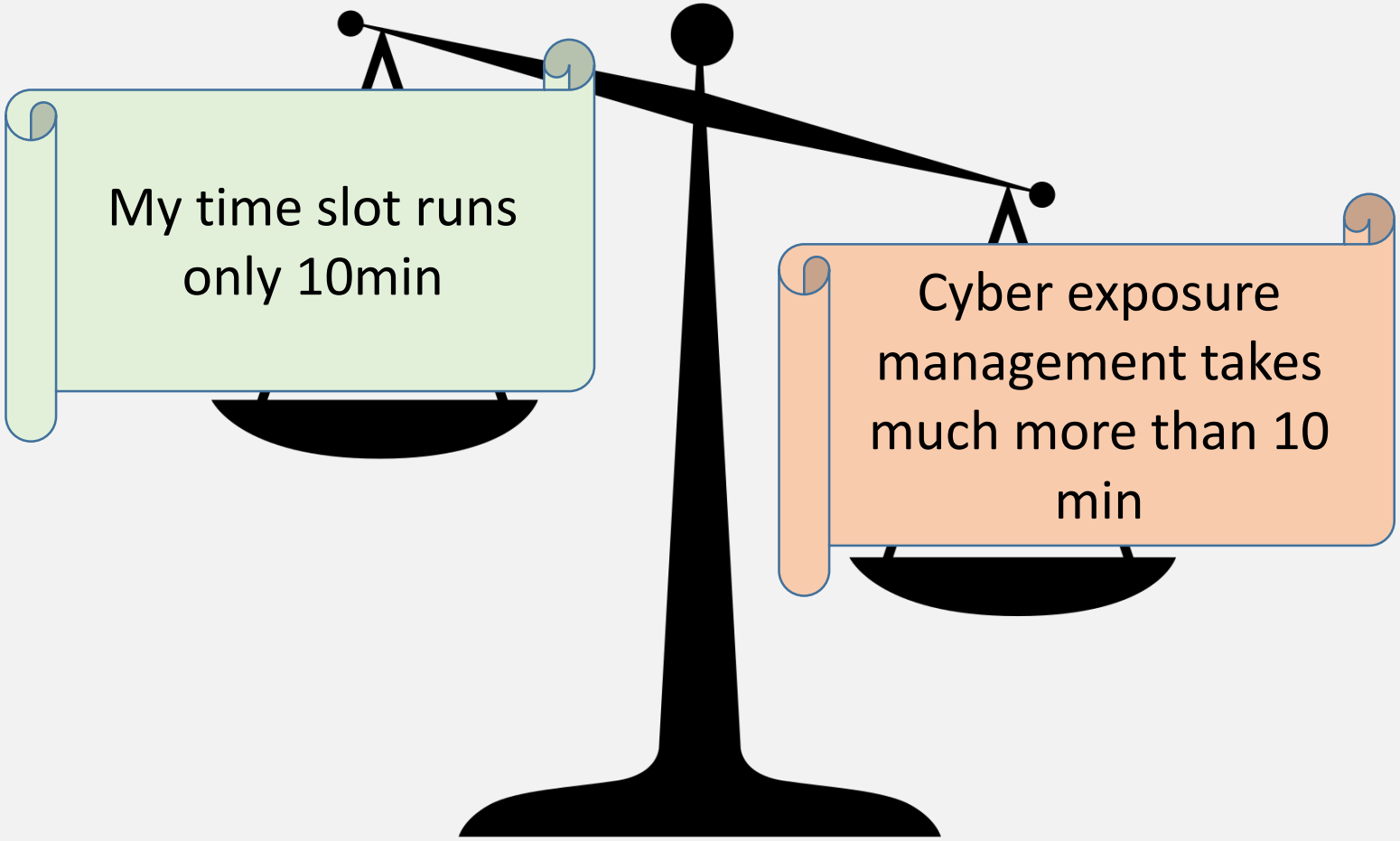
Cyber Exposure Management

September 10th, 2020 at 2020 ISCM Zurich virtual networking event:

Cyber accumulation risk - simply "another cat peril" or fundamentally different?

