



La Riassicurazione e la gestione dei Rischi



Corso SIA

Roma

04 Maggio 2021

Agenda



RISCHI CATASTROFALI



RISCHI EMERGENTI: SILENT CYBER

Il Contesto





1

I Rischi CATASTROFALI

La Modellizzazione del rischio Catastrofale

In Italia più di 400 terremoti distruttivi negli ultimi 2500 anni



Negli ultimi 2500 anni, l'Italia è stata interessata da più di 30.000 eventi sismici di media e forte intensità (superiore al IV-V grado della scala Mercalli), dei quali circa 560 di intensità uguale o superiore all'VIII grado (in media uno ogni 4 anni e mezzo).

Solo nel XX secolo, ben 7 terremoti hanno avuto una magnitudo uguale o superiore a 6.5 (con effetti classificabili tra il X e XI grado Mercalli).

I 10 terremoti più catastrofici degli ultimi 50 anni in Italia

Anno	Luogo	Magnitudo Mercalli
1968	Belice (Sicilia orientale)	6.1
1976	Friuli	6.5
1980	Irpinia	6.9
1984	San Donato Val di Comino (Appennino Centrale)	5.9
1990	Carlentini in Sicilia	5.7
1997	Umbria e Marche	6.0
2002	San Giuliano (Molise)	5.7
2009	L'Aquila	6.3
2012	Emilia Romagna	6.1
2016-2017	Italia Centrale	6.5

L'Italia è dunque un paese ad elevata "sismicità", caratterizzato da aree nelle quali i terremoti avvengono spesso ma sono di bassa energia (come Colli Albani a Sud di Roma, area vesuviana, area etnea), altre, invece, dove i terremoti avvengono più raramente ma sono di elevata energia (come Appennino calabro e Sicilia orientale).

Considerando i terremoti fino al VI grado della scala Mercalli, che producono cioè solo danni lievi, a parte la Sardegna, tutto il territorio nazionale è stato almeno una volta interessato da una scossa di questa intensità. Se consideriamo eventi di intensità superiore, non sono mai stati interessati il Piemonte, parte della Lombardia e dell'Alto Adige, la costa tirrenica dalla Versilia al Fiume Volturno, quella adriatica a sud di Ancona (escluso il Gargano) ed il Salento.

Penetrazione assicurativa

Le strutture costruite prima del 1996 sono considerate altamente vulnerabili.



Seppure il terremoto stia diventando un evento frequente, vi è una scarsa penetrazione assicurativa:

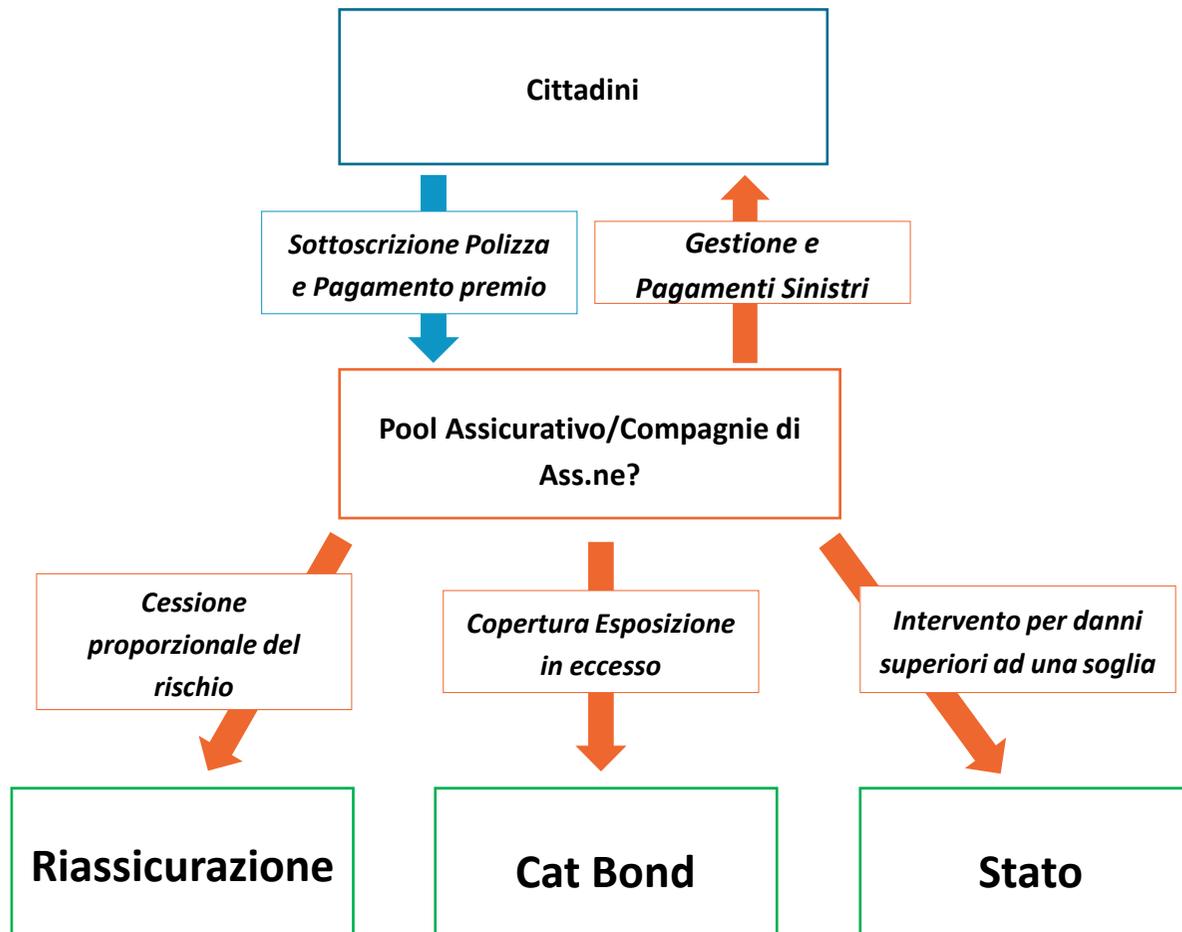
- si stima che i danni assicurati rappresentano tra il **2%-5%** del danno economico globale prodotto dai terremoti;
- generalmente la copertura terremoto è offerta a rischi commerciali ed industriali e si stima che solo il 30% di questa tipologia di rischi sia coperta.

Risarcimenti da Eventi Catastrofici



Ancora oggi lo Stato viene considerato come alternativa privilegiata per ottenere un risarcimento per i danni da evento catastrofico

Possibile soluzione?



Solvency 2 / Mercato / Riassicurazione



- Quanta Capacità Catastrofale?
- Quale strumento utilizzare per coprire efficientemente la eventuale capacità aggiuntiva?



Strumento/Azione	Costo/Complessità	Considerazioni
ILS (Cat Bond,...)	Molto Costoso e Complesso	Anche in termini di costo risulta conveniente per programmi multi peril e multi country
Internal Model	Molto Costoso e Complesso	Processo lungo e complesso + costi acquisizione Tool
Riassicurazione	Costo di Mercato	Estrema efficienza costi/benefici



RIASSICURAZIONE – LO STRUMENTO PIU' EFFICIENTE

Mercato ILS

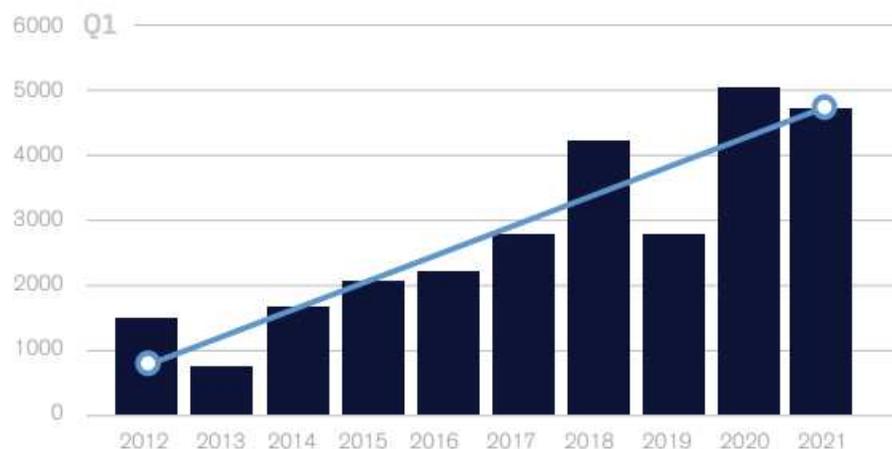
I **Cat Bond** rappresentano una reale alternativa al mercato riassicurativo e forniscono una soluzione efficiente al problema di “disaster gap”. Si tratta di obbligazioni che offrono una garanzia connessa al verificarsi di un evento calamitoso (uragano, terremoto o altro evento di carattere naturale) di entità prestabilita.

Oltre a rappresentare un'alternativa alla riassicurazione tradizionale premettono di trasferire i rischi a una platea più ampia di investitori.

I bond catastrofali, inoltre, hanno la caratteristica di essere collateralizzati al 100% e sono strutturati in modo da eliminare il rischio di controparte.

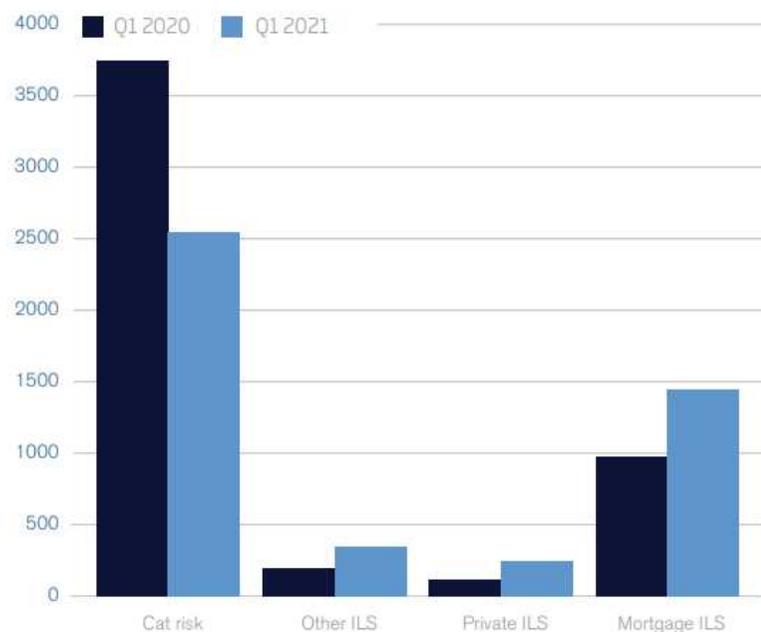
Nel primo trimestre del 2021 sono stati emessi \$ 2,8 miliardi di “property catastrophe bonds”.

Le emissioni di catastrophe bond and ILS del primo trimestre 2021 sono diminuite di 424 milioni di dollari su base annua rispetto al primo trimestre 2020, ma risultano sempre in crescita (+68%) rispetto alla media decennale. Infatti, il primo trimestre 2021 è il secondo più grande primo trimestre nella storia del mercato e questo è un segno di forte appetito da parte degli investitori.



