

SAS ERM - ESSEC CREAR Conference 2018

· July 27, 2018

Cyber Insurance *Market & Demand Dynamics*

Ram Garg CFA, MBA

General Manager

J B Boda & Co (Singapore) Pte Ltd



SINGAPORE
ACTUARIAL
SOCIETY



Disclaimer:

The views, information and content expressed here in are those of the author and do not represent the views of any of J B Boda Group Companies. The information provided should not be provided as legal advice or a definitive statement of law in any jurisdiction. For such advice, an applicant, insured or reader should consult their own legal counsel.

Agenda



- Market Dynamics
- Cyber Coverage
- Underwriting & Claims



Cyber Insurance Outlook – Global



“Cyber threats have become the risks of the century and if cyber security is one step behind new cyber threats, cyber insurance is two steps behind.”

Global Cyber insurance market is rapidly growing and expected to cross U\$7-8 billion by 2020.

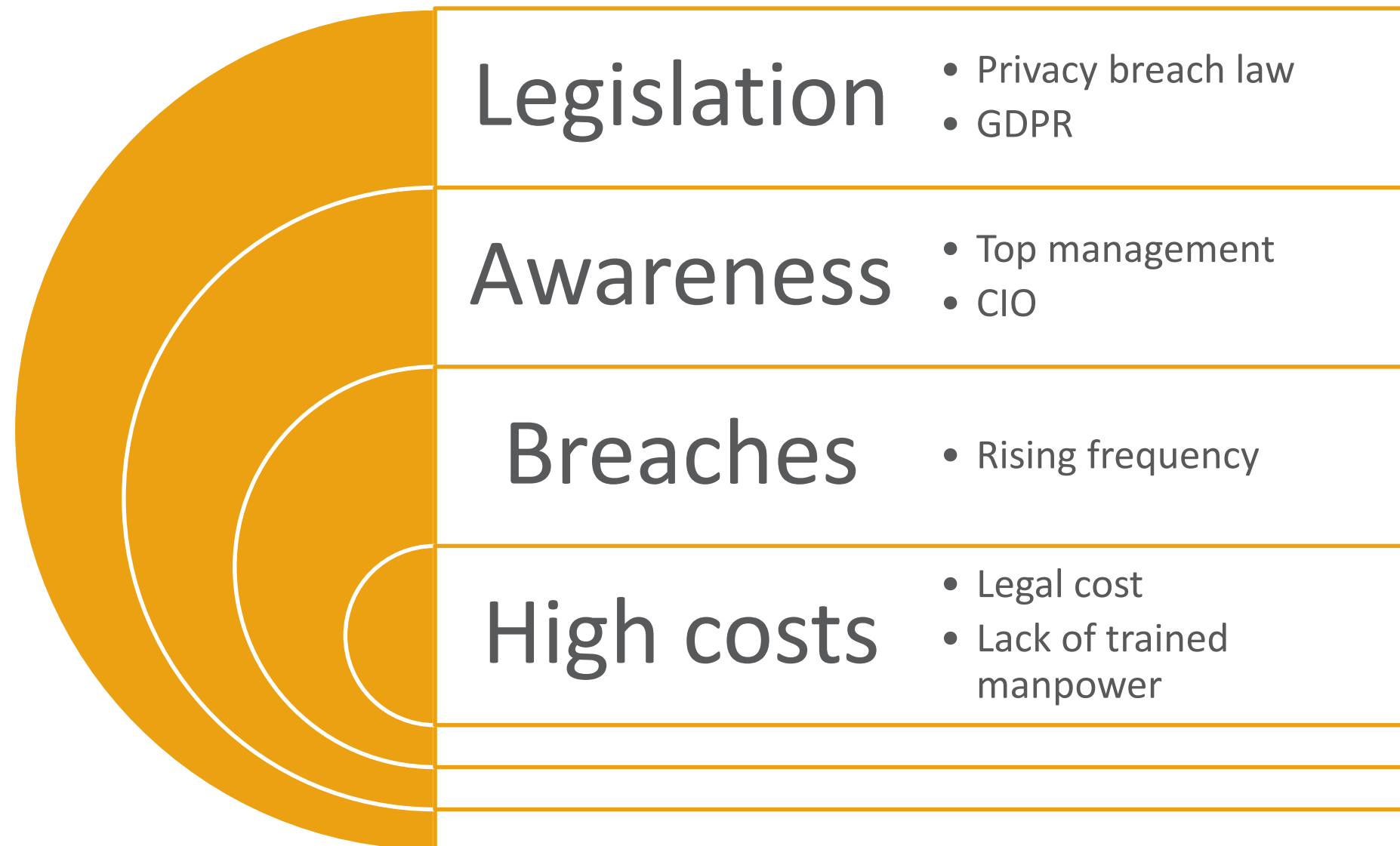
Cyber Insurance Market in Singapore

In its infancy

- 10+ insurers offer cover
- Singapore premium – USD 15 mln to 25 mln
- 2-3 Reinsurance capacity providers
- No standard policy wordings
- 15-50 underwriting questions
- High variation in premium rates
- Uncertainty of coverage
- Limited response service providers



