Cyber Risks
Threats – Trends – Mitigation

Nuremberg, 21st May 2019

Heidi A. Strauß, Dr. Michael Spreitzenbarth

Munich RE

Agenda

1. Introduction
2. Why is Cyber important?
3. Cyber business value chain
4. Future threats and trends

History of Munich Re


Image: Munich Re / Marcus Buck

1880

Munich Re is founded on 19 April 1880 at the instigation of Carl von Thieme, Baron Theodor von Cramer-Klett and Wilhelm Finck.


Image: Corbis

1906

First major loss in the 20th century: The earth-quake in San Francisco on 18 April 1906. Munich Re's liability: US$ 2.5m.

Munich Re deals with all aspects of claims on the spot.


Image: ERGO Versicherungsgruppe

1997

The insurance groups VICTORIA/D.A.S. and Hamburg-Mannheimer/DKV announce that they will merge under the name of ERGO Versicherungsgruppe AG.

ERGO, which belongs to Munich Re, is now represented in more than 30 countries.


Image: used under license from shutterstock.com

2010

New brand strategy in primary insurance: Direct insurer KarstadtQuelle Versicherungen is now trading under the ERGO Direkt brand. Over the course of the year, the Hamburg-Mannheimer and Victoria brands are also subsumed into the ERGO brand.

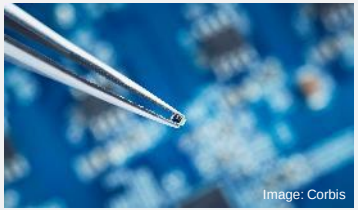


Image: Corbis

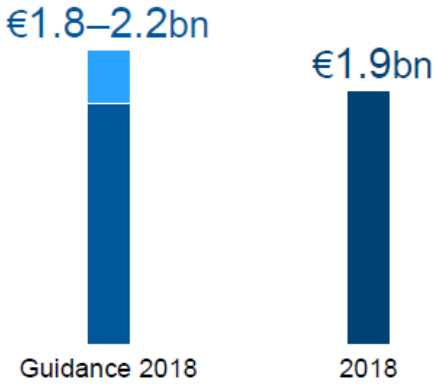
2015

Digitalisation and Big Data are changing the world. The new risk insurance field of reinsurance is part of that change and is currently developing innovative solutions for new risks and cover requirements.

Key figures 2018

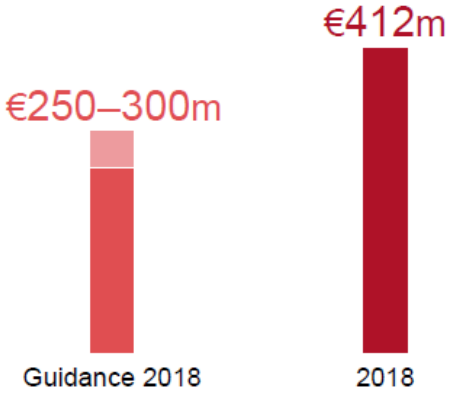
Munich RE

REINSURANCE
NET RESULT



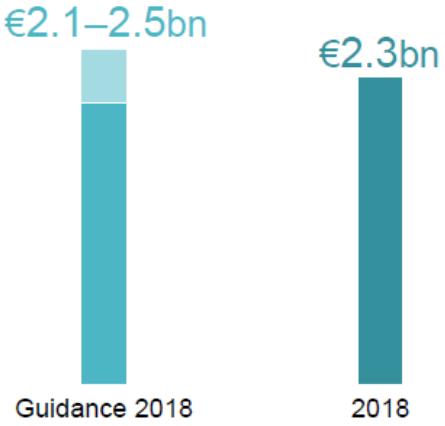
Profitable growth in P-C, technical performance at L&H above expectations

ERGO
NET RESULT



Strong earnings contribution, even when adjusted for one-offs

GROUP
NET RESULT



Return on equity 8.4% – Good start to the 2020 ambition

Note: Figures as at 31.12.2017 (31.12.2016).