Mercato ILS

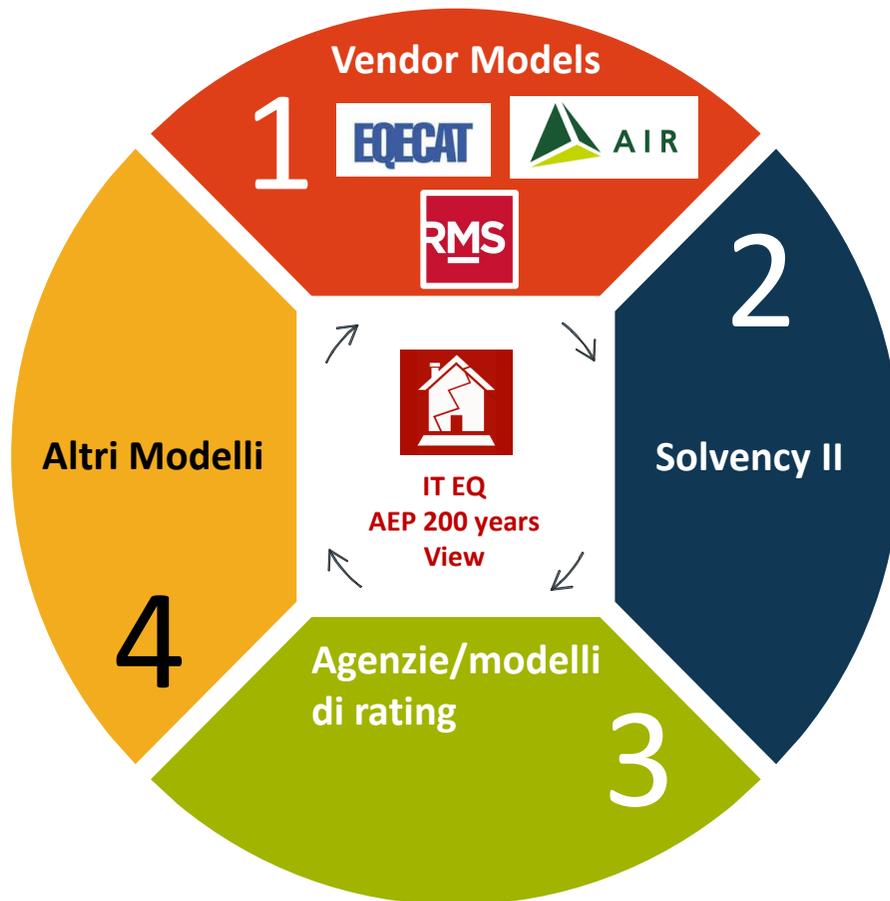
Il grafico sottostante presenta i diversi tipi di rischi per i quali sono stati emessi i bond nel 1° trimestre 2020 e 2021. È evidente che i **Property Cat Bond** rappresentano più del 60% delle obbligazioni totali e sono emessi soprattutto in US.



In generale, gli investitori hanno appetito a supportare i pool catastrofali soprattutto se contribuiscono alle questioni ambientali, sociali e di governance (ESG). Sono interessati anche a pool Cat non US per la diversificazione geografica degli investimenti.

Ci sono diversi pool catastrofali che comprano cat bond. Il cat pool bond più recente è stato in Europa ed è una transazione terremoto parametrica del 2015 per il Turkish Catastrophe Insurance Pool.

Solvency 2: Nat Cat Scenario / Mercato / Riassicurazione



Differenti Output per modelli differenti

Quale modello rappresenta verosimilmente il rischio di portafoglio?

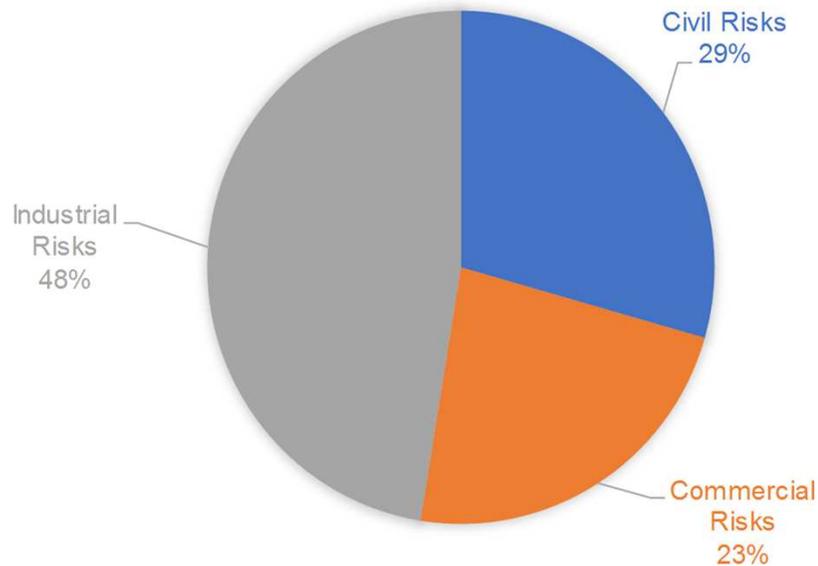
Necessità di una visione «personalizzata» e realistica del rischio

Solvency 2: Nat Cat Scenario / Mercato / Riassicurazione / Esempio

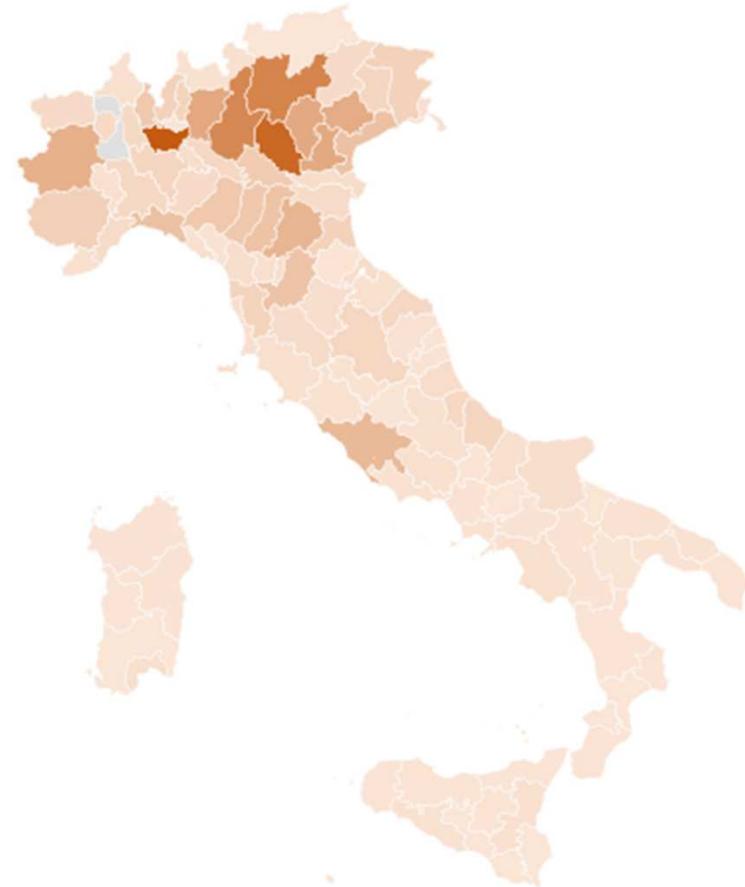
Esempio Portafoglio

- Somme Assicurate: **109 miliardi** di Euro
- Limiti di Indennizzo: **35 miliardi** Euro

Distribuzione per Tipologia di Rischio



Distribuzione per provincia



Solvency 2: Nat Cat Scenario / Mercato / Riassicurazione / Esempio



VENDOR MODELS

RMS: Euro 478,6m
EQECAT: Euro 283,4m
AIR: Euro 234,7m



MODELLI DI RATING

Ptf
(Esempio)
AEP 200
anni

STANDARD FORMULA EQ SCR (SOMMA ASSICURATA)



Euro 1.071m

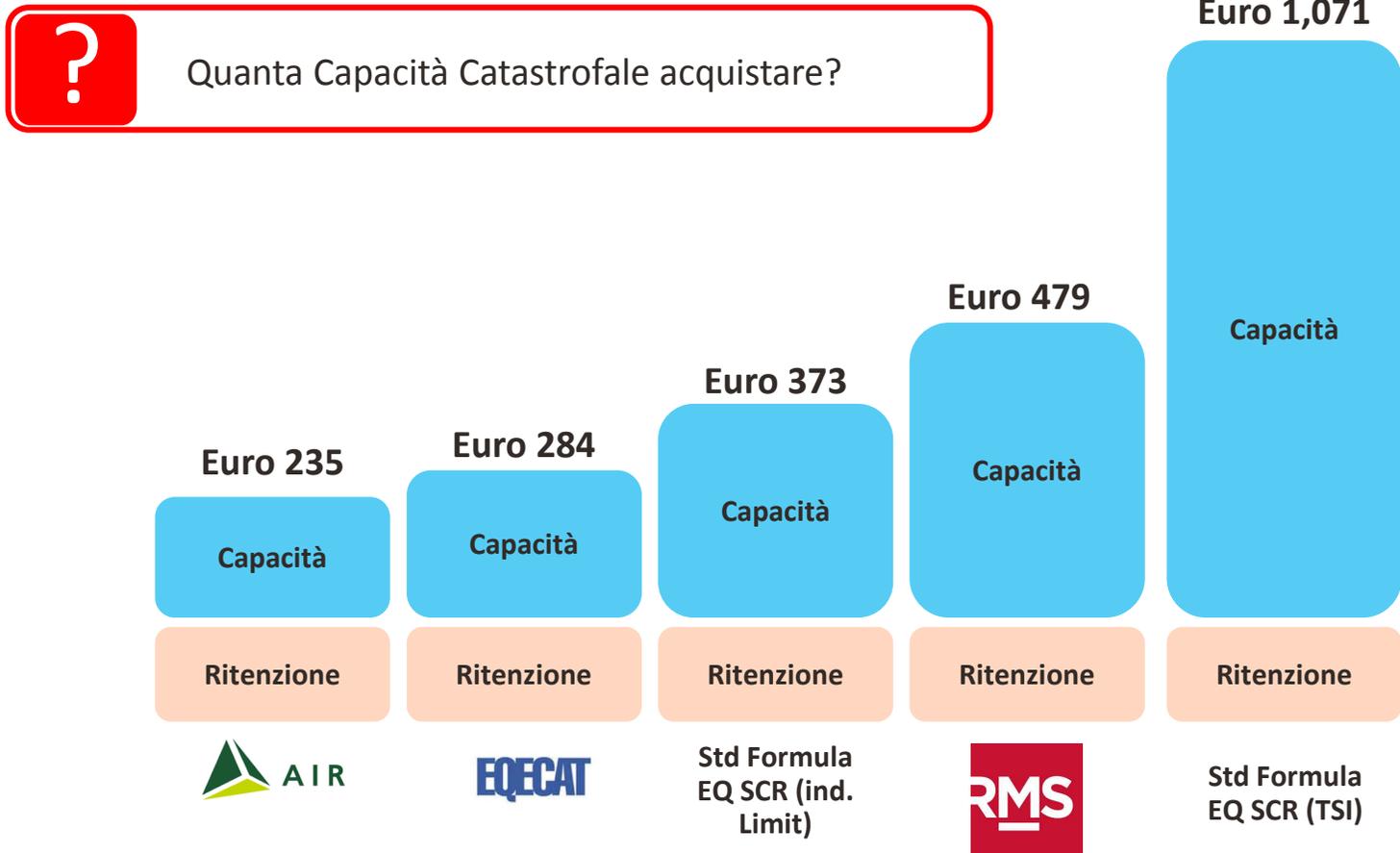
STANDARD FORMULA EQ SCR (LIMITI INDENNIZZO)



