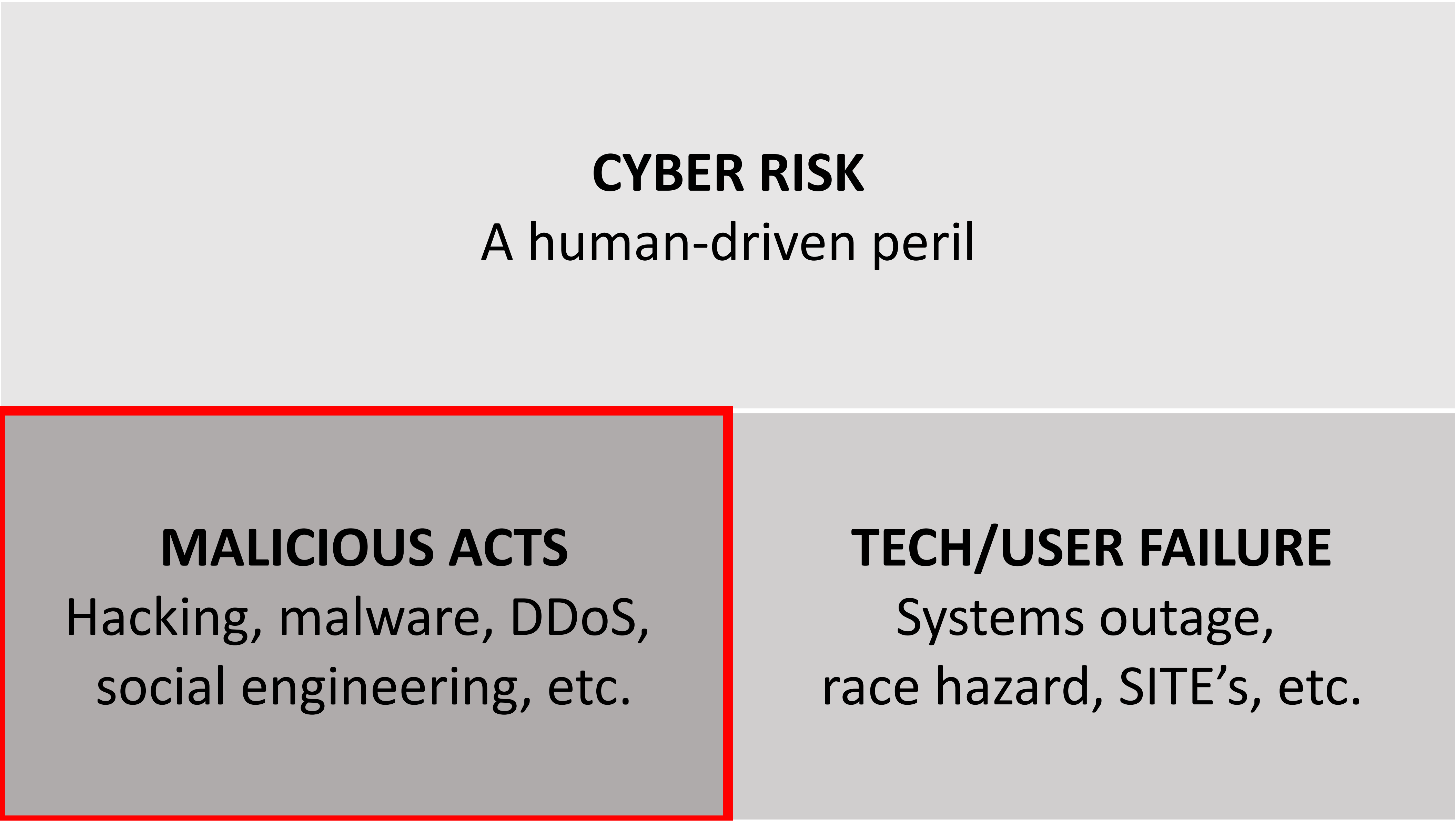
Propensity **T**o **B**e **A**ttacked

Why Is It Needed?