Key demand drivers



Marketplace: Wide differences

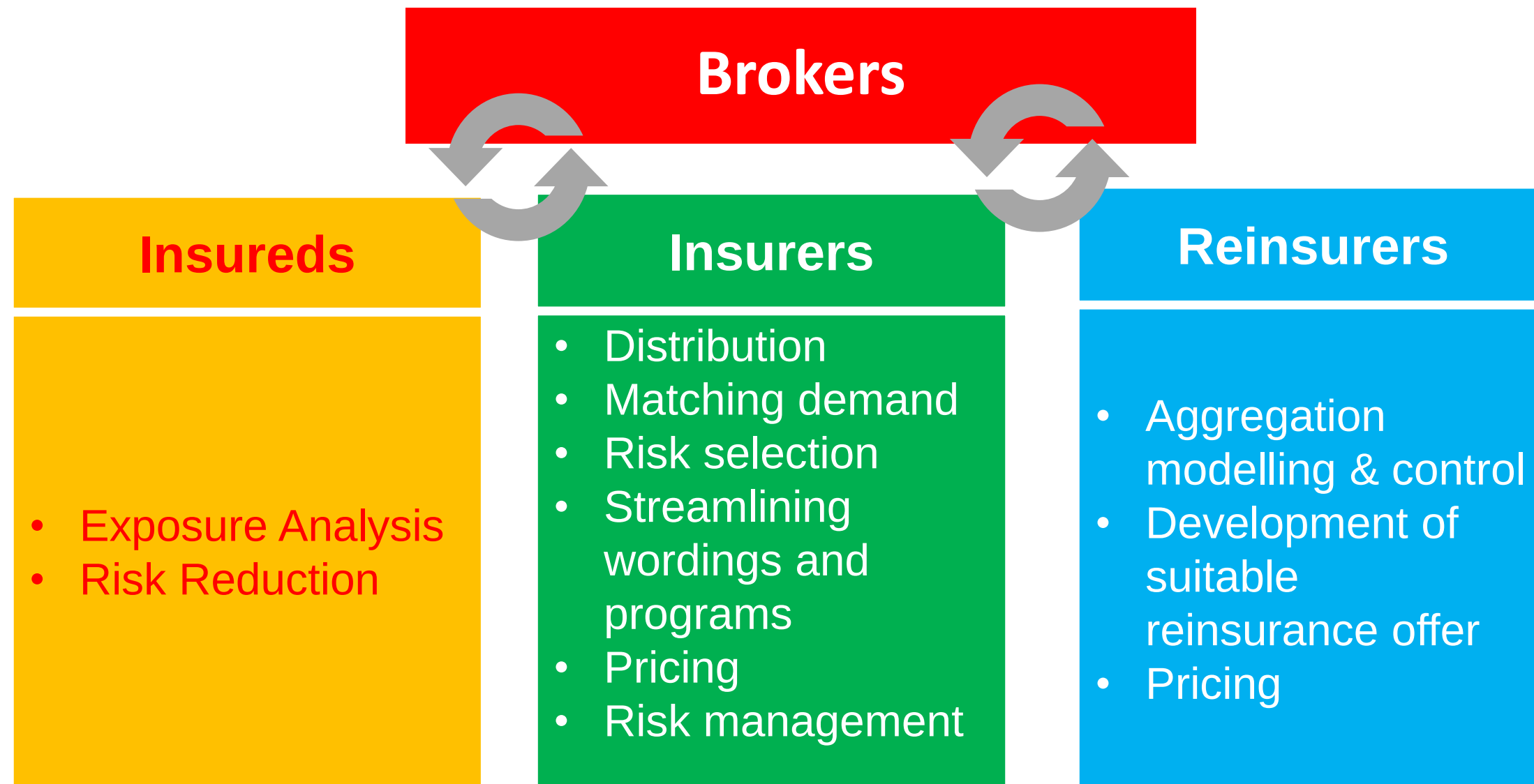
Demand Side

- Poor awareness of the risk
- Inconsistent policy wordings
- Limited coverage
- Legal landscape remains in flux