Euro 372,8m



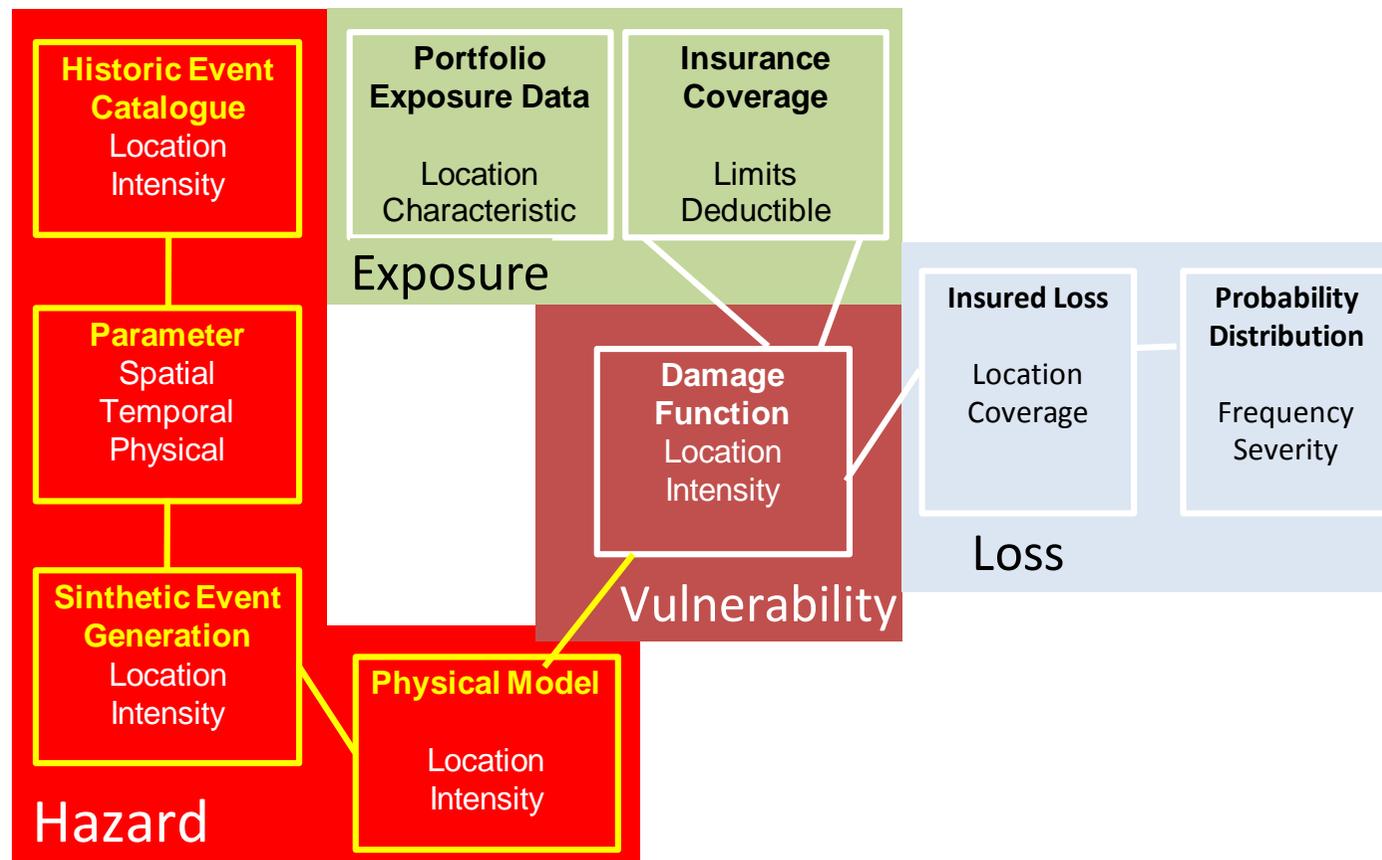
Solvency 2: Nat Cat Scenario / Mercato / Riassicurazione / Esempio



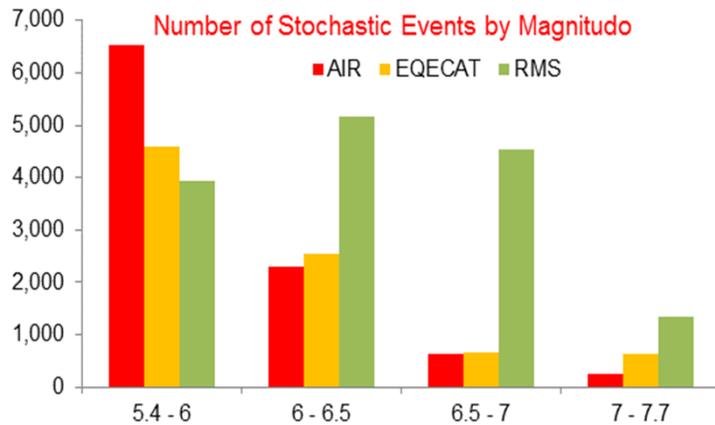


RISCHI CATASTROFALI E MODELLI DI VALUTAZIONE

Struttura del Modello

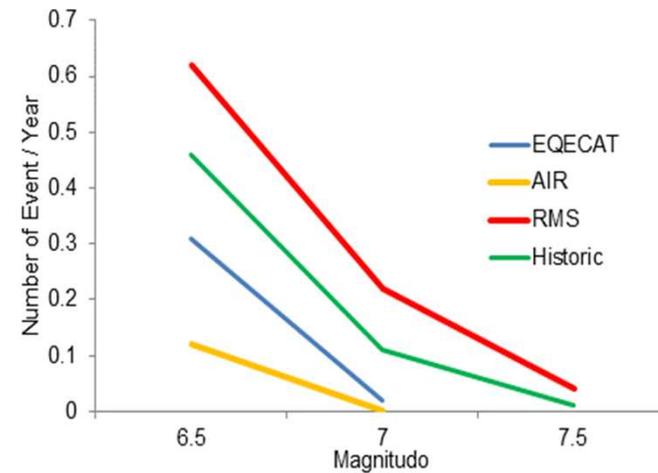
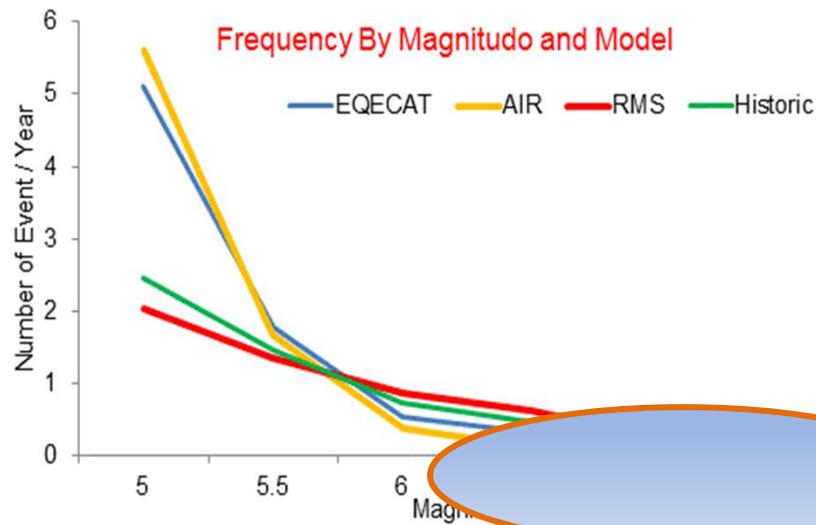


I modelli: Frequenza degli Eventi e differenze tra i modelli



Vendor	Eventi Magnitudo Bassa	Eventi Magnitudo Alta
RMS	-	+
EQECAT (RQE)	+	-
AIR	+	-

RMS molto più in linea con la frequenza storica



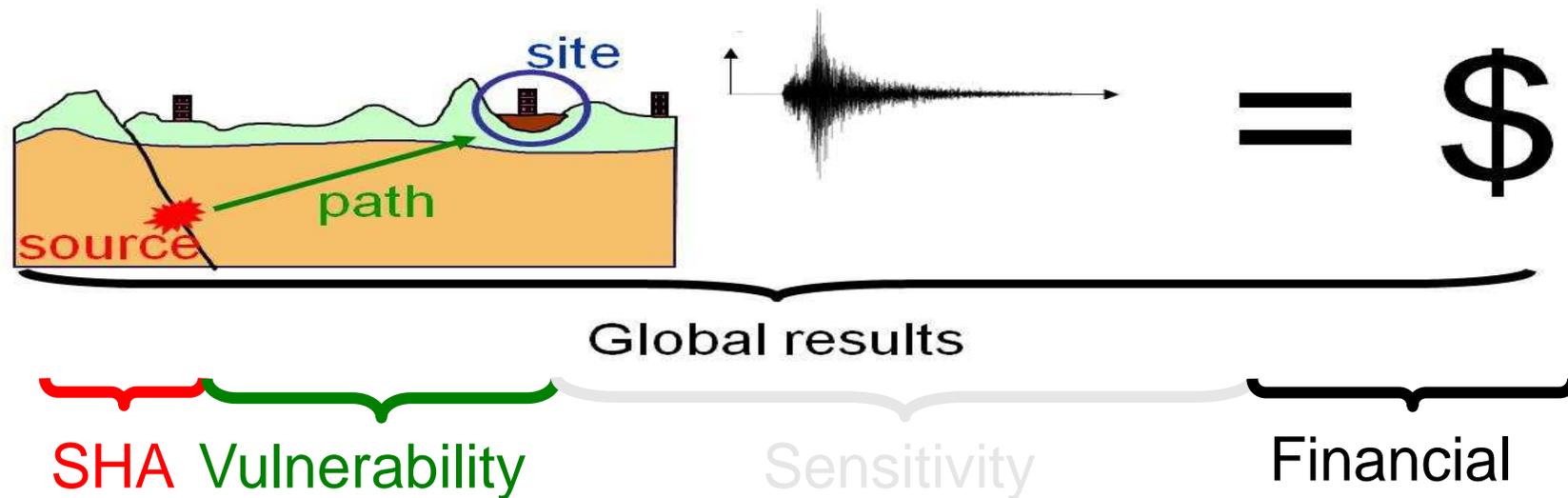


I MODELLI TERREMOTO

Cosa sono e come funzionano

Il modello Terremoto

Un modello probabilistico attraverso la combinazione delle probabilità di avvenimento degli eventi, della stima del movimento del terreno e del danno prodotto, definisce come risultato un **PML** (Probable Maximum Loss) dove ad ogni valore di danno è associata una probabilità (periodo di ritorno) di eccedere quel determinato valore



Il modello Terremoto

Ogni modello per la valutazione del rischio terremoto è costituito dai seguenti quattro moduli:



I modelli Terremoto

I tre principali modelli sono:

-  RMS
-  RQE
-  AIR

RMS v.18

E' il modello più comunemente usato in Italia per la valutazione del rischio terremoto e per definire la strategia di riassicurazione. Ha un database di circa 15.000 eventi ed è l'unico dei tre modelli a simulare eventi con epicentro in zone di frontiera. *RMS* è un modello stocastico sviluppato dalla società *RMS*, società di consulenza specializzata nello sviluppo di soluzioni per la gestione dei rischi. I risultati dell'analisi del rischio sismico sono generati utilizzando modelli sviluppati da Risk Management Solutions, Inc. Le tecnologie e i dati utilizzati per fornire queste informazioni si basano su dati scientifici, matematici e modelli empirici e sull'esperienza acquisita da parte di ingegneri sismici, geologi e geotecnici. Come per ogni sistema fisico complesso, particolarmente per quelli che presentano basse frequenze di avvenimento e severità molto importanti, i risultati reali di eventi catastrofici possono differire dai risultati simulati.



CoreLogic RQE v.19

E' il modello simile nell'impianto ad RMS, ma con un database di circa 8.000 eventi. RQE è un modello stocastico sviluppato dalla società *Eqecat*, società di consulenza nel settore assicurativo, riassicurativo e finanziario, e permette la gestione del rischio catastrofale.



