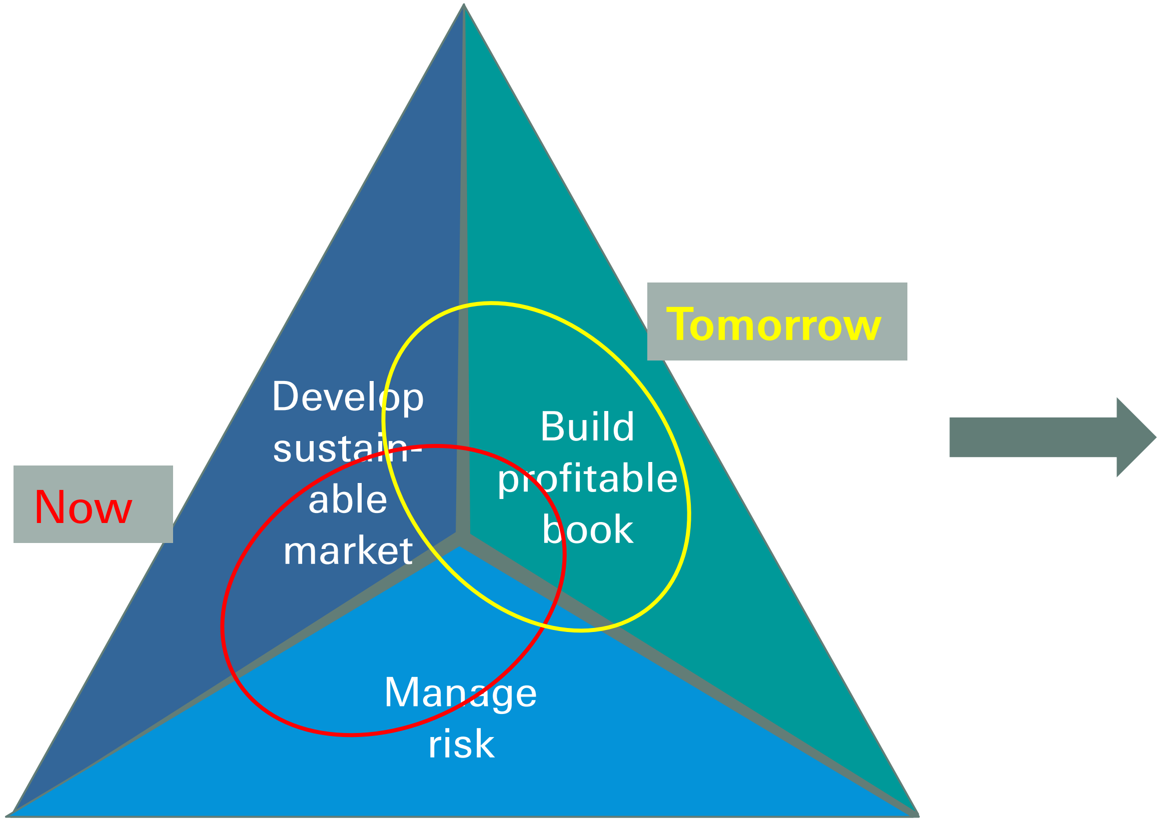
Cyber market´s present and future challenges