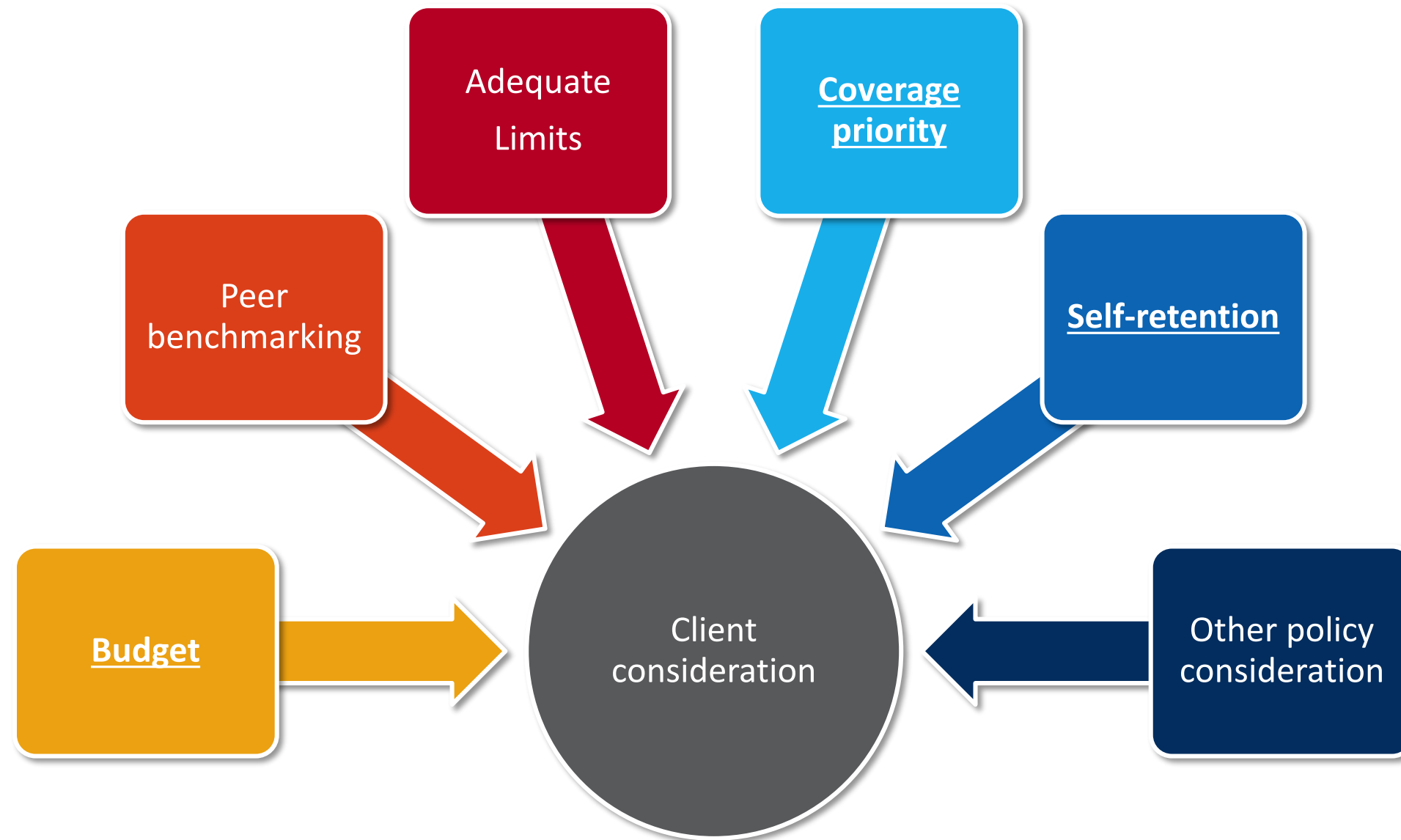
Supply Side

- Rapidly evolving risk landscape
- Lack of understanding of exposures
- Accumulation risk uncertainty