AIR v.7

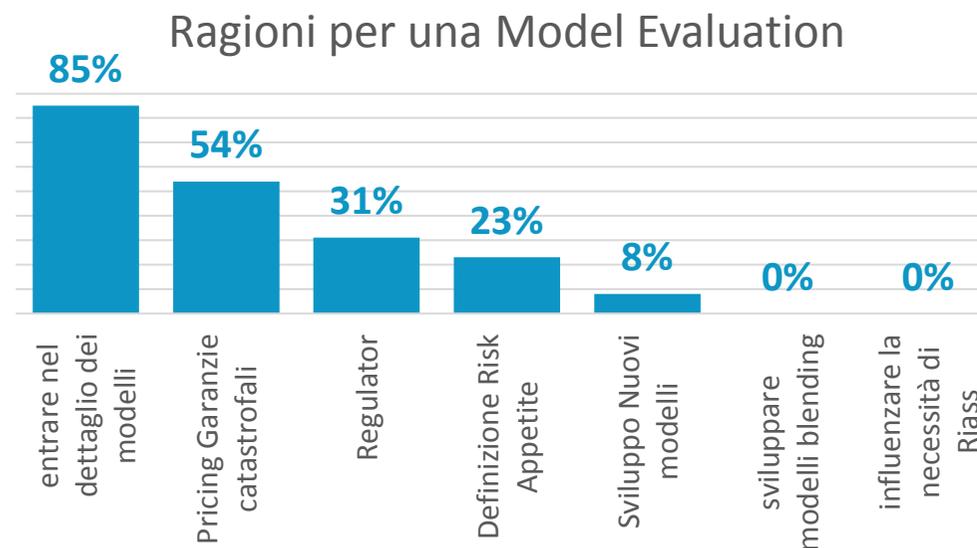
E' il modello principalmente usato nella stima degli uragani americani e produce risultati per il terremoto non in linea con gli altri due tool. Air è un modello stocastico sviluppato dalla società AIR Worldwide utilizzato da riassicuratori, assicuratori e da coloro che hanno l'esigenza di gestire il rischio come aziende, organizzazioni governative e parastatali, investitori, *hedge fund* e altri istituti finanziari. Nel 2009, una nuova versione ha apportato notevoli modifiche nella modellizzazione del rischio Terremoto nell'area Mediterranea contribuendo a ridurre, ancora più di prima, i risultati di PML su tutti i periodi di ritorno.



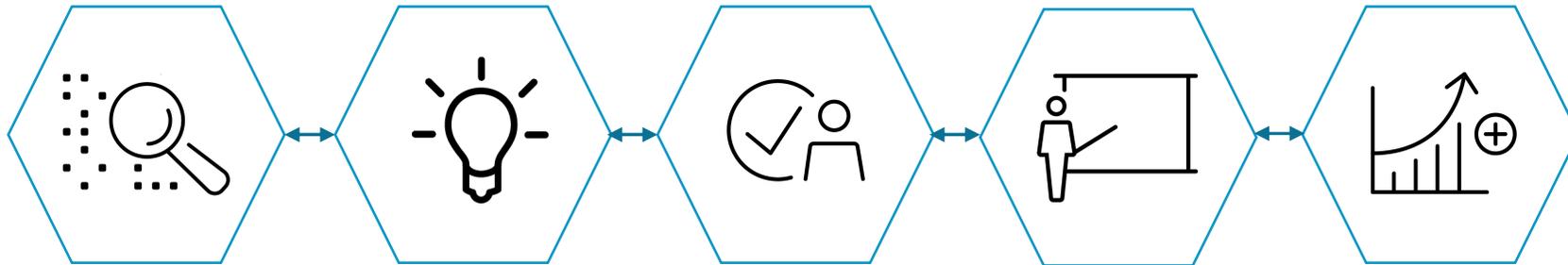
Necessità di sviluppo di una “View of Risk” personalizzata

- Data la complessità dei modelli e le nuove visioni dei rischi catastrofici conseguenti ai nuovi regolamenti le compagnie stanno dimostrando un interesse crescente verso una visione «customizzata» e realistica del rischio catastrofico
- Lo sviluppo di una propria visione del rischio rappresenta un insieme di azioni finalizzate alla «model evaluation» di modelli esistenti o alla creazione di nuovi modelli grazie a società del settore dedicate alla costruzione di modelli catastrofici, per tutti i maggiori Peril / Territori

- Un'indagine condotta da Aon Inpoint su 13 mercati riassicurativi operanti sul Mercato di Londra ha evidenziato la necessità del mercato stesso di una «model evaluation» dei rischi catastrofici



Sviluppo di una “View of Risk” – processo e soluzioni



- Analisi sulla consistenza del modello rispetto alla realtà
- Il processo può variare sulla base delle dimensioni delle compagnie
- Definizione di una visione appropriata del rischio
- Customizzazione
- Costruzione di un nuovo modello
- Acquisto di modelli o di componenti
- Partnership
- Valutazione con il cliente
- Valutazione dell'efficienza del New Model rispetto a quello corrente
- Divulgazione e presentazione ai Mercati Riassicurativi
- Integrazione in strutture preesistenti

Processo di «model evaluation»

Il processo di model evaluation sul quale si basa la definizione del View of Risk della compagnia è definito dalle seguenti attività:

Pre - selection

- Individuazione del Vendor Model
- Analisi di dettaglio dei moduli: Hazard, Vulnerability e Financial

Full Evaluation

- Analisi tecnica
- Tests & sensitivities
- Valutazione dei risultati

Data Quality

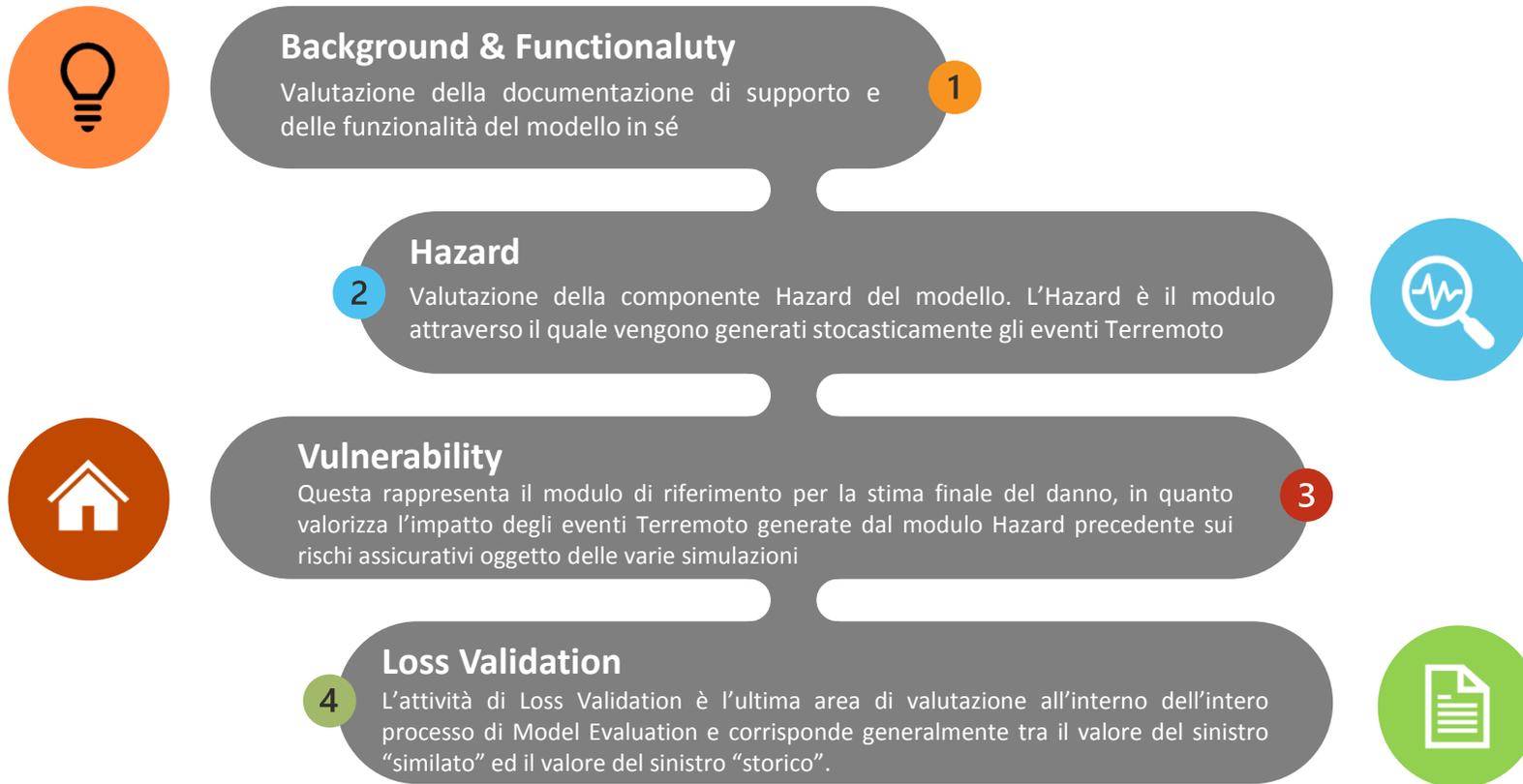
- Supporto nel geocoding
- Applicazione condizioni assicurative (deductibles, limits)
- Analisi rischi (Lob, occupancy)

Disclosure

- Presentazione metodologia
- Documento tecnico di exposure
- Documento tecnico dei risultati

Processo di «model evaluation»

Le caratteristiche dei modelli prese in considerazione nel processo di Model-Evaluation sono le seguenti:



Processo di «model evaluation»



In particolare, le attività di analisi dell'Hazard e della **Vulnerability** sono quelle fondamentali per valutare come il modello si adatta alle ultime evidenze scientifiche in merito al rischio Terremoto.

Le prime analisi hanno portato ad escludere RQE, in quanto il modello sembra essere il meno aderente alle recenti mappe di rischio.

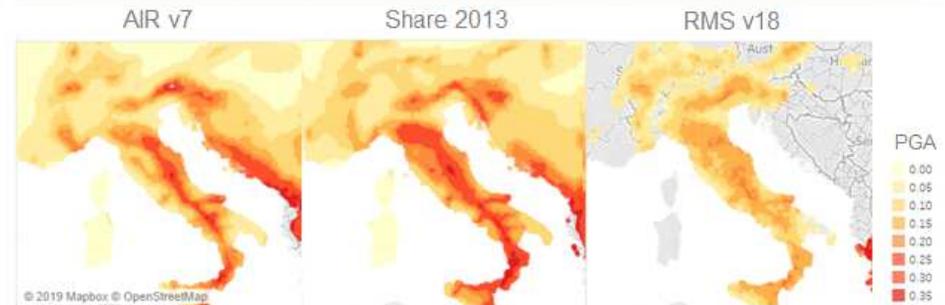
La modellizzazione dei terremoti deve infatti sempre tenere conto degli aggiornamenti più recenti delle mappe di pericolosità sismica (Hazard) e includere ad esempio le conoscenze derivanti dai recenti eventi storici.

NOTA: Generalmente tutti i modelli terremoto prendono come riferimento delle mappe di rischio sismiche (Hazard) standard ed ufficialmente riconosciute. Tali mappe standard sono generalmente costruite a livello europeo. L'ultima a cui si fa riferimento è quella derivante dal progetto SHARE del 2013 lanciato da GEM (Global Earthquake model), una fondazione di ricerca che opera in questo settore ed in partenariato con altri istituti di ricerca in giro per il mondo. Il progetto SHARE è in fase di aggiornamento ed a giugno 2021 verrà pubblicamente reso disponibile il nuovo Hazard Europeo (SERA) sul quale dovranno essere sicuramente aggiornati i modelli

Processo di «model evaluation»

Riportiamo qui di lato alcune evidenze dell'analisi dell'Hazard di RMS ed AIR, la cui mappa di pericolosità è stata confrontata con quella ufficiale di SHARE 2013.