The reinsurer´s view and expectations

Dr. Eric Durand, Swiss Re

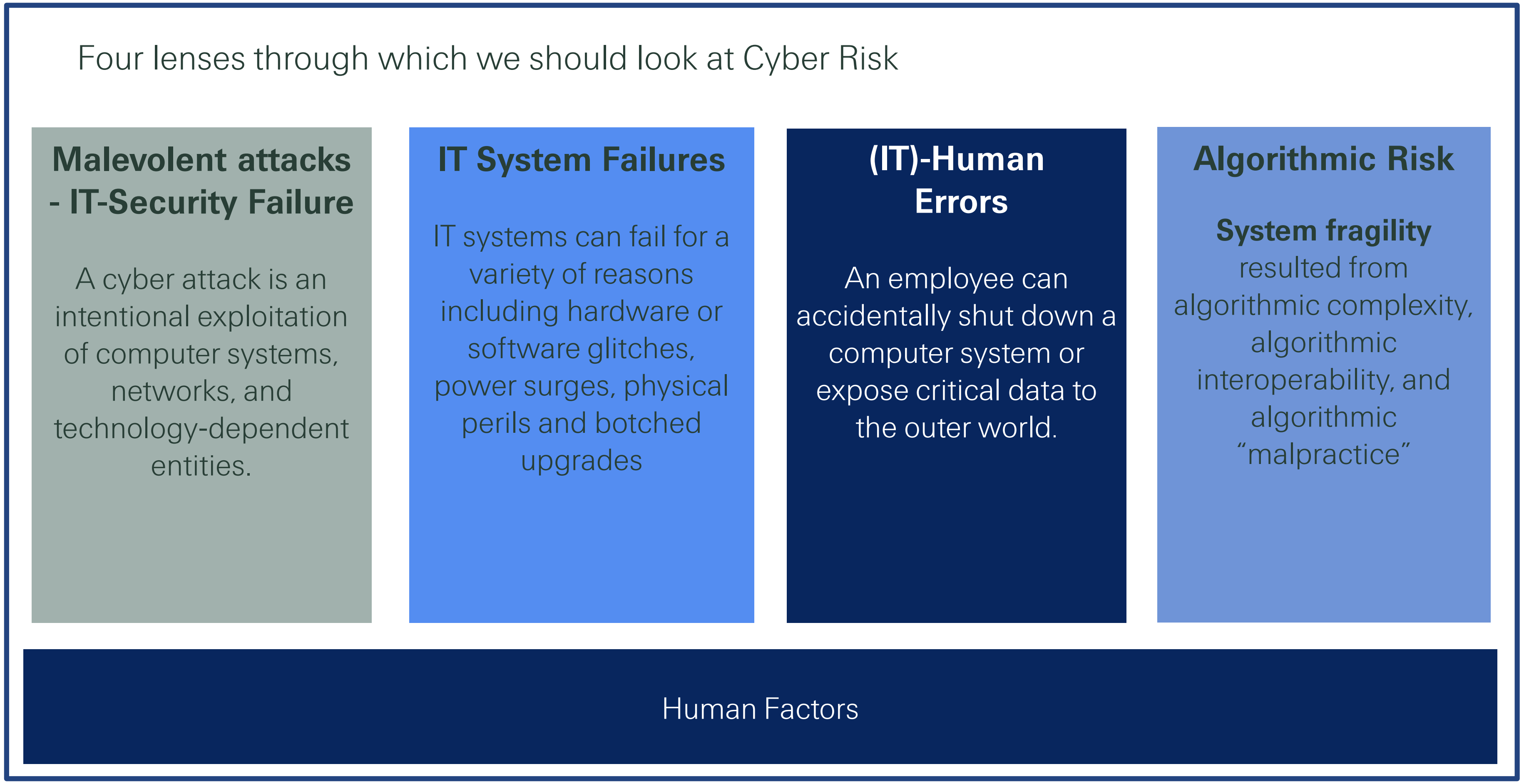
Introduction: The tasks at hand



"Develop sustainable market" is specific to a new LoB (Line of Business) such as Cyber

“4+1” pillar framework to address the cyber insurability problem

How to “understand” Cyber



Four lenses through which we should look at Cyber Risk

Malevolent attacks - IT-Security Failure

A cyber attack is an intentional exploitation of computer systems, networks, and technology-dependent entities.

IT System Failures

IT systems can fail for a variety of reasons including hardware or software glitches, power surges, physical perils and botched upgrades