Digital transformation offers new opportunities for reinsurers

Munich RE

Traditional Reinsurance

Effectively serving our clients and strengthening the business model

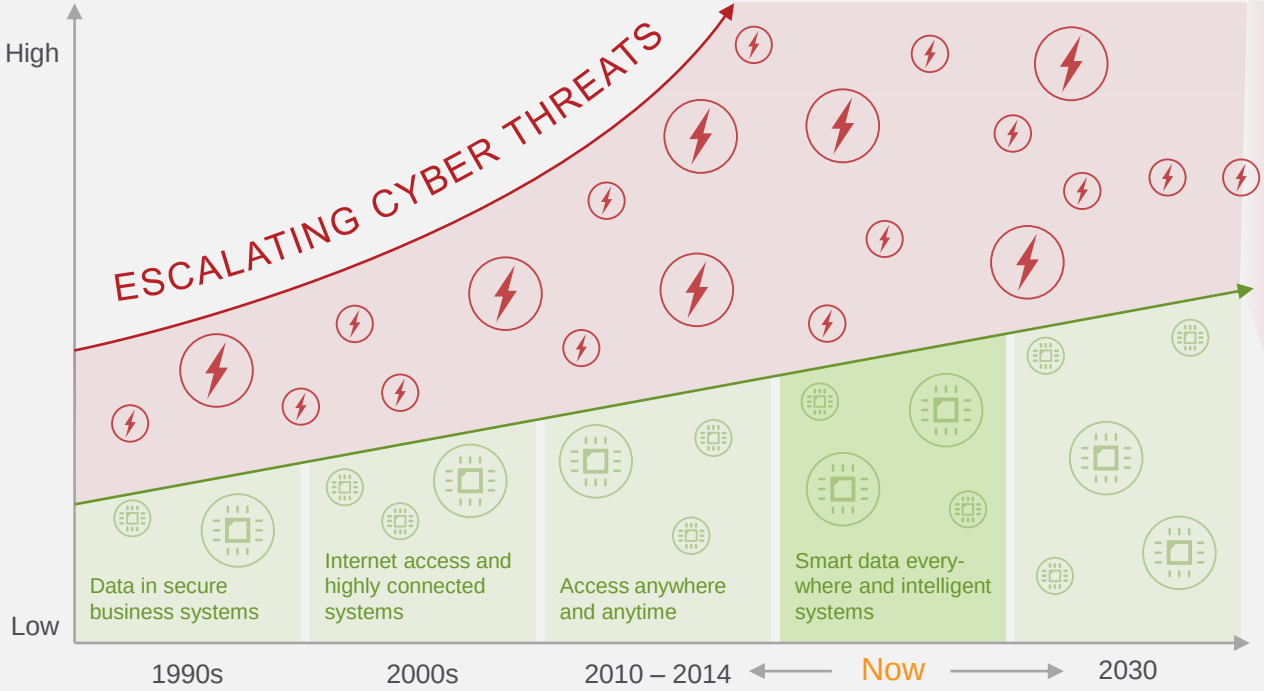
Risk Solutions

Reinforcing underlying profitability and growth

New strategic options

Building a diversified profit base

Cyber risks constitute one of the greatest threats we face



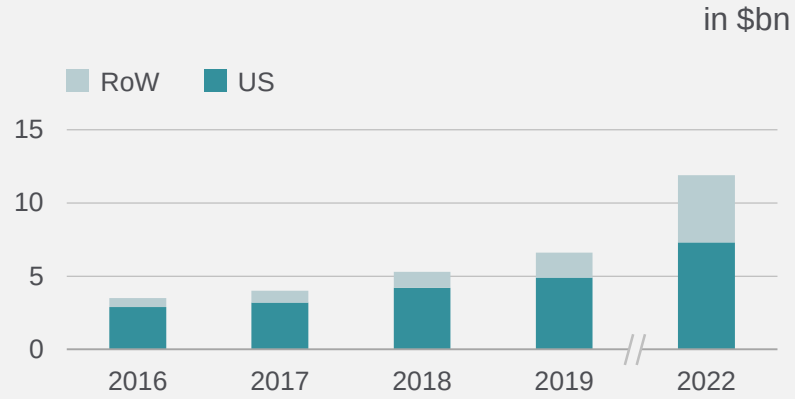
- Hackers
- Malware
- Cyber crime
- Data breach
- Identity theft
- Cyber warfare
- Insecure codes
- Cyber terrorism
- Network attacks
- Critical infrastructure attacks
- Foreign state sponsored cyber espionage

http://bwcio.businessworld.in/article/125-Billion-Connected-IoT-Devices-by-2030/26-10-2017-129552/
http://pardee.du.edu/sites/default/files/Cyber%20Risk%20Pardee%20Extended%20Report..pdf
http://publications.atlanticcouncil.org/cyberrisks//