PGA (Peak Ground Acceleration)



Nella figura viene rappresentato l'indice **PGA** per AIR, RMS e Share 2013. Il PGA che sta per «**Peak Ground Acceleration**» è la misura della massima accelerazione del suolo indotta dal terremoto e registrata dagli accelerometri. Diversamente dalla scala Richter, che misura l'ampiezza globale di un terremoto, il PGA misura l'intensità di un terremoto in una singola area geografica. La figura evidenzia come l'Hazard di AIR sia più coerente con la mappa di pericolosità di Share 2013 rispetto a quanto lo è RMS.

Riportiamo infine un'evidenza dell'analisi delle curve di vulnerabilità.

Considerando una generica location a Milano e i seguenti differenti materiali di costruzione:

- Muratura non Rinforzata (URM)
- Muratura Rinforzata (RI Masonry)
- Cemento Armato (RC)
- Acciaio (Steel)

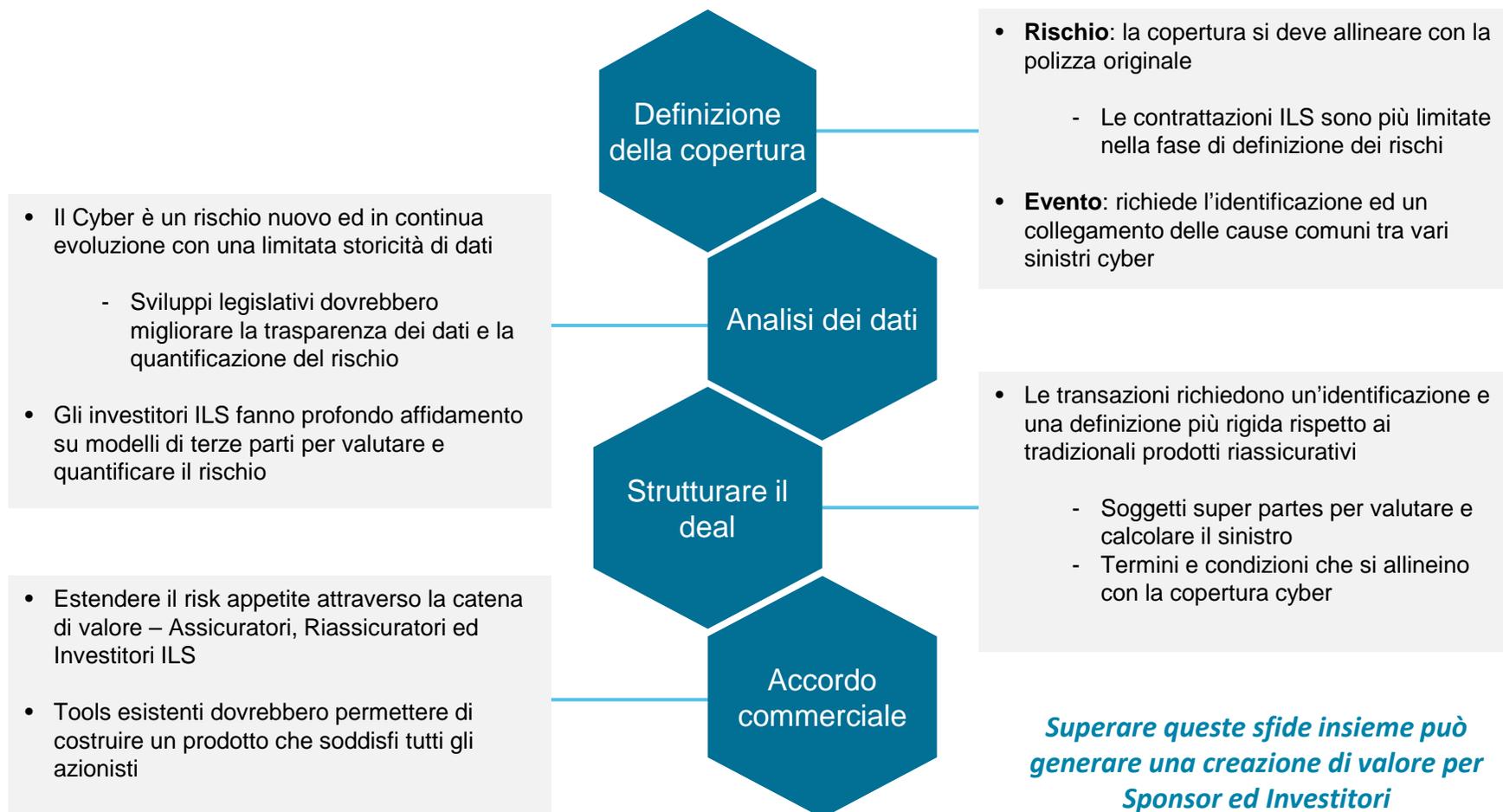
si evince che RMS sovrastima la vulnerabilità, mentre, al contrario, AIR la sottostima.

Sulla base delle precedenti considerazioni sia in termini di hazard sia di Vulnerability, la valutazione del rischio Terremoto potrebbe essere frutto di un blend (mix) tra gli outputs derivanti da RMS e quelli derivanti da AIR

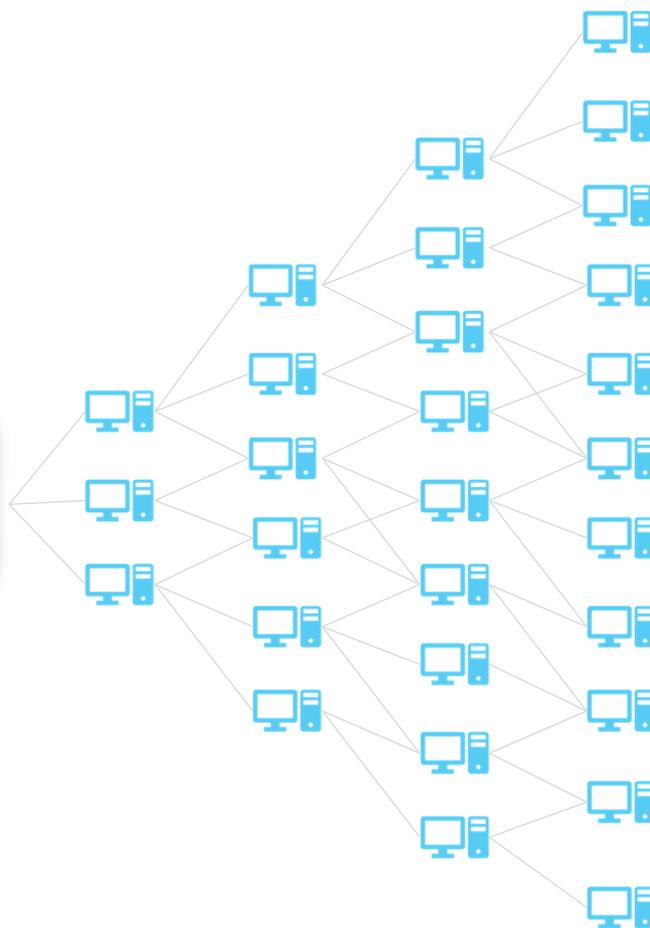
Cyber



Sfide della (Ri)Assicurazione Cyber



Il rischio Cyber è al 2° posto tra i rischi più temuti dalle aziende



In poche ore...



150 paesi coinvolti

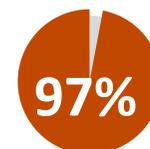


200.000 macchine infettate



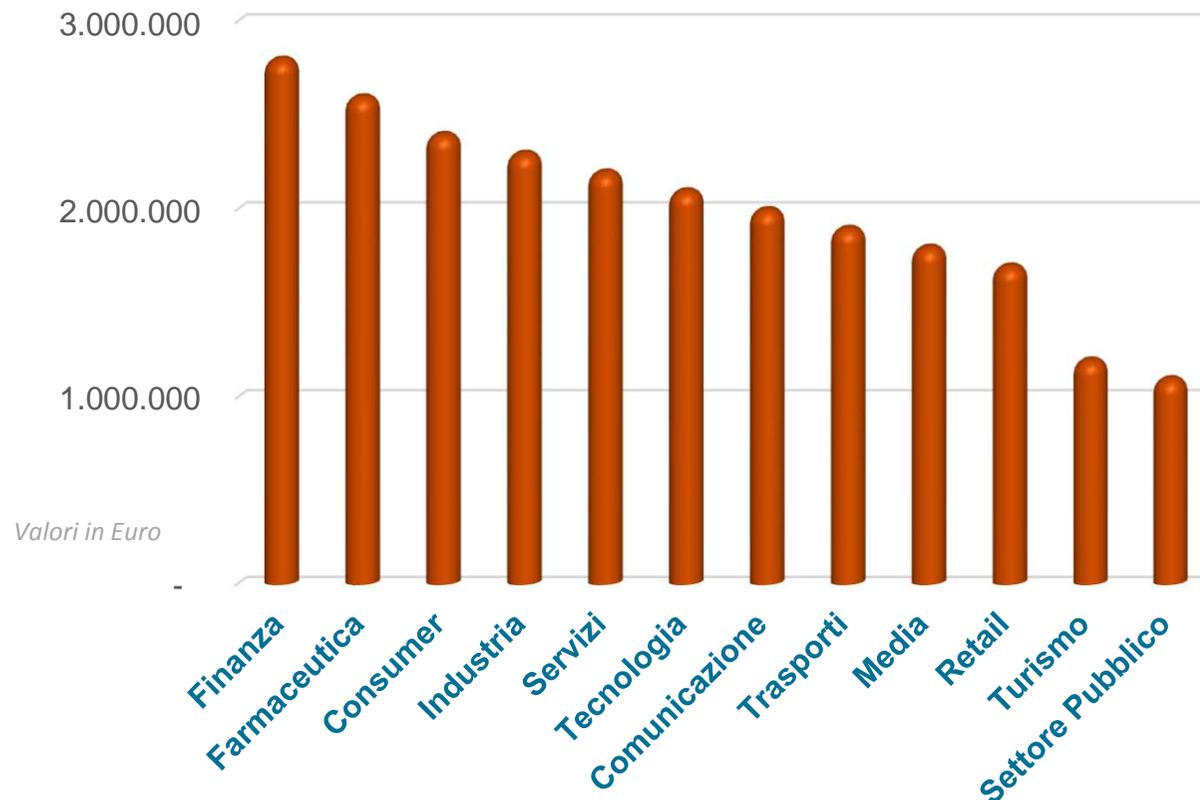
4.000.000.000 di USD di danno

...dopo un anno...



Delle aziende risulta ancora vulnerabile come prima dell'attacco

Danno medio da attacchi cyber alle imprese in Italia per tipo di attività



Nel 2017, in Italia i danni Cyber ammontavano a circa Euro **10mld**

Mediamente servono **205 giorni** ad una azienda per rendersi conto di essere sotto attacco;
74 giorni invece per riprendersi dall'attacco.

Tra il **30%-50%** delle aziende italiane subiscono danni da attacchi informatici.