(IT)-Human Errors

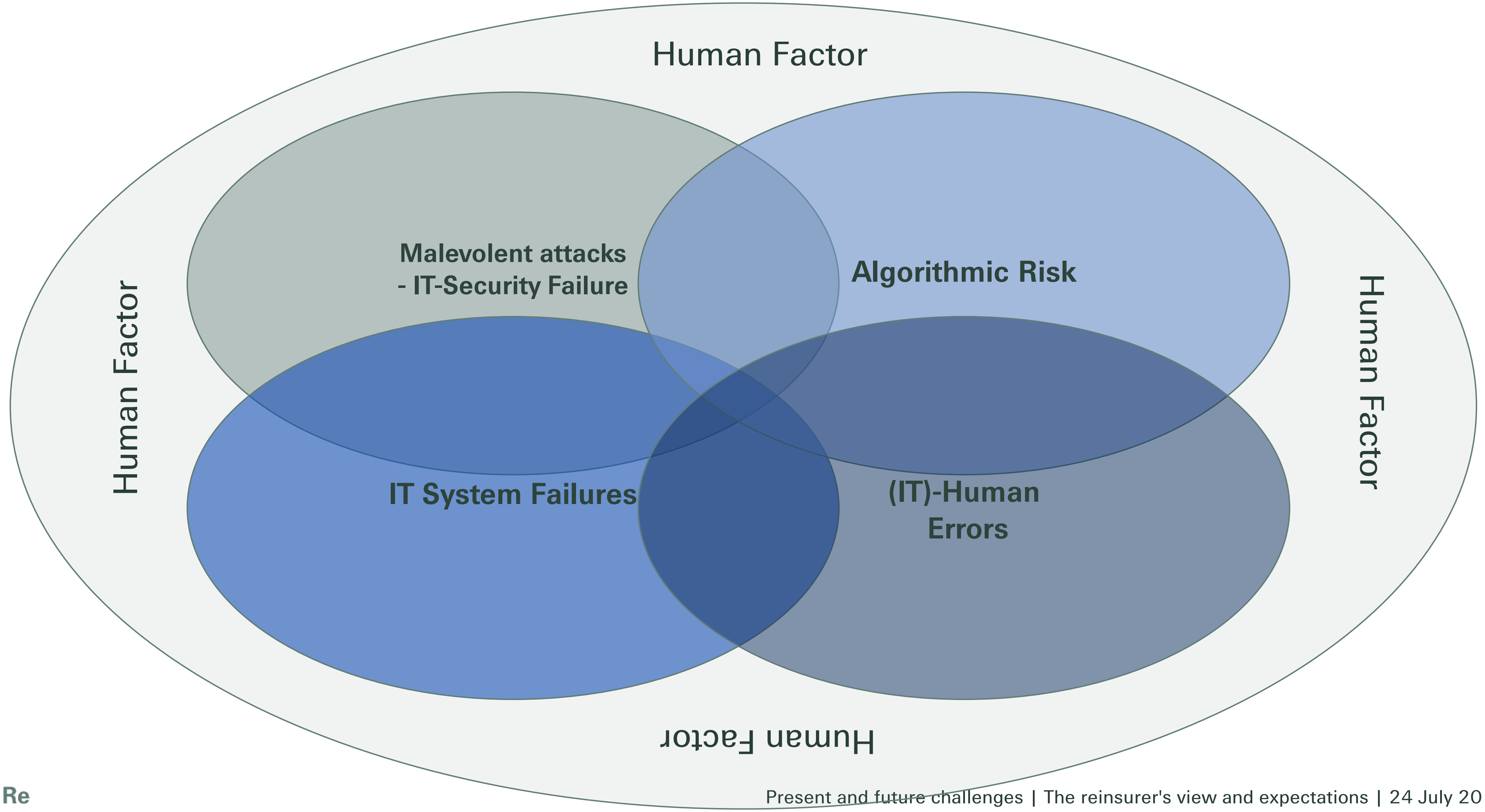
An employee can accidentally shut down a computer system or expose critical data to the outer world.

Algorithmic Risk

System fragility resulted from algorithmic complexity, algorithmic interoperability, and algorithmic “malpractice”