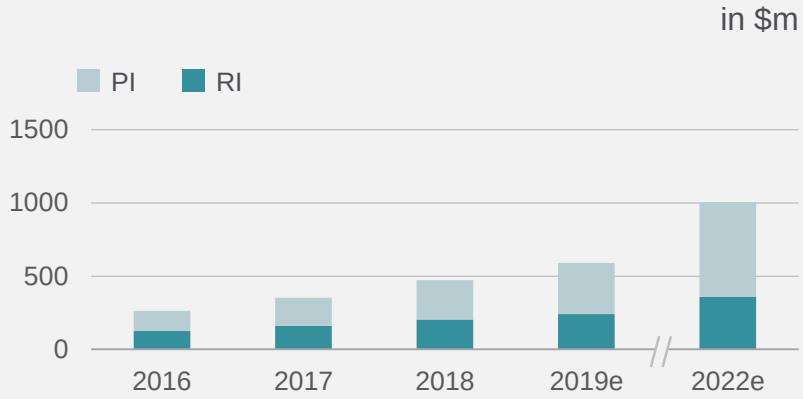
Strong long-term growth in cyber (re)insurance expected

Munich Re with leading-edge expertise and market presence

GWP global cyber insurance market[1]



GWP Munich Re cyber portfolio



REINSURANCE: First mover and global market leader

- Dynamic growth through joint projects with cedents
- Steady growth in the US, accelerated growth in Europe
- Strong accumulation models, increased expert headcount
- Network with external cyber service providers further extended (underwriting, data, claims services for cedents/insureds)

PRIMARY INSURANCE: Specialised single-risk taker

- Hartford Steam Boiler: Established player in US for SMEs and individuals
- Corporate Insurance Partner: Focus on larger corporate clients – Cooperation with IT providers and Beazley

[1] Munich Re estimates

2 Importance of Cyber

Example: Amazon S3 Outage

Event background

- Amazon Web Services (“AWS”) is the world’s largest cloud infrastructure provider.
- In February 2017, Amazon’s “S3” (‘Simple Storage Solution’) service suffered a widespread outage.
- For over 4 hours, all services dependent on AWS infrastructure in Northern Virginia were unavailable.
- The outage was caused by human error as one of Amazon’s engineers inadvertently took down all servers in the region.
- Analytics firm Cyence suggested that S&P500 companies lost $150m, and financial services firms lost $160m.