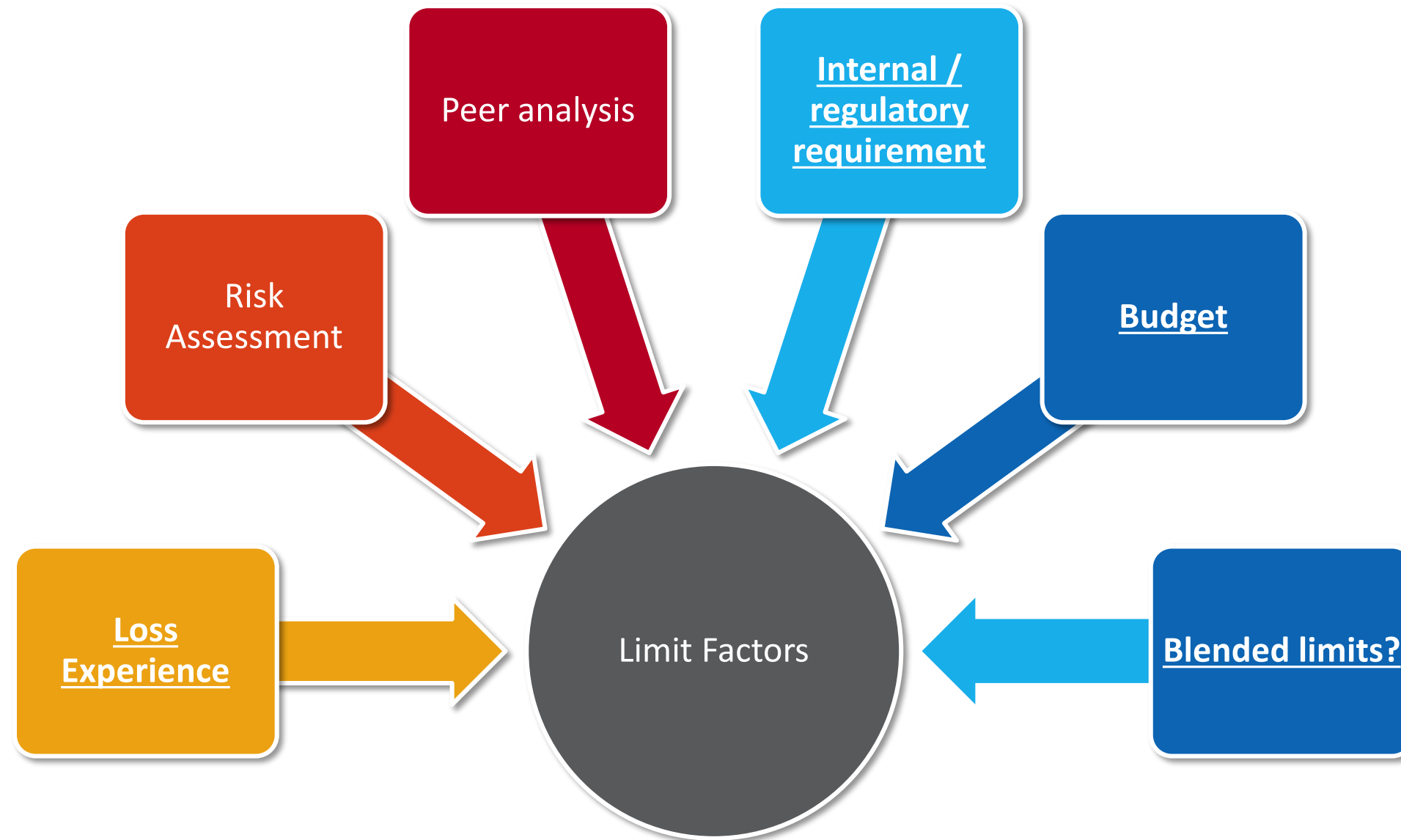
Addressing Challenges in Risk Transfer



Policy Considerations



Policy Limit Considerations



Cyber Incidents and Policy limit

- **SingHealth** cyberattack likely to be state-sponsored; Medical data a goldmine for hackers – *Forensic investigation cost will be significant higher in such cases.*