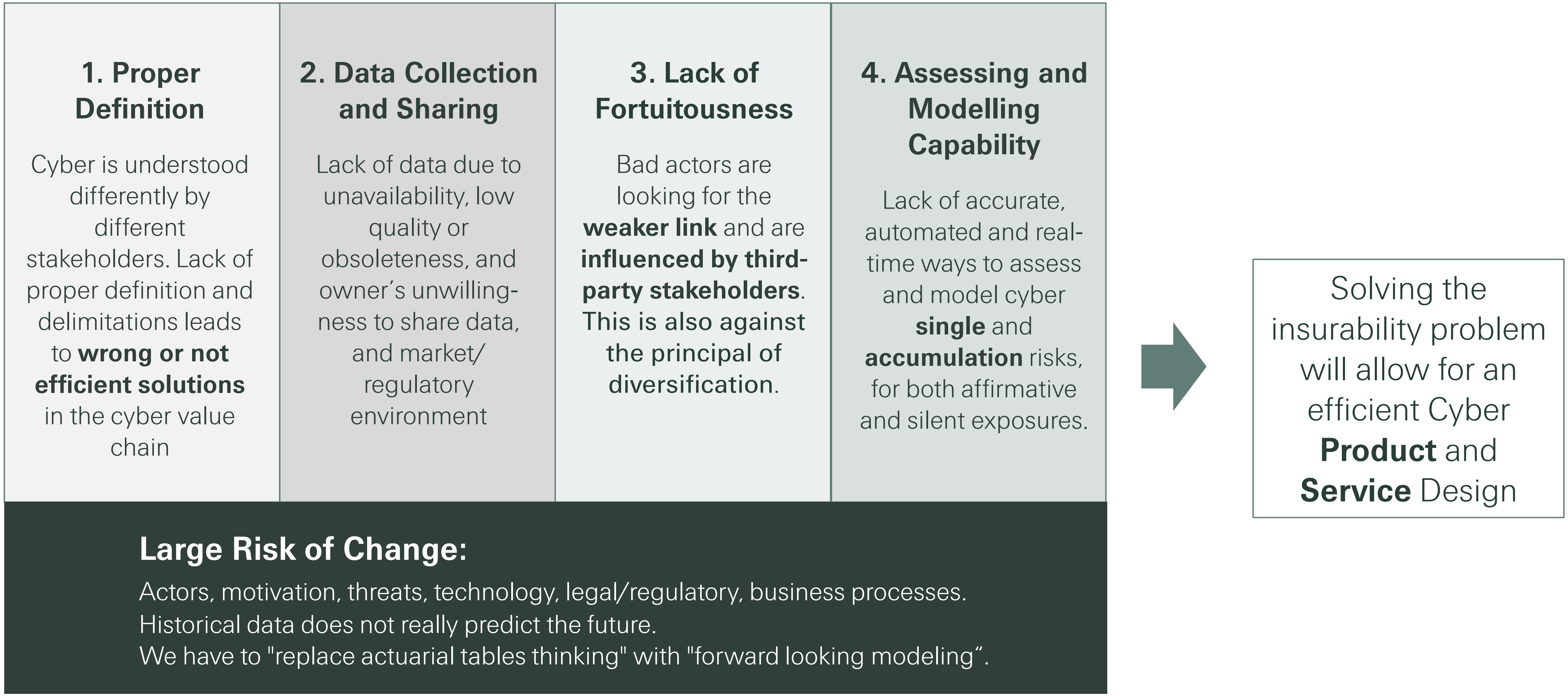
Human Factors

“4+1” framework to address the cyber insurability problem



Cyber Insurability

Breaking up the cyber insurability problem into four main cyber challenges



1. Proper Definition

Cyber is understood differently by different stakeholders. Lack of proper definition and delimitations leads to **wrong or not efficient solutions** in the cyber value chain

2. Data Collection and Sharing

Lack of data due to unavailability, low quality or obsoleteness, and owner´s unwillingness to share data, and market/ regulatory environment

3. Lack of Fortuitousness

Bad actors are looking for the **weaker link** and are **influenced by third-party stakeholders**. This is also against the principal of diversification.

4. Assessing and Modelling Capability

Lack of accurate, automated and real-time ways to assess and model cyber **single** and **accumulation** risks, for both affirmative and silent exposures.

Large Risk of Change:

Actors, motivation, threats, technology, legal/regulatory, business processes.
Historical data does not really predict the future.
We have to "replace actuarial tables thinking" with "forward looking modeling".

Solving the insurability problem will allow for an efficient Cyber **Product** and **Service** Design

Proper Definition

Issues	Solutions ?
IT-security – OpRisk – Claims – UW-ing: Common terminology and taxonomy	
Insured vs Insurers, e.g. Cyber exclusion clauses	
Cyber War and Cyber Terror definition	
What is a Cyber event ?	
Silent, non-affirmative, inherent, residual and others	
Cyber Security vs. Cyber Hygiene vs Cyber Resilience	

Data collection and sharing

Issues	Solutions ?
Common understanding of data – First Party vs. Third Party	
Confidentiality issues (e.g. GDPR)	
Limitation (purpose) in policies and contracts	
Single data or only aggregated (e.g. PERILS for Natural Catastrophes), even Index/Indices ?	
Competitive advantage vs. enough market understanding	
Anti-trust and Competition Laws	