Image: Hamza TArkkol / Getty Images

Image: Science Photo Library / Getty Images

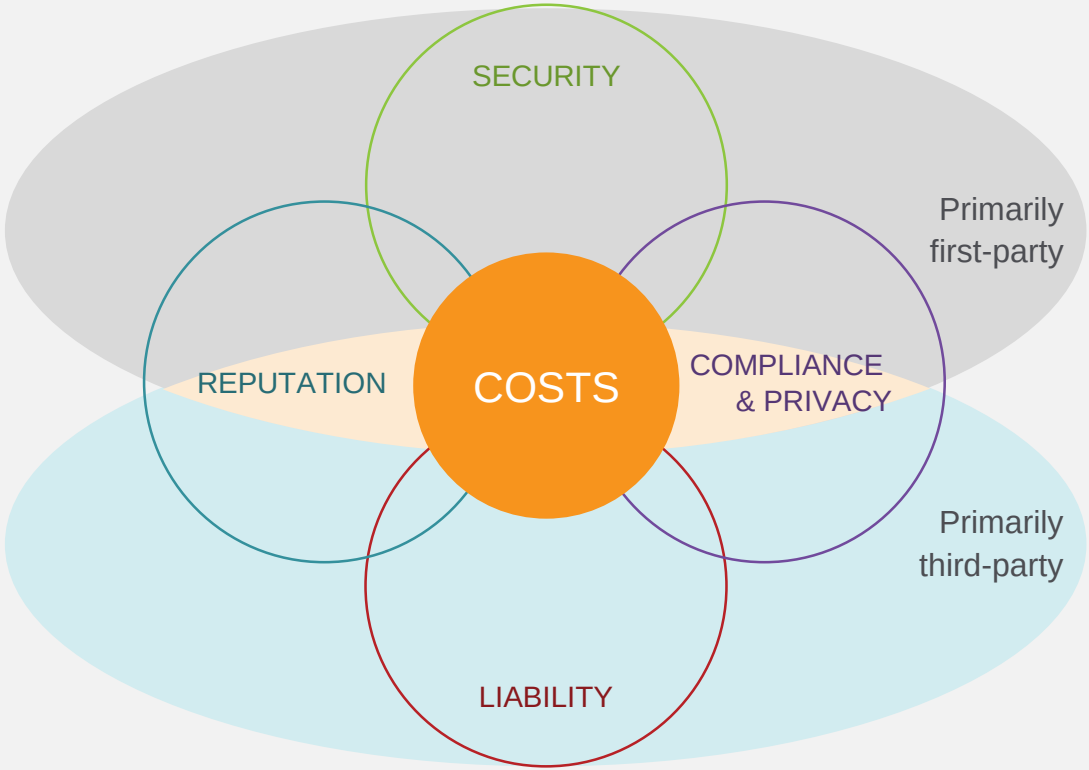
Image: Mischa Keijser / Getty Images

Accumulation insights

This incident fits within the event definition of the Munich Re “IT service provider outage” scenario, which assumes widespread (contingent) business interruption losses.

Dimensions of cyber risks

- Denial of service
- Extortion
- Electronic vandalism
- Theft of data
- Computer virus



- Privacy laws
- EU directive
- HIPAA + HITECH
- Gramm-Leach-Bliley

- Loss of reputation after cyber incident
  - by third party
  - own fault
- Systematic posting of wrong information

- Intellectual property infringement
- Product/service failure
- Privacy violation

Possible costs after an incident

Munich RE

Impact on Business

- Data recovery
- System recovery
- System update to prevent future incidents
- Production interruption
- Forensic investigations
- Incident response
- Crisis mgmt.
- Redesign of critical infrastructure

Liability

- Losses (i.e., 3rd party revenue losses
- Notifications, call centre costs, postage
- Credit monitoring
- Identity restoration
- Infringement of trademarks

Legal implications

- Law suits (from vendors, customers, business partners)
- Legal advice
- Defence costs
- Fines and penalties
- Class action litigation

Miscellaneous

- Loss of revenue
- Loss of contracts
- Reputational damage
- Share price impact
- Reduced sales
- Future sales impact
- Extortion payments
- Public relations costs
- Devaluation of intellectual property

Preparation and professional consulting significantly decreases costs

Cyber (re-)insurance outlook

Significant expansion of coverage types

Munich RE

Already in the market

Loss or theft of data

Data is destroyed or stolen; covered in private, commercial and industrial lines of business

Privacy breach protection

Consumer data is stolen or lost, or non-compliance with privacy legislation by a company

Cyber extortion

Threat of loss or destruction of own or customer data

Property damage

First or third-party property damage as a consequence of a cyber event

(Contingent) Business interruption

Business interruption or contingent business interruption resulting from a cyber event

... first offerings

Product liability

Third-party property damage or bodily injury caused by software failure within a product

Reputational damage

Loss of profit resulting from reputational damage as a consequence of a cyber event

... not yet

Loss of intellectual property

Loss of profit as a consequence of stolen trade secrets, or other commercially sensitive information

Increasing exposure and complexity of coverages

Munich Re offers a fully fledged, market proven product with solutions for the whole value chain

Risk Assessment

Insurance policy

Pre-Incident Services

Post Incident Services

3 Cyber business value chain

Cyber scenario chain

A framework: From the technical incident to the insured consequence

Munich RE

Scenario party

Threat

Target

- → Industry: Automotive, … (exception: private households)
- → Market: USA, Germany, …
- → Company size: SME, Large

(Re-) Insurance

- → PI policy type: All risk, …
- → RI participation: Per Risk XL,QS, AggXL, CXL,…