- **Equifax** only had \$75M in cybersecurity insurance but expect claims of at least \$275M!

Agenda

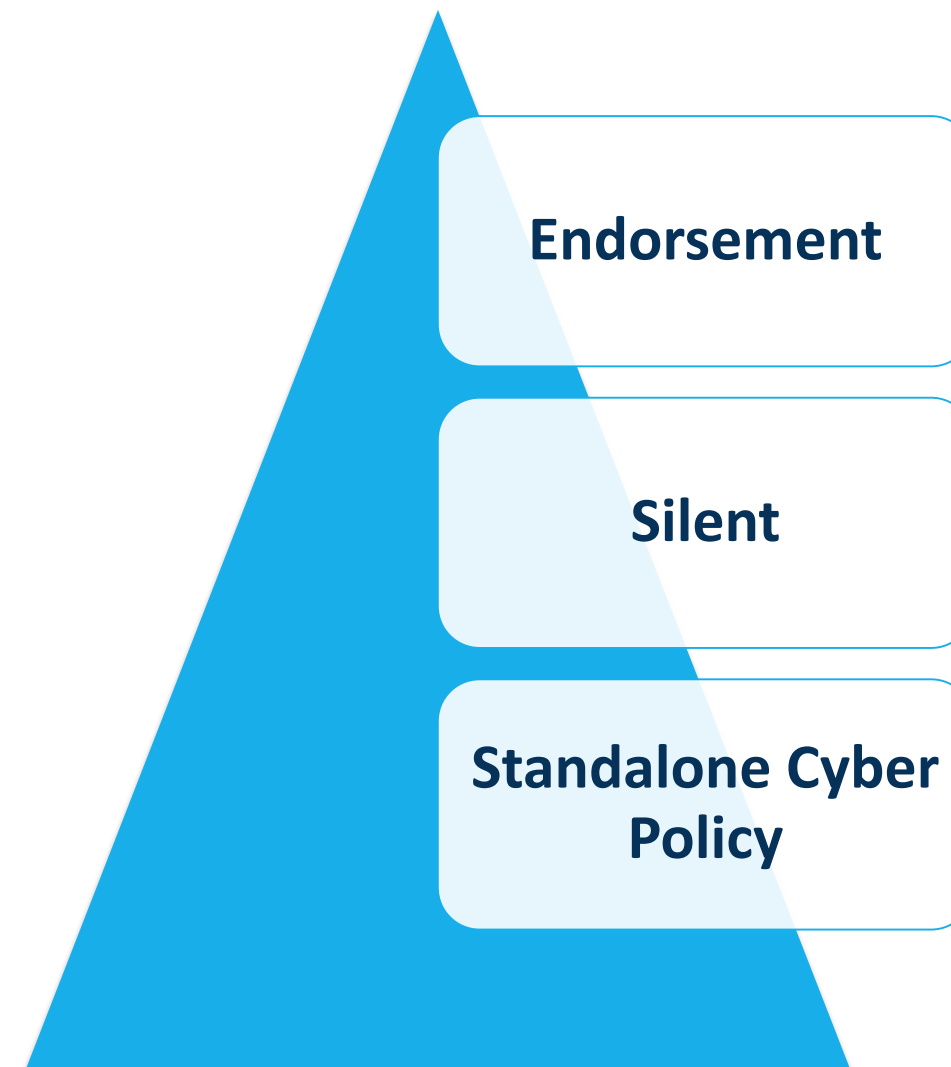


- Market Dynamics
- **Cyber Coverage**
- Underwriting & Claims



Existing and future insurance products

- **Standalone:** Industry specific coverage
- **Imbedded into a P&C product:**
Attach Cyber endorsement into policies such as Property BI, PI, BBB, Crime etc
- **Silent Cyber**