In 1 anno di osservazione, di queste il 45% circa ha subito da 2-5 attacchi, il 17% circa più di 5 attacchi. Indipendente, invece, la distribuzione geografica, il numero di addetti ed il livello di tecnologia adottata

Fonte: Banca d'Italia

I principali incidenti cyber tradizionale



- ① **VIOLAZIONE DATI CONFIDENZIALI (DATI PROPRI E DI TERZI)**
- ② **MALFUNZIONAMENTO DEI SISTEMI INFORMATICI/RETE DI COMUNICAZIONE**
- ③ **CANCELLAZIONE O DETERIORAMENTO DEI DATI**
- ④ **VIOLAZIONE DATI CONFIDENZIALI (DATI PROPRI E DI TERZI)**
- ⑤ **CRITTOGRAFIA DEI DATI E FURTO/FRODE FINANZIARIA**

Rischio Cyber sotto la lente di ingrandimento anche da parte dell'EIOPA



Bisogno di **maggior consapevolezza nella gestione del rischio**, in riferimento alle reali esigenze dei clienti

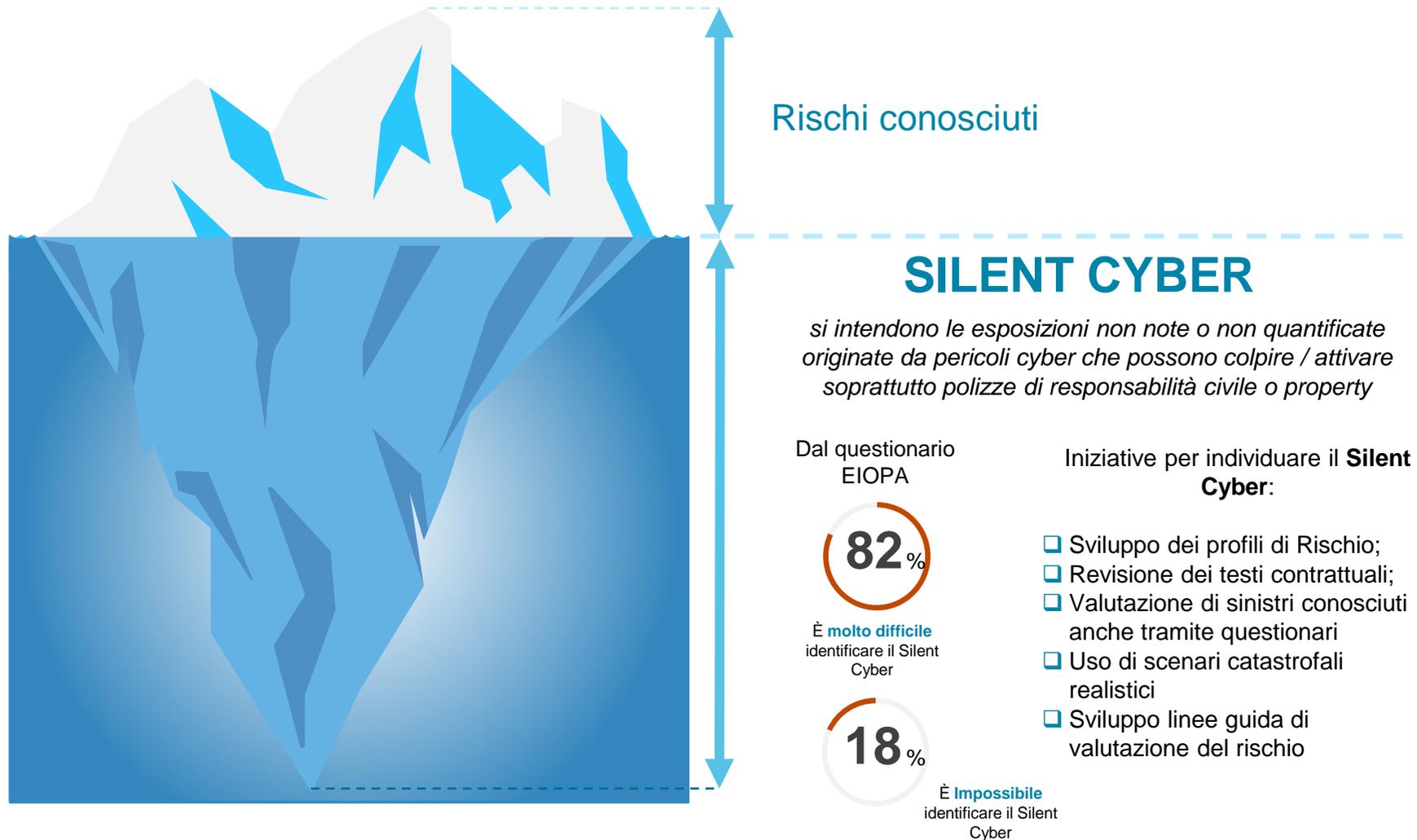
La **mancaza di sottoscrittori specializzati** e soprattutto di **dati e modelli quantitativi** rappresentano un ostacolo non di poco conto nel concretizzare l'opportunità di sviluppo dell'industria assicurativa

Con la maggior consapevolezza del rischio, nonché con i cambi di normativa e il verificarsi di una maggior frequenza di attacchi cyber, dovrebbe **umentare anche significativamente la richiesta e la necessità di copertura assicurativa cyber sul mercato**

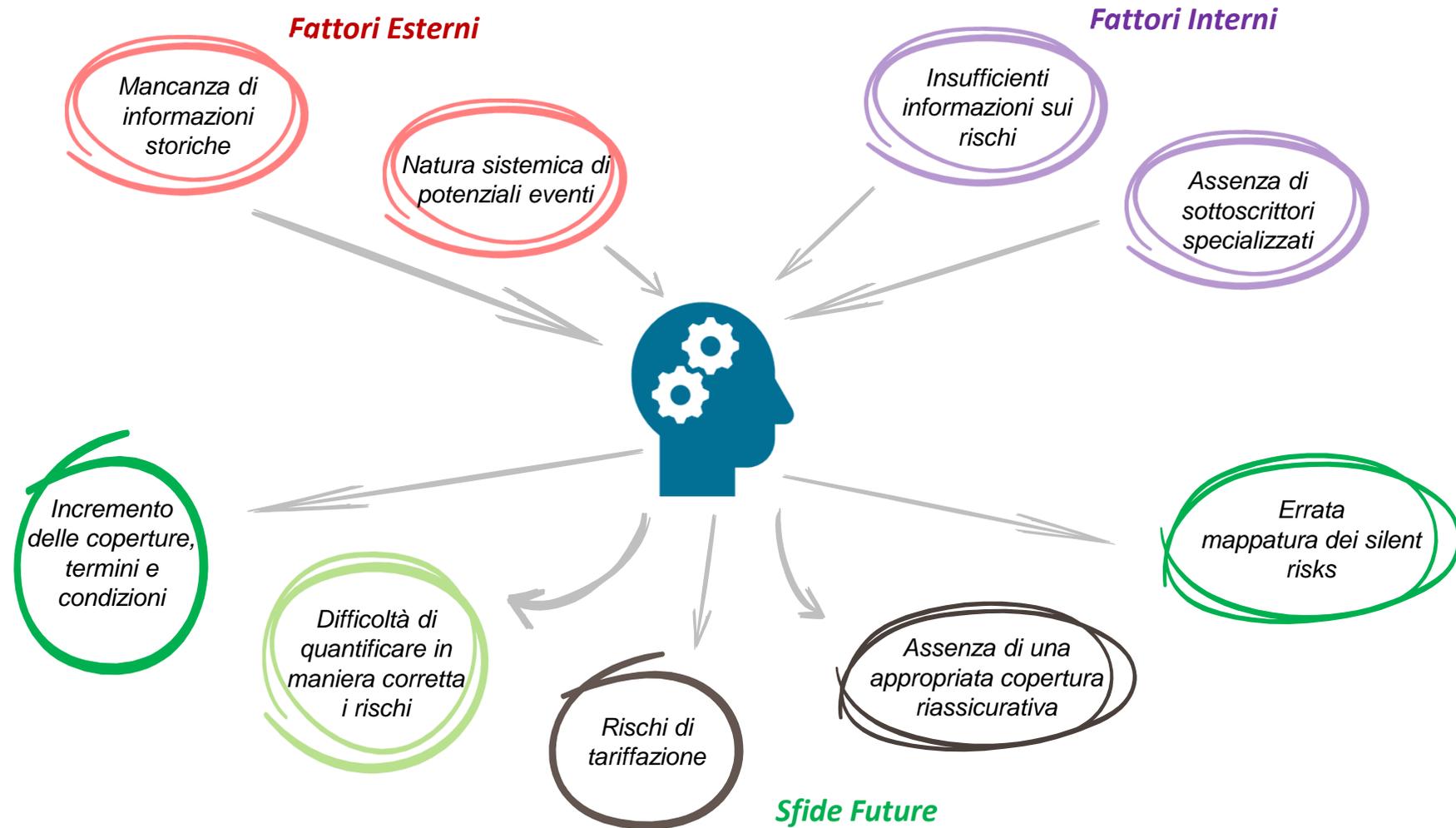
Al momento i modelli qualitativi sono utilizzati molto più frequentemente di quelli quantitativi nello stimare pricing, esposizioni e cumuli. La mancanza di dati, infatti, è il principale ostacolo di molti modelli. Inoltre, il **silent cyber** è stato definito da EIOPA come **uno dei principali rischi emergenti** nella corretta identificazione e quantificazione dei cumuli di rischio

Non solo il business commerciale, ma anche il **continuo sviluppo tecnologico** e dei suoi fruitori fa pensare ad una domanda crescente di copertura cyber anche su base individuale

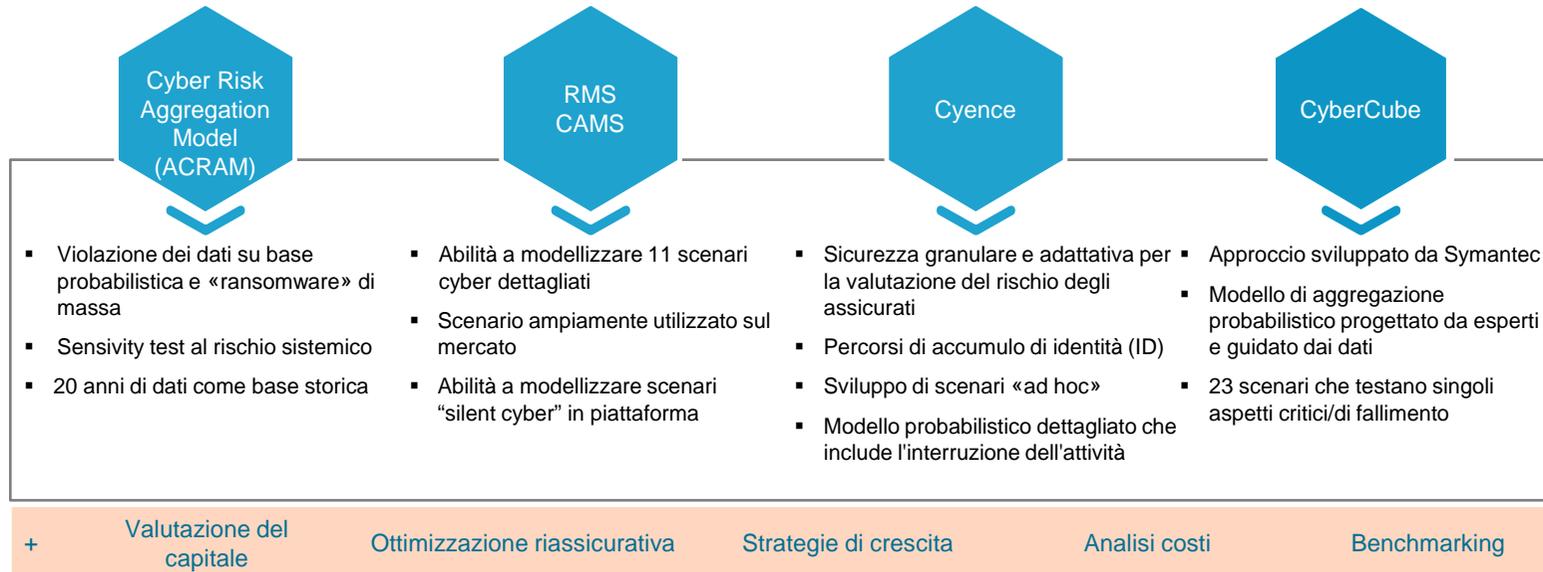
Silent cyber: la parte sommersa di un iceberg