Underwriting requires pre-bind analytics.

Measures for risk selection need to be transparent.

A single risk score, if it encapsulates the right ingredients, is a very useful measure.



CYBER RISK

A human-driven peril

MALICIOUS ACTS

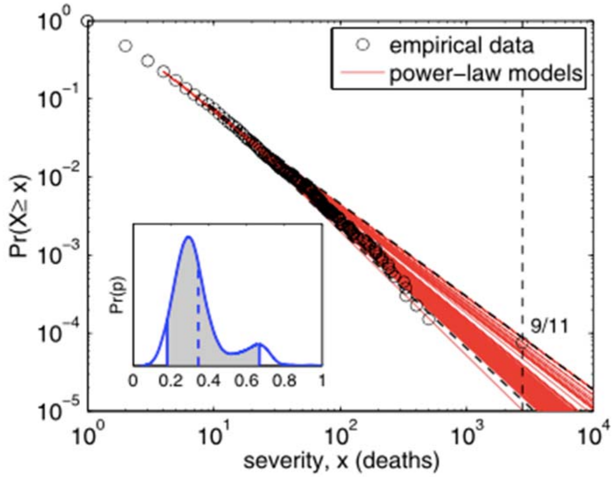
Hacking, malware, DDoS,
social engineering, etc.

TECH/USER FAILURE

Systems outage,
race hazard, SITE’s, etc.

Cyber – An Anthropogenic Peril

A function of attacker and defender interplay, i.e., adversarial, with adaptive threat landscape.



Unlike Nat Cat, man-made peril properties are

emergent observations from **complex adaptive systems**,

not derived from **underlying physical principles**.

Examples: cyber, and especially violence (crime, political violence, war, terrorism). Limited research in this area.

P(Deaths) = Deaths$^{-\alpha}$

"Fat Tails"

Cyber: A Rapidly Adapting Landscape

Risk = Threat + Defence

Change occurs when the following happens:

- Adaptation by perpetrators and/or victims.
- Criminal proceedings.
- Target substitution.

All these are cost-benefit changes.

For cyber, the "macro-level" risk landscape experiences change on the scale of circa 2 years.

DEFINING PTBA: **ATTACKER PROFIT FUNCTION**

Expected income for attacker, from cyber-attack, is value of records hacked, plus any other value from target:

I = NC + O

Attackers have costs, so “profits” are difference between (daily) costs and potential income:

P = I – Kt

Therefore, we define the attacker profit function:

P = NC + O - Kt

PROFIT FUNCTION BEHAVIOUR BY ATTACKER

Attacker	Profit function (P = NC + O – Kt)	**Motivation/Sophistication/Funding**
Nation State	P = O – Kt	Disruption, espionage, highly sophisticated and well-funded
Criminal	P = NC + O - Kt	Financial gain, O is mostly ransom, wide spectrum of sophistication/funding
Hacktivist	P = O – Kt	Disruption, curates victims that give maximum publicity, less sophisticated/funded
Insider	P = NC + O - Kt	Financial gain, disruption, retaliation, sophistication/funding is less meaningful

Defining PTBA: **Profit Maximisation & Target Ranking**

For each attacker, aim is to maximise profit function across all targets:

$$\mathbf{Max(P) = Max(NC + O - Kt)}$$

Given this, attackers can sort potential targets, allowing ascertainment of target desirability.

From the target's perspective, they appear at a percentile rank **R**, in each attacker's list.

For a target, summing R, across attackers n, is a measure of the susceptibility of the target.