Hans-Joachim Guenther, PeriStrat® LLC

Good news… bad news

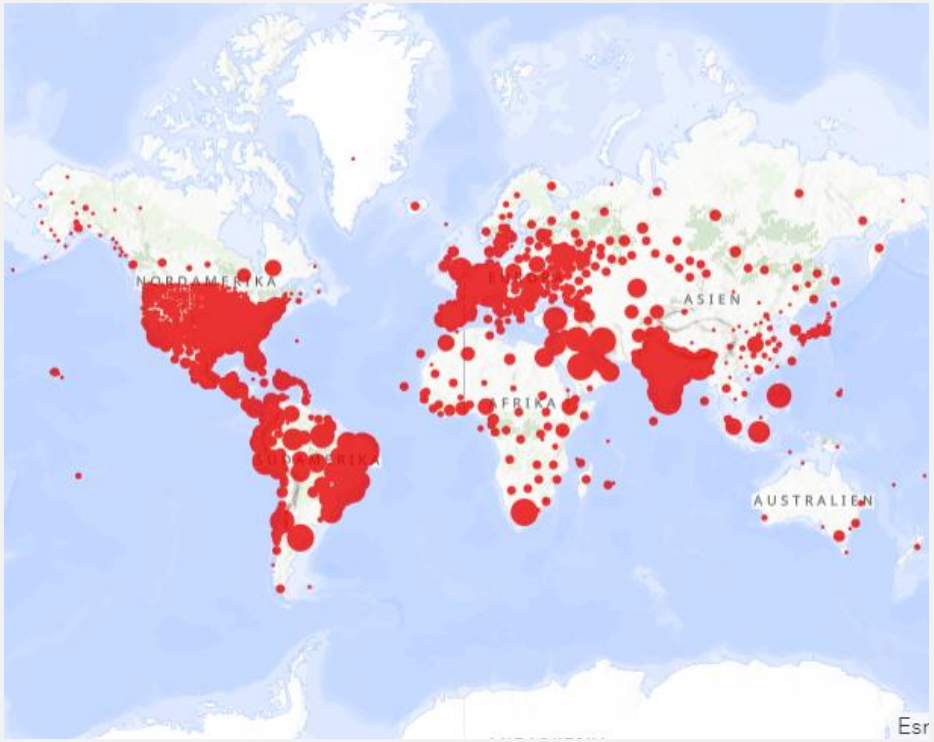


Cyber is fundamentally different…

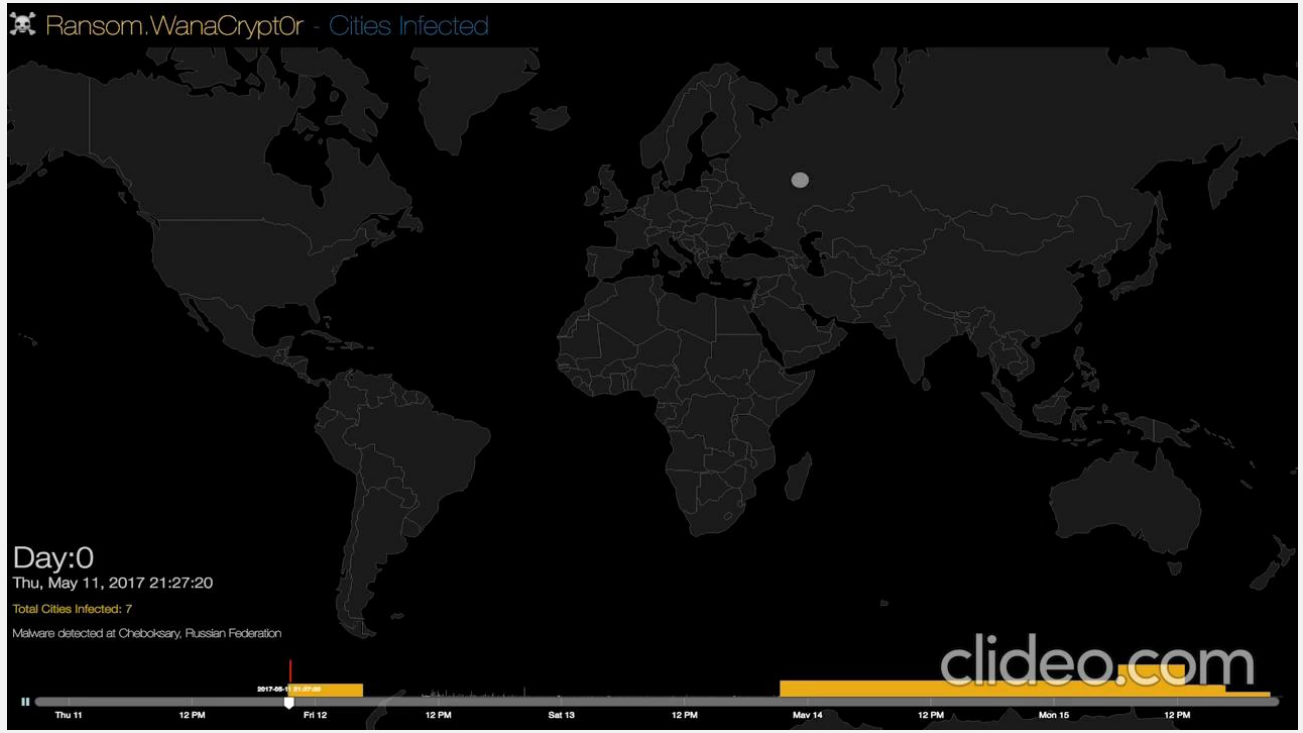
Man made

- Critical threat to individuals, business, nations
- Highly contagious
- Dynamically changing
- Difficult to contractually frame
- Already partially covered under various policies
- Criminal motivation
- Part of non kinetic war