Necessità di una maggiore conoscenza del cyber risk



Processo di modellizzazione



Approccio multi-modello nell'aggregazione IT

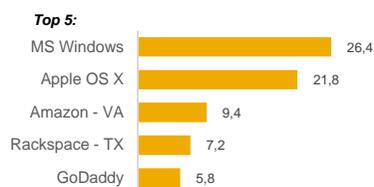
	Selezione rischi	Aggregazione	Analisi Probabilistica	Cat + Non-cat	Telemetria	Adozione sul mercato
AIR						
Bitsight						
Corax						
CyberCube						
Cyence						
FICO						
RMS*						
Security Scorecard						

Legenda: Debole In sviluppo Adeguato Forte

Esempi di output di modellizzazione cyber usando modelli commerciali per scenari IT

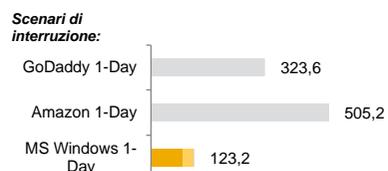
Processo di modellazione

1 Aggregazione



Identificare i fattori chiave che determinano le perdite a livello di portafoglio

2 Analisi Scenari



Valutazione di scenari chiave

3 Stima PML



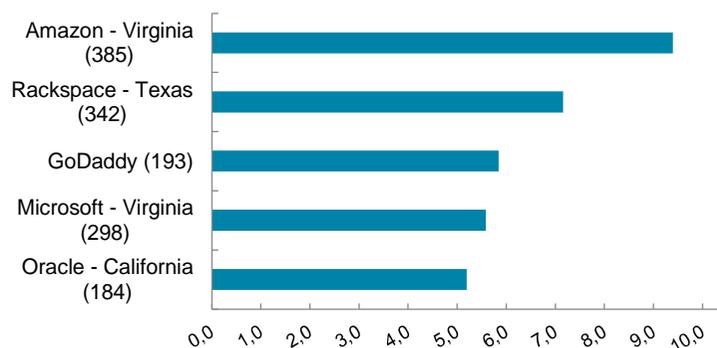
Curva di scenari attesi di perdita

4 Ottimizzazione Riass.ne

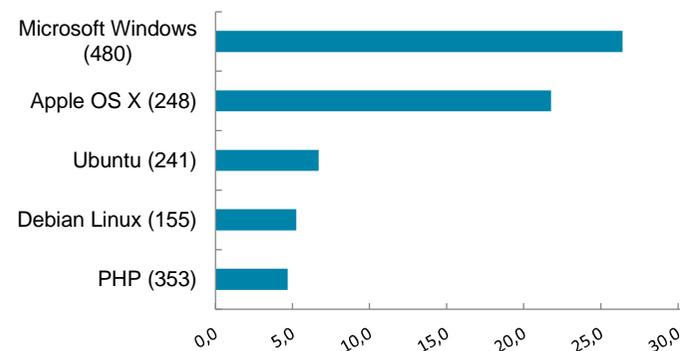


Valutazione efficienza economica del programma

Sinistri Attesi a seconda dei Provider (\$ milioni)



Sinistro atteso a seconda dei Software (\$ milioni)



Fonte: Aon Benfield Analytics

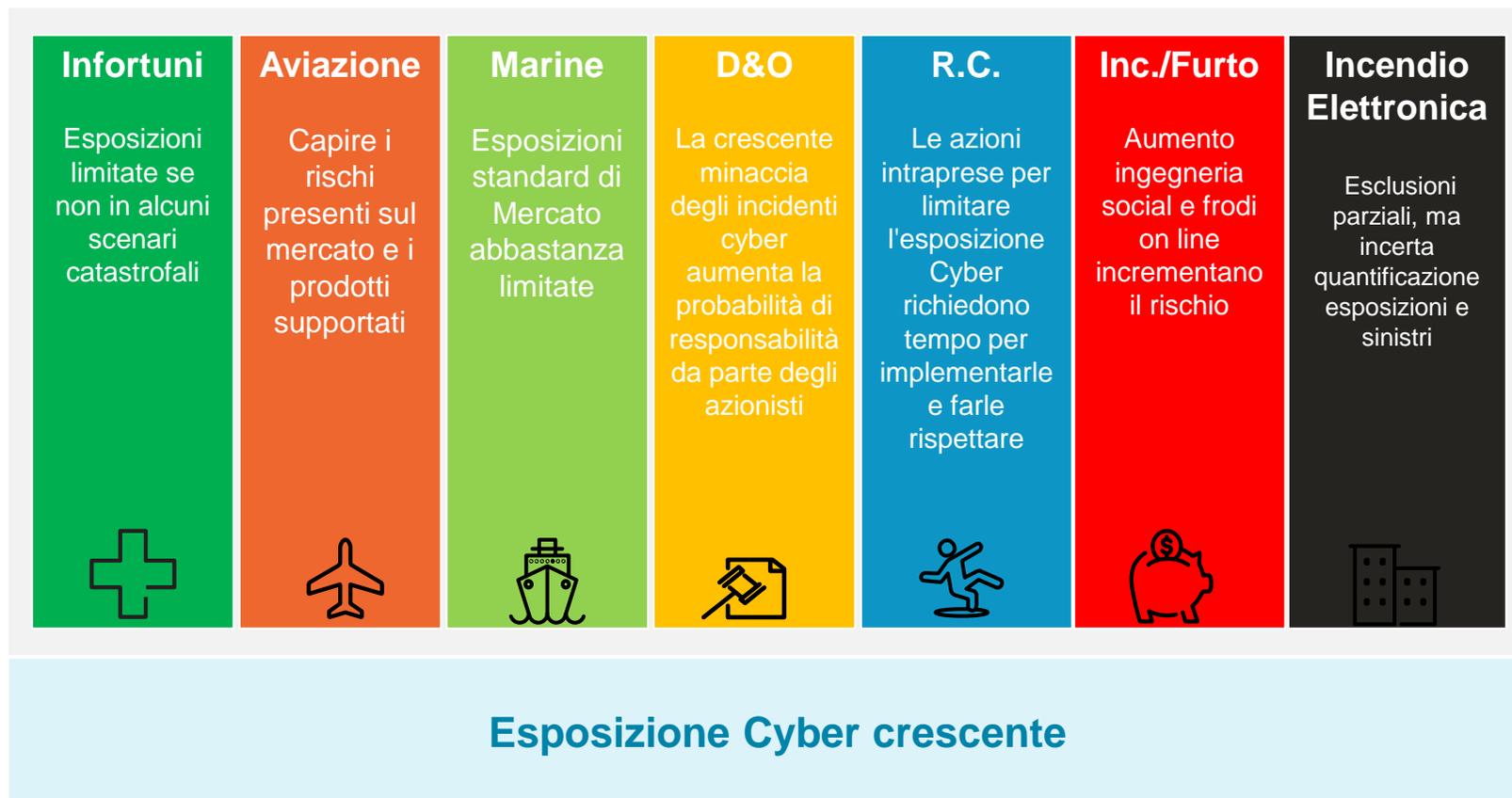
Definizione, quantificazione e copertura di uno scenario Silent Cyber



Migliorare coperture, pricing e capacità

Modellizzazione condivisa e spiegata ai mercati riassicurativi per garantire prezzi ottimali

Fase 1: individuare i rischi Cyber negli attuali portafogli assicurativi



Fase 2: valutare le esclusioni e più in generale i wording

Di lato sono mostrate alcune delle aree ritenute fondamentali:

- Estesa definizione di danni a cose per includere i danni ai dati
- Le esclusioni si concentrano su attacchi mirati, ma non tengono conto di eventi indiscriminati
- Le esclusioni si concentrano su eventi maligni piuttosto che sul potenziale danno accidentale
- Esclusioni guerra hanno lo scopo di impedire che le perdite dello stato nazionale siano indifendibili in tribunale
- Attacchi di negazione dell'accesso non sufficientemente trattati
- Disconnessione tra la definizione di un evento cibernetico e l'esclusione cibernetica

Esclusioni trattati		Cat	Risk
"E-risks" in conformità con le disposizioni delle polizze originali		Sì	Sì
Dati (senza danni fisici)		No	No
DDoS		Sì	Sì
Attacchi alle terze parti		Sì	Sì
Danni / interruzioni accidentali		No	Sì
Esclusione guerra		No	No
Conseguenza di danni fisici	Interruzione d'attività	Sì	Sì
	Dati	Sì	Sì

Vista la complessità del processo di valutazione dei wording, si ritiene che le attuali soluzioni InsureTech possano essere un valido strumento di supporto

Fase 3: lo sviluppo degli scenari per la copertura Silent Risk - RMS

RMS CYBER SCENARIOS

CAMS 1.0

Affirmative Cover (IT)



Infiltrazione Dati
Leakomania



Negazione di Accesso
Mass DDoS



Errore del Provider dei Servizi Cloud
Compromissione del Cloud



Furto Cyber
Furto finanziario



Ransomware
Estorsioni – virus riscatto

CAMS 2.0

Silent Exposure (OT)



Cyber Attacco alle **Centrali Elettriche USA**
*Blackout * v1.1*



Cyber Attacco alle **Centrali Elettriche UK**
*Infrastrutture Integrate * v1.1*



Cyber Attacco ad **Edifici Commerciali**
Induzione di incendi tramite le batterie dei laptop



Cyber Attacco ai **Porti marittimi**
Sistema di gestione portuale



Cyber Attacco alle **Industrie Chimiche**
Attacco ICS



Cyber Attacco alle **Piattaforme Petroliere**
Scatenare Esplosioni



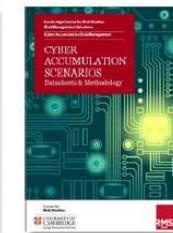
Sybil
Logic Bomb



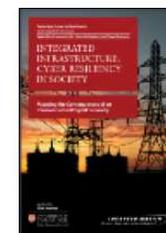
US Cyber
Blackout



Exposure Data
Schema



Accumulation
Scenarios



UK Cyber
Blackout



Cyber
Terrorism

Fase 3: lo sviluppo degli scenari per la copertura Silent Risk

Scenario	Rami Coinvolti
Ransomware (virus di riscatto) di massa	Molteplici (p.e. Cyber, Property ed Elettronica, D&O)
Attacchi per sistemi di automazione degli edifici	Property, RC Generale
Sforamento diga	Molteplici (Property, Infortuni, D&O, RC Generale)
Controllo mezzi di trasporto	Property, Elettronica, Infortuni ed RC Generale
Controlli industriali / di produzione	Property, Elettronica ed RC Generale
Violazione dei dati di massa	Cyber
Blackout Europeo	Molteplici (Property ed Elettronica, D&O, Infortuni, Marine, Aviazione ed RC Generale)
Attacco contro i passeggeri di un aereo	Aviazione ed RC Generale
Attacco navigazione marittima (AIS e GPS)	Marine ed RC Generale
Attacco alla gestione del carico	Marine
Attacco DDoS su piattaforme di trading finanziario per creare guadagni finanziari	Cyber
Transazioni fraudolente che sfruttano l'infrastruttura centralizzata	Cyber
Manipolazione di Mercato	Cyber
Fallimento credenziali accidentali	Property e Cyber
Manipolazione processo di fabbricazione	RC Generale