We thus define the *Propensity To Be Attacked*:

$$\mathbf{PTBA = (\Sigma_n R) / n}$$

PTBA Behaviour

$$\mathbf{PTBA = (\Sigma_n R) / n}$$

$0 < \text{PTBA} < 1$

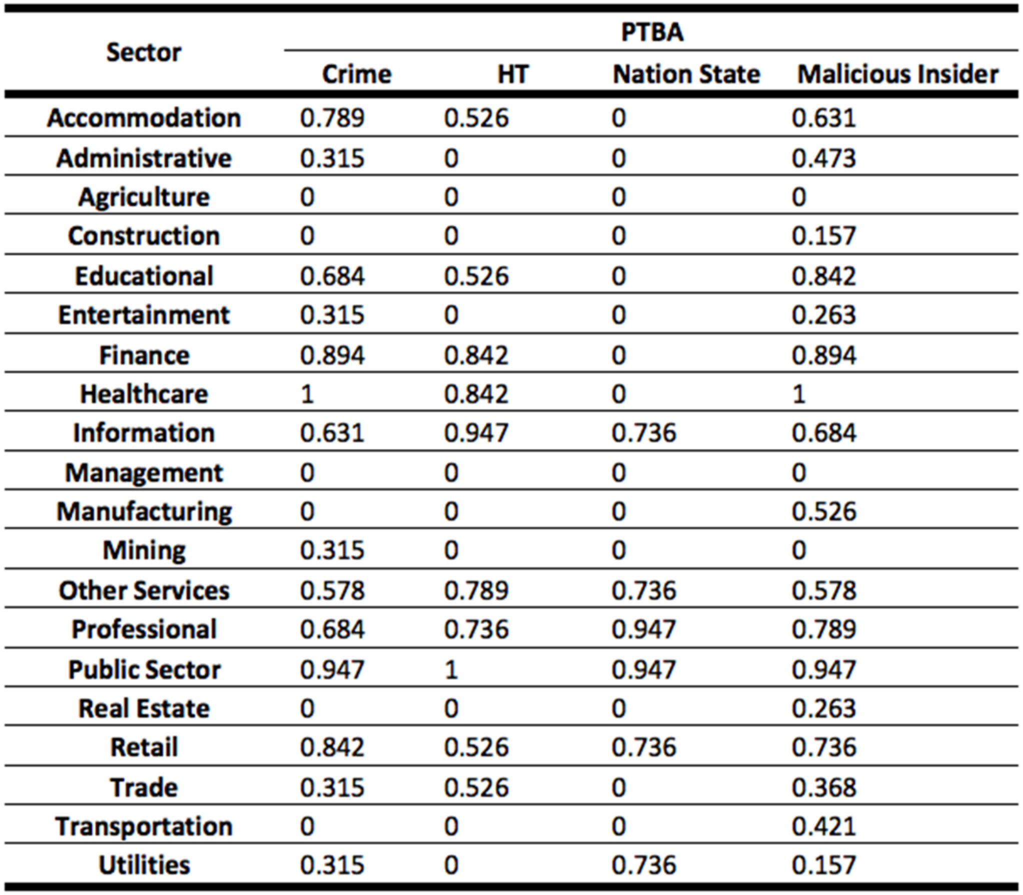
PTBA varies by industry, some industries are targets for more attackers due to the value of their assets compared to others (e.g., healthcare)