Scenario step

Threat actor → Cyber threat → IT-components affected/ point-of entry → Consequence/ Economic loss → Insured interest affected → LoB/CoB affected

Possible characteristics

Threat actor	Cyber threat	IT-components affected/ point-of entry	Consequence/ Economic loss	Insured interest affected	LoB/CoB affected
▪ Government ▪ Teenager ▪ Terrorist ▪ Rogue Employee ▪ IT-Freak ▪ Competitor ▪ Activist Group	▪ Hacker attack ▪ Malware (Virus, Worm) ▪ Social Engineering (Phishing, USB Drop) ▪ Cyber Extortion (Ransomware, …) ▪ DDoS ▪ Disclosure of data	▪ Server outage ▪ Network outage ▪ Firewall bypass ▪ Loss of control of software ▪ Software manipulation ▪ Hardware manipulation	▪ Physical losses/damages (MB, fire, …) ▪ Non-physical losses/damages (loss of data, non-availability of systems, service or supply chain interruption, reputational loss, data breach) ▪ Business interruption ▪ Additional costs (data restorage, information cost, …) ▪ Bodily injury	▪ Property Damage (PD) ▪ BI/CBI ▪ BI (non-damage) ▪ Machinery breakdown ▪ Pure data loss ▪ Bodily injury ▪ Third party PD ▪ Third party financial loss ▪ Cyber Police: Privacy Breach, BI, …	▪ Property: Fire ▪ Property: Engineering ▪ Property: Other ▪ Casualty: General Liab. ▪ Casualty: Prof. Indemn. ▪ Casualty: MedMal ▪ Casualty: Financial lines ▪ Casualty: Motor ▪ Casualty: PA ▪ Cyber ▪ Marine ▪ Aviation
▪ (Accidental)	▪ Security failure (general) ▪ System failure ▪ Program failure ▪ Human error				

Key question

Motivation for cyber attack	Technical tool utilized for attack	The technical consequence	The economical consequence	Triggered insurance coverage/claim	Business line affected

Cyber risk management on UW level

Cyber risk management on UW level

Risk assessment: Incident resilience

Munich RE

Risk assessment | Pricing | Wording | Loss monitoring

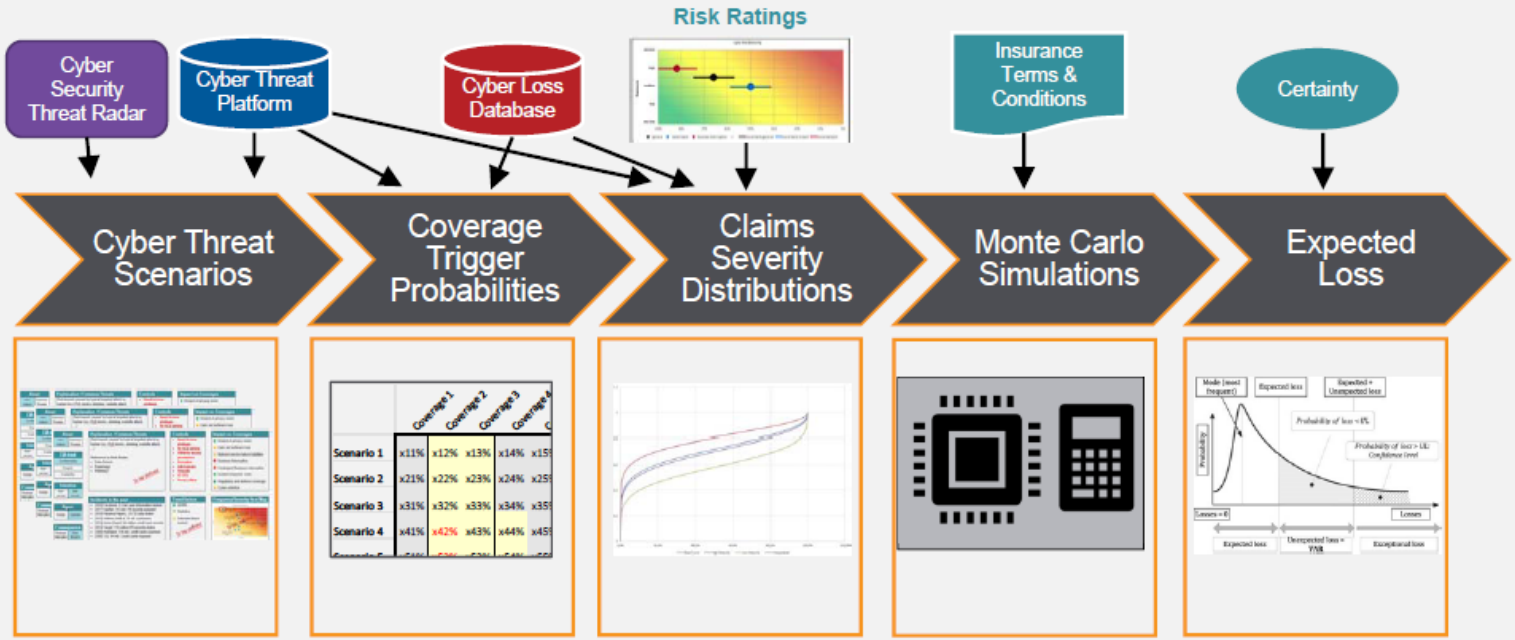
1. Organization
2. Information security governance and compliance
3. Inventory and classification of assets
4. IT system hardening and encryption
5. Patch management
6. Malware protection
7. Application security
8. Network security
9. Access control
10. Risk assessment, incident management, disaster recovery and business continuity
11. Awareness