Selezione degli scenari adeguati: come approcciare i mercati Riassicurativi

Esempio calcolo dei sinistri legati alle reali esposizioni agli scenari

Scenario	Danni a cose	Interruzione attività	D&O	Ripristino dopo evento
Attacco contro serre industriali	€352m	€234m	€32m	€0m
Attacco Blackout contro Tokyo	€56m	€6,302m	€230m	€100m
Attacco monitoraggio trasporto merci	€0m	€400m	€150m	€0m
Attacco contro la rete ferroviaria	€150m	€203m	€0m	€0m
Furto finanziario di massa	€0m	€0m	€0m	€0m

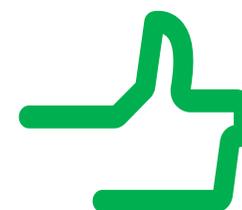
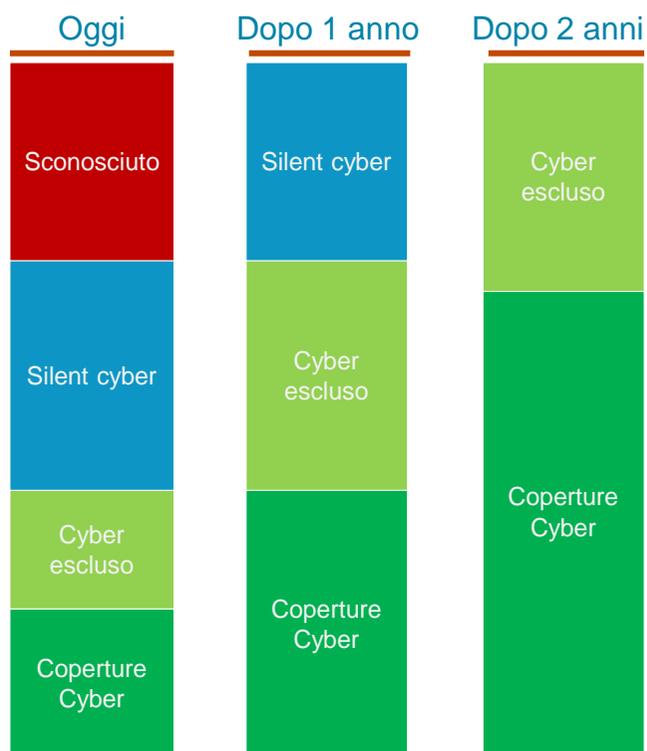
La parametrizzazione di ogni singolo scenario e i relativi sinistri attesi consentono ai riassicuratori di comprendere e stimare meglio l'esposizione di ogni singola compagnia



Il lavoro sugli scenari permette ai Riassicuratori di avere una visione più completa e soprattutto analitica del rischio

Fase 4: una strategia a lungo termine per il trasferimento del Cyber Risk

Piano a lungo termine per sottoscrivere il cyber risk, o escluderlo

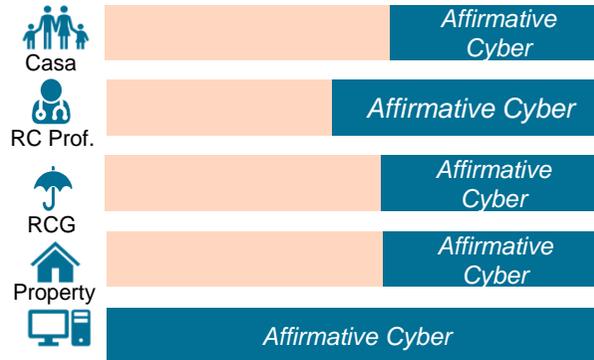


Perfezionare la strategia da adottare per il futuro, e a trasferire tale messaggio ai mercati riassicurativi.

In questo modo sarà possibile affinare le soluzioni riassicurative in linea con i progressi ottenuti di volta in volta, seguendo la strategia pianificata

Fase 5: coperture Riassicurative Cyber - benchmarking

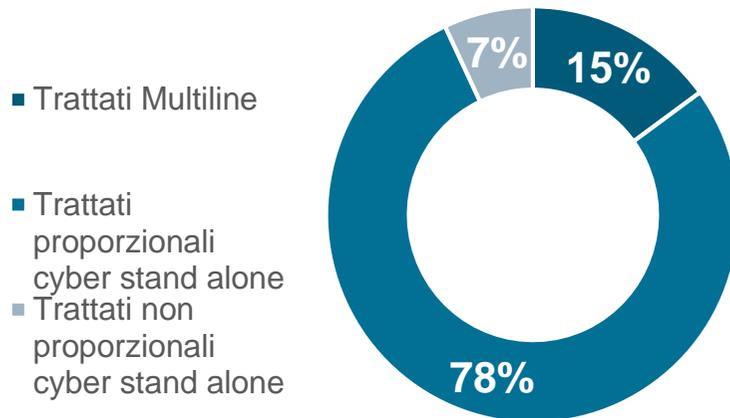
Obiettivo è quantificare le esposizioni al Silent Cyber e sviluppare una strategia per eliminarla o coprirla, in base alle esigenze del cliente.



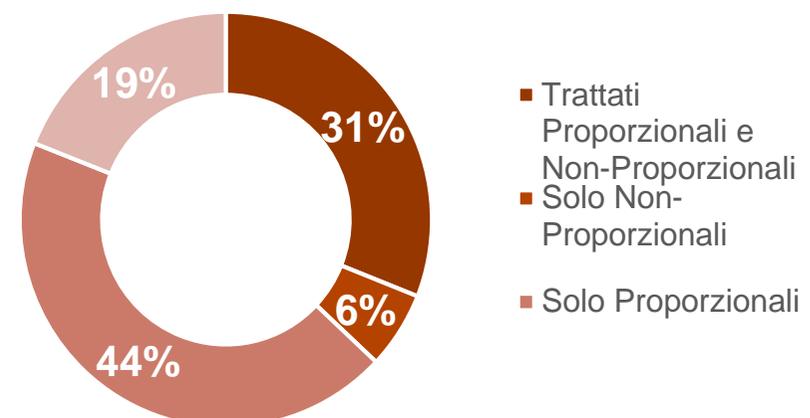
Strutture riassicurative flessibili (es. Q/S, Aggregate XL, Stop Loss ...)

La risposta del mondo riassicurativo:
«una maggiore certezza nelle esposizioni si dovrebbe tradurre in una più ampia flessibilità e maggior efficienza delle coperture disponibili»

Premi Ceduti per tipologia di trattato



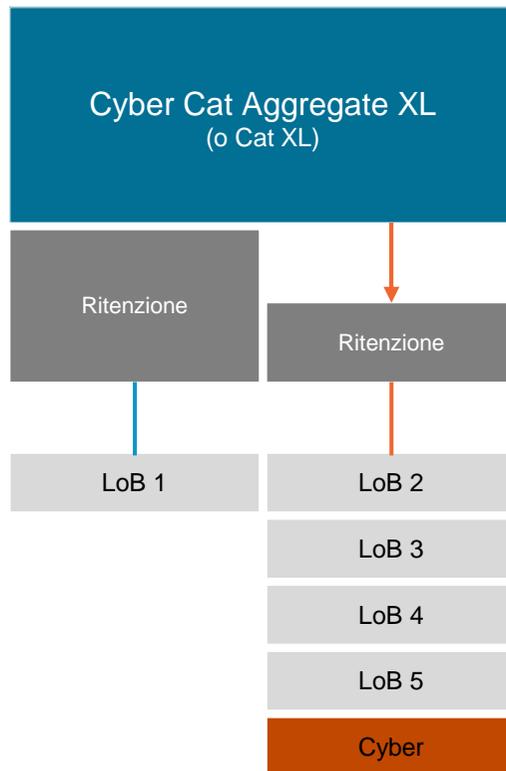
Tipologia di coperture riassicurative



Fonte: Aon Reinsurance data

Fase 6: esempi e caratteristiche delle coperture riassicurative

Caratteristiche coperture riassicurative



Aggregate XL

- Strutturato sul ritenuto delle coperture di riassicurazione esistenti permette di coprire anche il rischio sistemico
- **Punto di attacco:** dipende dalla “cyber tolerance” di ogni singola compagnia che prediligerà evitare sorprese in caso del sinistro di punta, o piuttosto coprire un numero definite di perdite?
- **Costo della capacità: RoL** mediamente **tra 5-10%** in funzione delle coperture sottostanti e delle misure di controllo poste in essere per mappare il rischio cyber
- Il costo è stimato al netto dei premi ceduti alle altre coperture riassicurative

Altri esempi di coperture

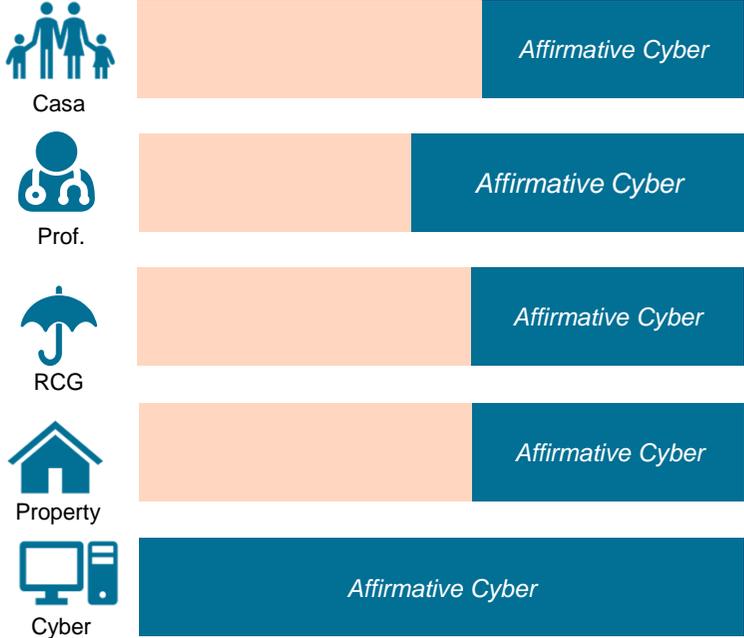
Quota share

- Termini e condizioni dipendono fortemente dal volume premi ceduti
- La presenza di un cap di copertura (abbastanza frequente) dipende dalla natura delle esposizioni sottostanti
- Le commissioni riconosciute copriranno i costi originali più un’eventuale una “profit commission”

XL

- Copre le punte salvaguardando i risultati di bilancio a fronte di un singolo sinistro importante che colpisca ad esempio l’aggregate XL, mantenendo però bassi livelli di redditività del capitale
- Il costo è frutto del profilo di rischio sottostante

Fase 7: soluzioni per *l'affirmative cyber* per i rami tradizionali



Una maggiore sicurezza e trasparenza in merito alle esposizioni cyber sottostanti porterà ad un aumento della capacità riassicurativa



Ciò si tradurrà anche in una riduzione dei prezzi di riassicurazione, mentre cresce la raccolta premi originale associata al Cyber

La struttura finale potrebbe essere uno Stop Loss (Aggr. XL) che copra le esposizioni *Affirmative Cyber* in tutti i portafogli presenti



In futuro il rischio Cyber sarà sottoscritto e valutato in modo appropriato per tutti i rami che compongono il portafoglio della compagnia. Ciò ridurrà l'incertezza e consentirà la strutturazione di forme riassicurative più efficienti.

GIANPIERO MUCCILLO



GRAZIE!

Domande?