Better protected firm may have higher K and t – reduces PTBA

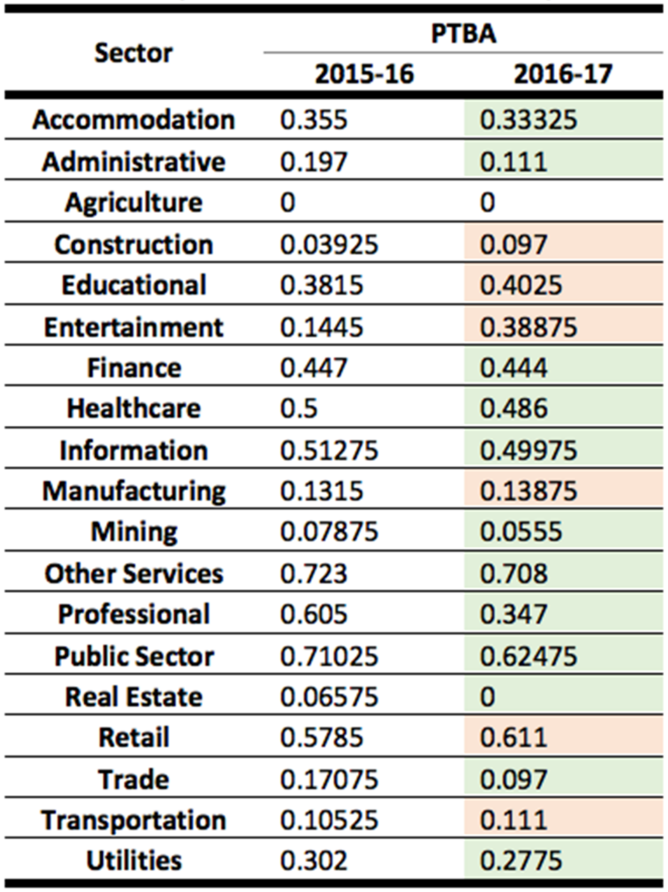
Annual revenue does not always correlate to higher PTBA

Actual Example Of PTBA Calculation

For transparency we have used VCDB database to calculate PTBA



Sector	PTBA			
	Crime	HT	Nation State	Malicious Insider
Accommodation	0.789	0.526	0	0.631
Administrative	0.315	0	0	0.473
Agriculture	0	0	0	0
Construction	0	0	0	0.157
Educational	0.684	0.526	0	0.842
Entertainment	0.315	0	0	0.263
Finance	0.894	0.842	0	0.894
Healthcare	1	0.842	0	1
Information	0.631	0.947	0.736	0.684
Management	0	0	0	0
Manufacturing	0	0	0	0.526
Mining	0.315	0	0	0
Other Services	0.578	0.789	0.736	0.578
Professional	0.684	0.736	0.947	0.789
Public Sector	0.947	1	0.947	0.947
Real Estate	0	0	0	0.263
Retail	0.842	0.526	0.736	0.736
Trade	0.315	0.526	0	0.368
Transportation	0	0	0	0.421
Utilities	0.315	0	0.736	0.157



Sector	PTBA	
	2015-16	2016-17
Accommodation	0.355	0.33325
Administrative	0.197	0.111
Agriculture	0	0
Construction	0.03925	0.097
Educational	0.3815	0.4025
Entertainment	0.1445	0.38875
Finance	0.447	0.444
Healthcare	0.5	0.486
Information	0.51275	0.49975
Manufacturing	0.1315	0.13875
Mining	0.07875	0.0555
Other Services	0.723	0.708
Professional	0.605	0.347
Public Sector	0.71025	0.62475
Real Estate	0.06575	0
Retail	0.5785	0.611
Trade	0.17075	0.097
Transportation	0.10525	0.111
Utilities	0.302	0.2775

Real World Uses For PTBA

Threat Landscape: Overview of threats and emerging trends, set of PTBA approximates Threat Landscape

Cyber security: a quantifiable way to measure threat landscape

To predict and measure changes in threat landscape (see next slide)

Cyber insurance: underwrite based on changes in threat landscape

Build models (especially frequency) based on PTBA

Goes beyond Cyber, extends to other attacker driven perils

Risk Selection & Pricing

Avoid high risk industries,

Refine pricing metric to reflect PTBA

Rebalance your portfolio based on PTBA

CHANGE IN CYBER LANDSCAPE

Changes in threat landscape explainable using trends in profit function

$P = I - Kt$

When I changes, e.g. decrease in asset value and the profit margins are down for the attacker, a new attack vector emerges that makes more income

When K changes, e.g. cyber security patches the gaps, firms become more aware of the threats, it becomes cheaper to attack due to new exploit, etc.

When t changes, e.g. firms tighten their security, new attack vector makes it easier and cheaper to attack, etc.