Medical vs. IT viruses



Source: Covid-19 Spread, John Hopkins University as per September 2020



Source: YouTube, WannaCry Ransomware Infection Heat Map

Health Care vs. IT Sector

- The pattern appears to be very similar!
- Could health care pandemic risk management measures be utilized?

There is incubation time allowing for decision taking time

- No, an **IT virus spreads within hours compared to weeks for medical virus**

Close borders, check travelers, etc.

- No, **data travel is too big, too fast and global** compared with human mobility

Containment, quarantine

- Effected units can be unplugged to contain the virus in a machine or network and stop spreading.
- Effectiveness of this measure **depends on how fast the virus spreads and how quickly action is t**aken. Velocity of virus attacks require almost immediate action which is unlikely to happen fast enough.

Killer switch

- It **might exist for an IT virus**

Cyber Exposure Clusters

Silent vs. Affirmative

Silent	Affirmative
Cyber unintentionally covered due to wording ambiguities… Does data represent a physical asset… often unclear… Privacy breach covered in GL unless explicitly excluded	Contractually agreed coverage
Surprise factor? Like Titanic hitting the iceberg	Limited surprise factor; potential surprise about future cyber loss scenarios which were not assessed when coverage was designed affirmatively
Highly contagious across full spectrum of LoB written	Contagious due to accumulation risk in one event
unpriced	priced
Not supported by working capital	Working capital allocation
Normally no coverage for cyber specific extra expenses, however potentially full exposure to CBI and BI limits	Specific coverage for cyber extra expenses at defined limits

First vs. Third Party

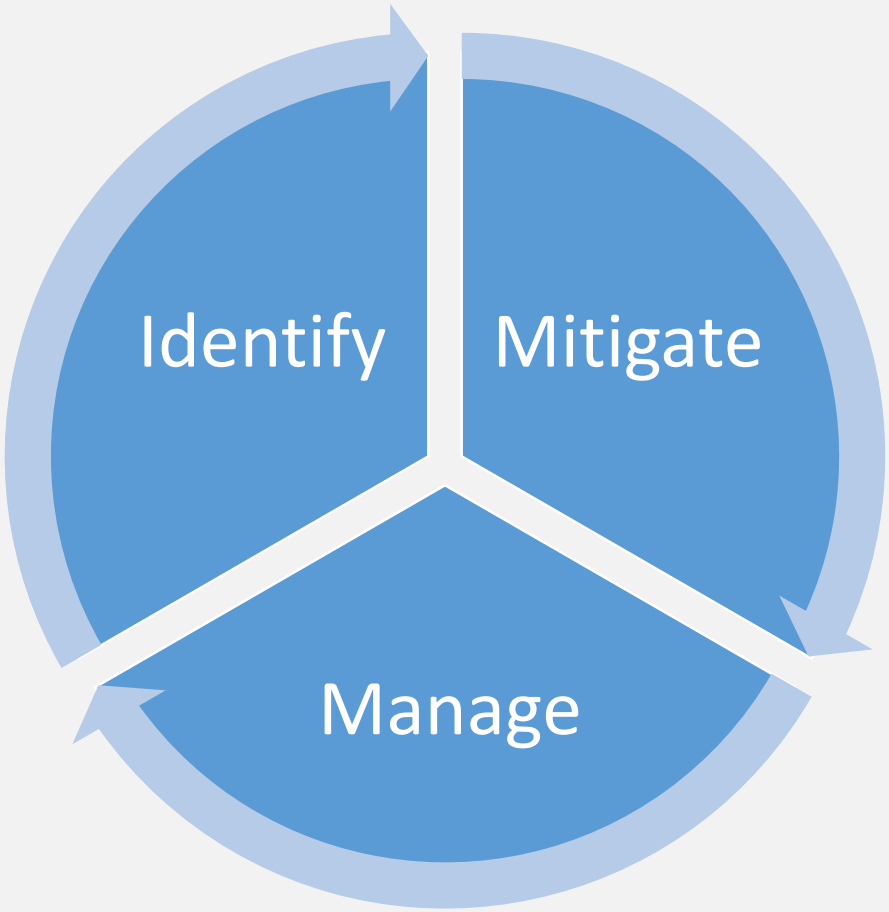
First	Third
Property damage	Physical damage
Loss of earning (BI, CBI, additional expenses)	Bodily injury
Specific expenses	Financial loss
• Legal advice	• Network liability
• Notification cost	• Privacy breach
• Forensic investigation	• Penalties due to authorities, customers (GDPR,…)
• System restoration	• D&O, E&O
• Ransom payment	

The insured interests are broad.