Stand Alone Cyber Insurance – First Party Loss

First Party	Network business interruption	Loss of income and extra expense resulting from a total or partial failure of by DOS, malicious code, unauthorized access/use to computer system
	Intangible property	Costs to restore or recreate data or software resulting from network security failure
	Loss of Digital Assets	Expenses & costs incurred resulting from damage, alteration, theft, digital assets caused by DOS, malicious code, unauthorized access/use to
	Crisis Management costs	Legal costs to comply with privacy regulations, credit monitoring, PR, costs, resulting from a security data breach, privacy breach or breach of
	Cyber Extortion	Extortion expenses and monies paid resulting from a threat to destroy or assets which are acquired by unauthorized access

Stand Alone Cyber Insurance – 3rd Party Loss

Third Party	Litigation and regulatory	Covers the costs associated with civil lawsuits, judgments, settlements or penalties resulting from a cyber event.
	Regulatory response	Covers the legal, technical or forensic services necessary to assist the policyholder in responding to governmental inquiries relating to a cyber attack, and provides coverage for fines, penalties, investigations or other regulatory actions
	Notification costs	Covers the costs to notify customers, employees or other victims affected by a cyber event, including notice required by law
	Crisis management	Covers crisis management and public relations expenses incurred to educate customers concerning a cyber event and the policyholder's response, including the cost of advertising for this purpose.

Continue..

Stand Alone Cyber Insurance – 3rd Party Loss

..Continue

Third Party	Credit monitoring	Covers the costs of credit monitoring, fraud monitoring or other related services to customers or employees affected by a cyber event.
	Media liability	Provides coverage for media liability, including coverage for copyright, trademark or service mark infringement resulting from online publication by the insured.
	Privacy liability	Provides coverage for liability to employees or customers for a breach of privacy

Silent Cyber and Untested Policy Wording



PRA SS4/17

Agenda



- Market Dynamics
- Cyber Coverage
- **Underwriting & Claims**



Underwriting & Claims

“Pre-bid” Underwriting

- Questionnaire / Proposal Form/ Interviews
- Online assessment
- External penetration assessment
- Full review
- Cost is key consideration