Lack of fortuitousness

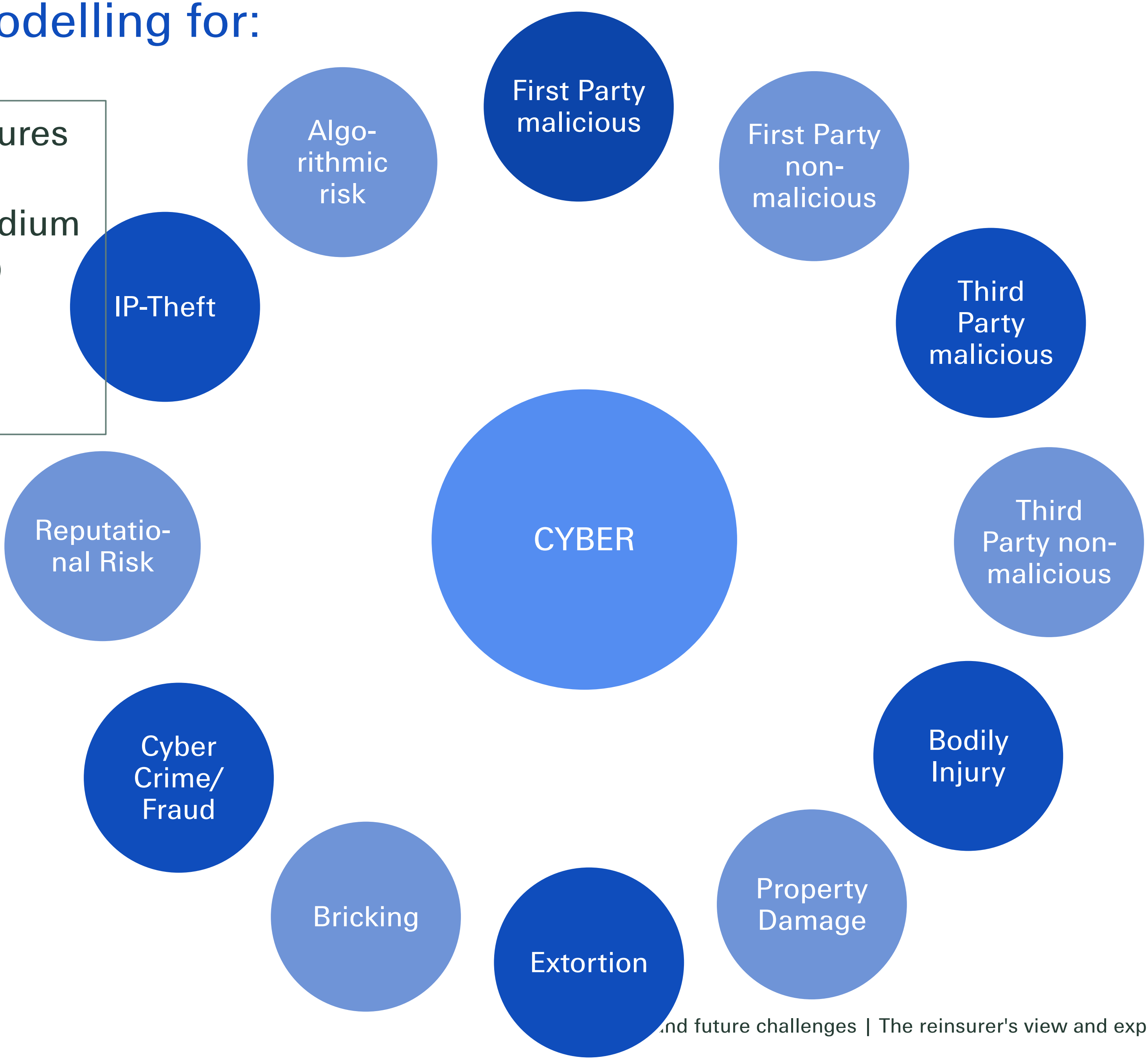
Issues	Solutions ?
Hackers target the weakest corporates	
Acts or communication of a government may increase motivation to attack corporates in this country	
Acts of a major corporate may increase motivation to attack corporates of the same industry segment.	
Doing nothing increases your chance of being attacked compared to peers which improved.	
Accumulation risk	

Assessing and modelling

Issues	Solutions ?
Single risks: Scoring - Underwriting - Costing	
Accumulation: over a portfolio of singles risks – over reinsurance treaties	
Accumulation vs. Aggregation vs. Clash vs Digital Dependencies (Interconnectedness)	
Treaty Costing	
Forward Looking Models with Risk-Drivers based probabilistic models.	
Dynamic system (real-time assessment), dynamic covers	
Rapid increase of Internet linked devices	

Assessing and modelling for:

For Critical Infrastructures
For Large Corporates
For SMEs (small & medium enterprises)
For Private Lines
Different exposures
Different budgets