Type of attack

Type	Background	Motivation	Who	Impact
Single target attack	• Typically IP theft or data theft or ransom • Exposure depends by data value (high value attracts attacks)	• Espionage • Theft • Ransom	• Single hacker group and state sponsored • Mostly single hacker group	• Classic portfolio diversification principles still hold • However diversification by region isn't of the same relevance as in other LoBs due to the cross-border/ global nature of cyber attacks
Multiple target attack	• Typical stealth approach • Multiple systems at different sites and/ or different service providers working in the same value chain of the targeted organization are attacked to obtain unauthorized access	• Espionage • Theft • Ransom	• Single hacker group and state sponsored • Mostly single hacker group	
Hyper target attack	• Typical state sponsored attack • Widespread infection across entire economy targeted to maximize GDP impact and potentially destabilize countries	• Destruction • non-kinetic war	• Mostly state sponsored	• Portfolio diversification heavily impaired • Increased risk of insolvencies due to heavy dependence between individual insured risks

How to Manage Cyber Risk?



Standard approach…

You can only mitigate and manage risk you properly identified and understood first!

Priorities…

Its not pricing which matters most but tail risk identification to understand capital at risk and chance for insolvency!

Identification

Wording

- Proper identification requires wording assessment and profound knowledge about relevant clauses and their impact if combined

Insured Interests

- Matching insured interests with coverage available identifies vulnerability of given policy

Scenario

- Rather than testing policies against a broad number of stereotype scenarios beforementioned steps allow for choosing the most relevant scenarios to identify the tail risk

Limit at risk

- Identification process allows for computation of full notional limit at risk

Mitigation

De-Leverage

- Exit business with high contribution of notional cyber exposure and no other business with positive margin linked to undesired cyber exposure

Wording

- Identify wordings with highest contribution of notional cyber exposure and negotiate wording improvement or exit

Move to affirmative

- Push silent exposures to become affirmative, e.g. explicitly include exposure for additional price in existing policies

Management

Tail Risk

- Use undiversified notional exposure and analogies from other LoBs to pitch an initial capital at risk
- Manage increased working capital vis-à-vis rating capital requirements and approved company risk appetite

PML

- Use selection of relevant scenarios, incident data and expert judgement call to arrive at insured claims frequencies, use severity from existing LOBs adjusted by expected exhaustion of limits at risk

Pricing

- For the time being cyber risk management will be scenario based and therefore technically of limited value for a full actuarial pricing
- However use cost of capital for capital at risk as benchmark plus loading as minimum price

UW

- Use knowledge about wording and clauses to avoid adding new silent exposure and to improve wording certainty
- Seek proactively mix of industries, territories and limit sizes to support diversification even though it might be very limited

Key Issues going forward

- Fast adoption of cyber risk trends in risk management
- Bridging the gap between cyber incident records and insured claims
- Access inside-out data to verify transmission mechanism between cyber incident and insured claim
- Record incurred claims data and use at best in the modelling value chain, but don’t believe any extrapolation from claims will deliver an outlook for the future
- Monitor coverage design and resulting exposures against changing threat landscape
- Insurability of state sponsored cyber attacks

Speaker’s short bio

Hans-Joachim Guenther graduated at Cologne University in economics and moved into insurance and reinsurance. So far, he spent more than 30 years in the risk taking and risk managing space.

Before setting up PeriStrat LLC in Zurich in 2015 he worked for Gerling Global Reinsurance in Cologne and Zug, Converium in Zurich and Endurance in Zurich at senior executive level. Since 2015 he spent almost 3 years as interim manager in Singapore driving Asia Capital Reinsurance’s turn-around of their business. In his career he covered European and Asian markets across all non-life lines of business and developed a distinct understanding of a truly global industry. He created and managed teams from different cultural backgrounds and build a strong and diverse personal network across the industry.

Currently he is independent Non-Executive Director at Humboldt Re advising a large Swiss Pension Fund and Argo Managing Agency Limited as well as consulting a young technology company specialized in predictive maintenance and working on risk management approaches for cyber exposures.

Contact data:

PeriStrat LLC (also PeriStrat GmbH) Forsterstrasse 76 CH-8044 Zürich Switzerland	+41 (44) 253 25 56 (t) +41 (44) 253 25 57 (f) message@peristrat.com www.peristrat.com