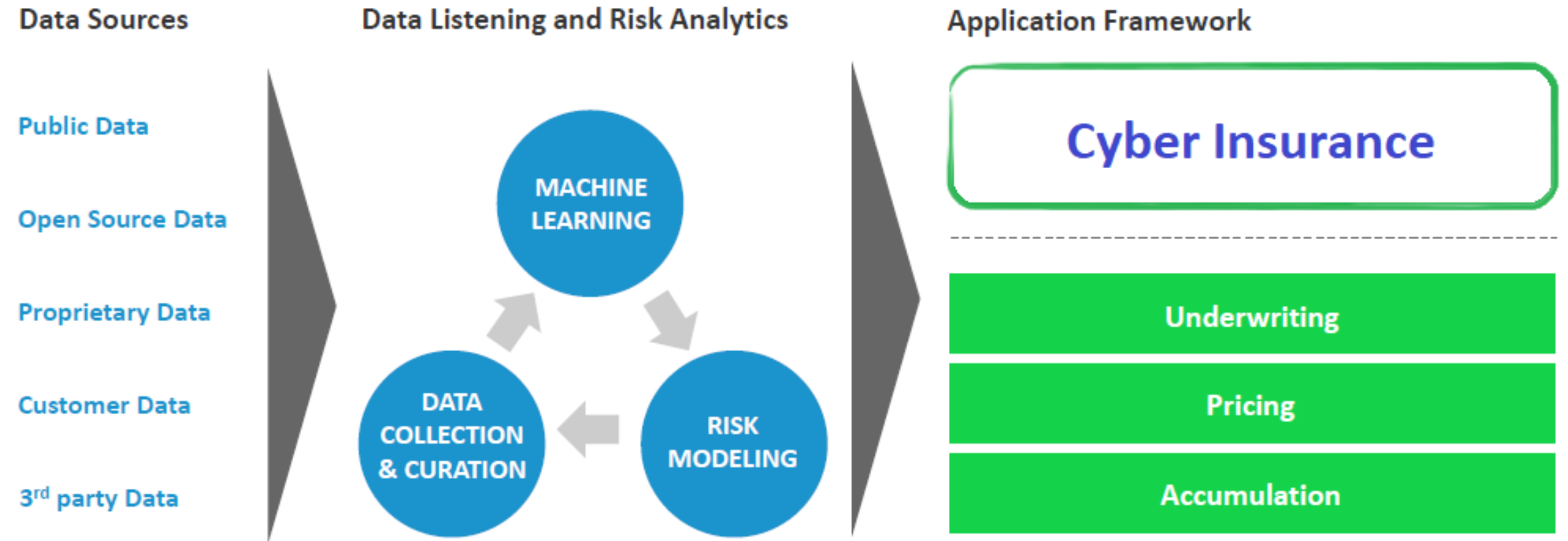
Post “Bid” value added service

- Pen testing
- Documentation and process review
- Training
- Incident response procedure

Claims front, different models may be adopted

- Dedicated hotline
- Panel
- Hybrid

Future of Underwriting



UW Information: Current method

Industry	Recovery Plan	Demography	Revenue	Security
				

UW Information: *The insured's industry*

Some industries have more significant exposure to PHI or PII. For example, companies in the healthcare industry are likely to have PHI. In the retail industry, companies might be further subcategorized based on characteristics such as the number of credit card transactions processed yearly.

Industry



UW Information: *Geographic spread of operations*

Companies with a global footprint face different risks in different jurisdictions. The US is a fairly litigious environment with significant privacy laws and regulations, creating significant exposure. Other jurisdictions may not have robust regulation or enforcement, reducing the risk of exposure from a breach.



UW Information: *Security and privacy controls*

- Companies that can demonstrate high quality controls will generally see lower premiums.
- Notably, quality is not based solely on the technology a company uses to protect data. Rather, quality is the combination of people, processes and technology that a company uses to safeguard PHI and PII.
- While some insurers continue to inflict lengthy applications on applicants, much more commonly carriers ask the company to participate in a briefing at which individuals with responsibility for management and security of PHI and/or PII provide information and respond to questions.



UW Information: *Data breach team choice*

- If the insured wants to utilize its own data breach team rather than using the carrier's team, the premium will likely increase.
- Policies requiring the insured to use the carrier's data breach team reflect the savings a carrier is able to realize as a result of providing high volume business to chosen experts.
- Some carriers will not write a policy that permits the insured to choose its own data breach team.



Accumulation of risks

- The accumulation potential of cyber risks is not fully understood.
- Firstly, a single cyber event can trigger a multitude of stand-alone cyber policies, due to the fact that contingent business interruption is a common feature of cyber policies, but also because everything is interconnected.
- The rise of the IoT will increase connectivity and so trigger even more potential losses.
- Main exposures for accumulation scenarios could be:
 - The clash among different lines of business
 - The coverage of contingent business interruption
 - The outage of external networks such as the internet, telecommunication networks or utility providers
 - Other service providers with a high client concentration, such as cloud providers or DNS servers
 - Security gaps in widely used standard software products

Cyber Pricing Techniques

It is a Different Ballgame

- Data issue
- No Geographical Limitation
- Network Risk
- Significance of the Human Element
- Correlation of Attacks
- Definition of a Cyber Cat
- Technology Evolution
- Silent Coverage





thank
you

Ram Garg
DID: +65-6309 1158
Mobile: +65-8322 9962
E-mail: ram@jbboda.com.sg