CYBER

First Party malicious

First Party non-malicious

Third Party malicious

Third Party non-malicious

Bodily Injury

Property Damage

Extortion

Bricking

Cyber Crime/ Fraud

Reputational Risk

IP-Theft

Algorithmic risk

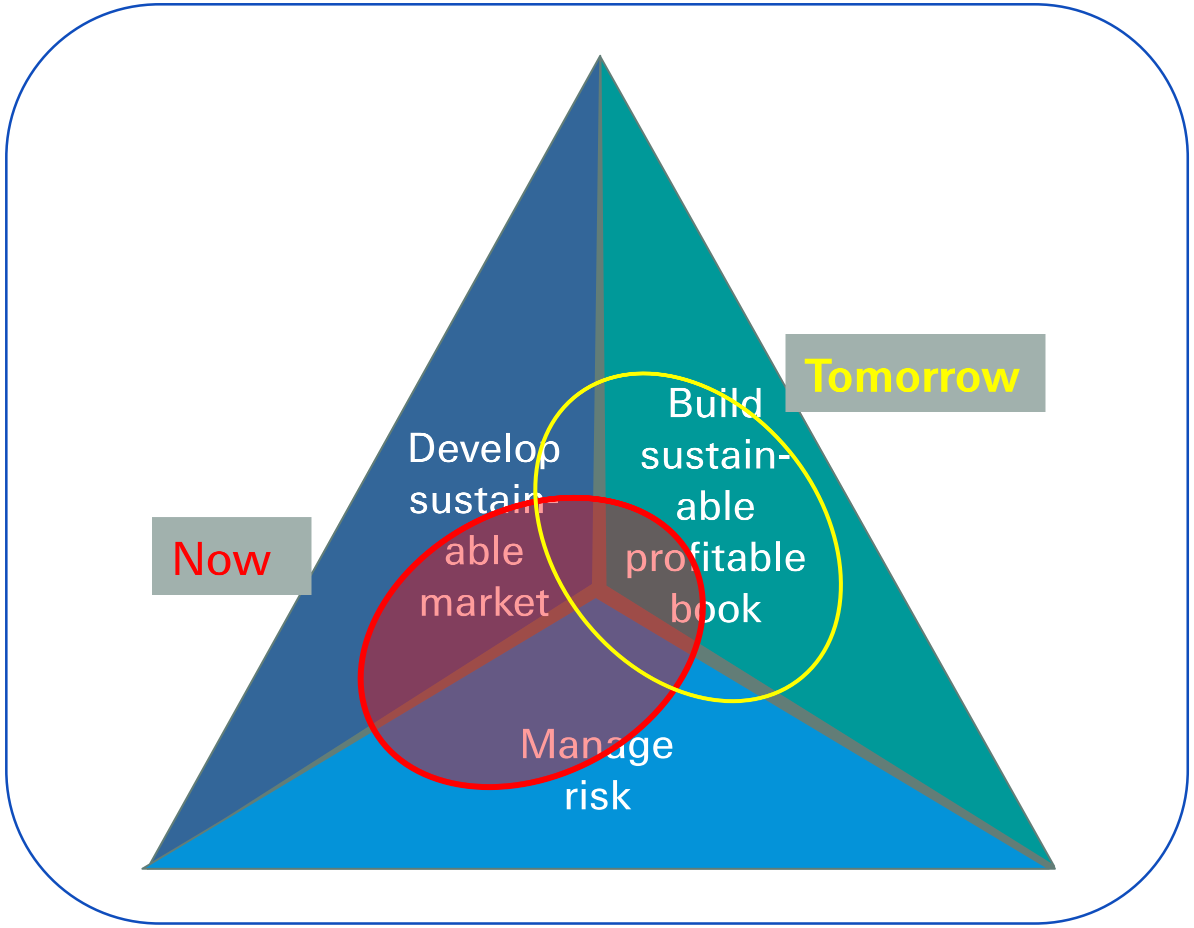
(Further) expectations:

Expectations	Solutions ?
Minimal IT- and Information Security standards/best-practice/good-practice	
Sharing of interest (Insured – Insurance – Reinsurance – State)	
Develop homogeneous Risk Assessments, fight information asymmetry	
Consider technical mono-culture	
Consider herd effect	
Introduce “security by design” for IoT, OT and IT (e.g. car crash tests)	
Expand economic models IT-security/hygiene investment vs cost of insurance	

Sharing of responsibility

- SW/HW producers
- trade associations
- (re)insurers
- insurance associations
- regulators
- law makers

Conclusion: The tasks at hand


Tomorrow
Build sustain-able profitable book
Develop sustain-able market
Now
Manage risk