Cyber Threat Scenarios – Introduction

Cyber Pricing (in a nutshell)

Munich RE

Risk assessment | Pricing | Wording | Loss monitoring



Source: Cambridge Cyber Exposure Data Schema

Cyber risk management on UW level

Wording

Risk assessment | Pricing | **Wording** | Loss monitoring

… still differ a lot, depending on market, company, jurisdiction …

Source: CRO Forum – Cyber Working Group

Cyber risk management on UW level

Loss monitoring

Risk assessment | Pricing | Wording | Loss monitoring

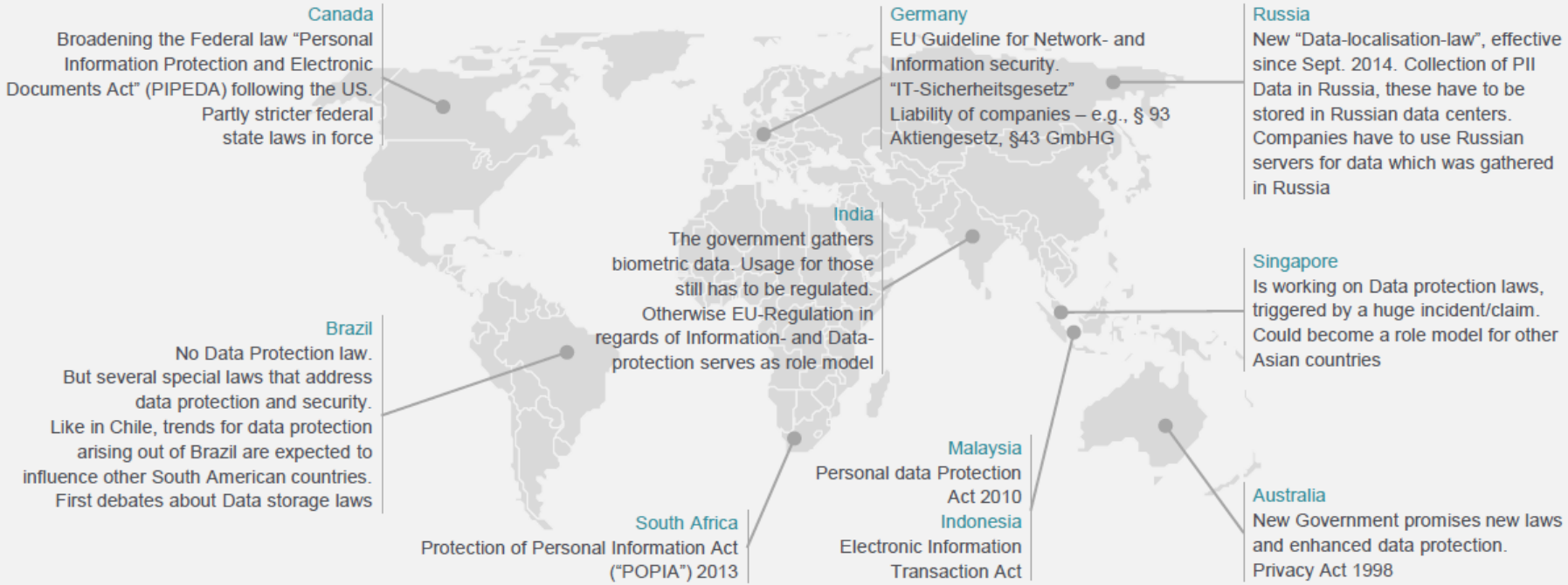
THE GENEVA ASSOCIATION

Project **CIDER**:
Cyber Incident Data Exchange Repository

Source: CRO Forum – Cyber Working Group

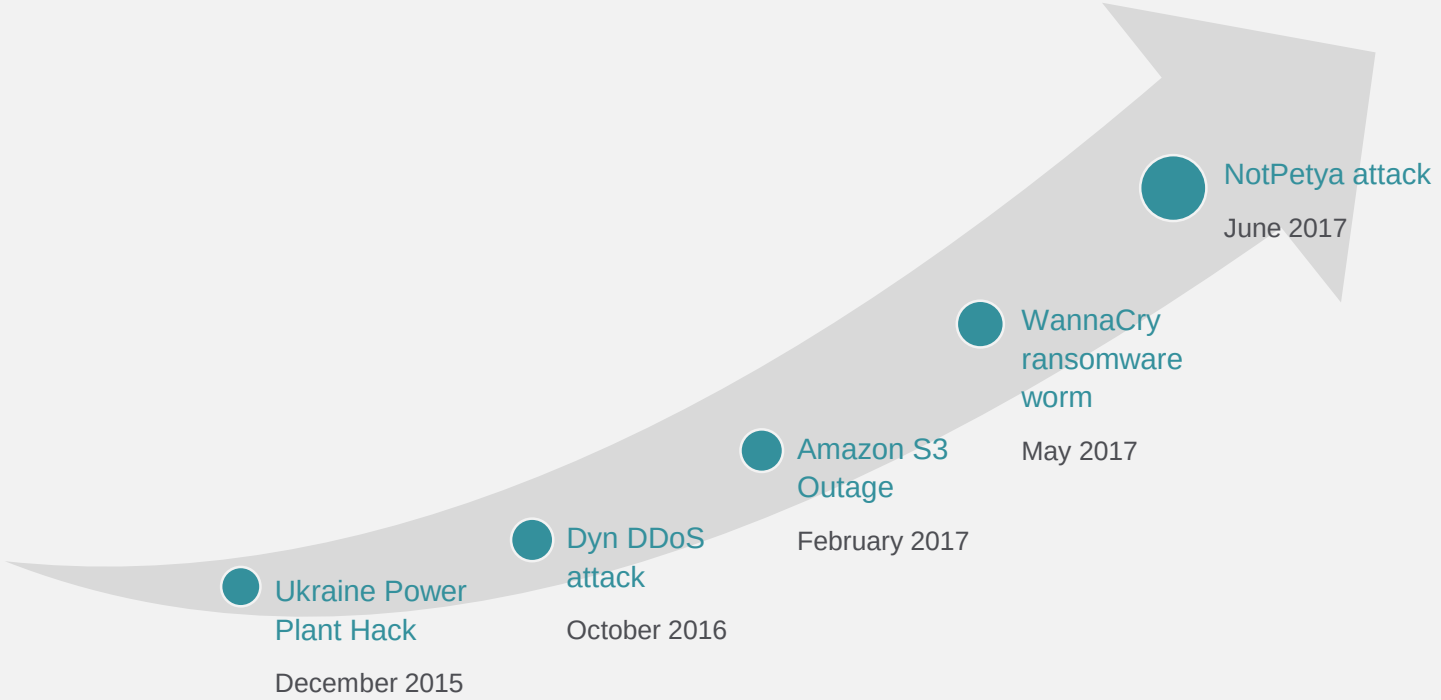
A major driver, changing constantly

Regulatory requirements

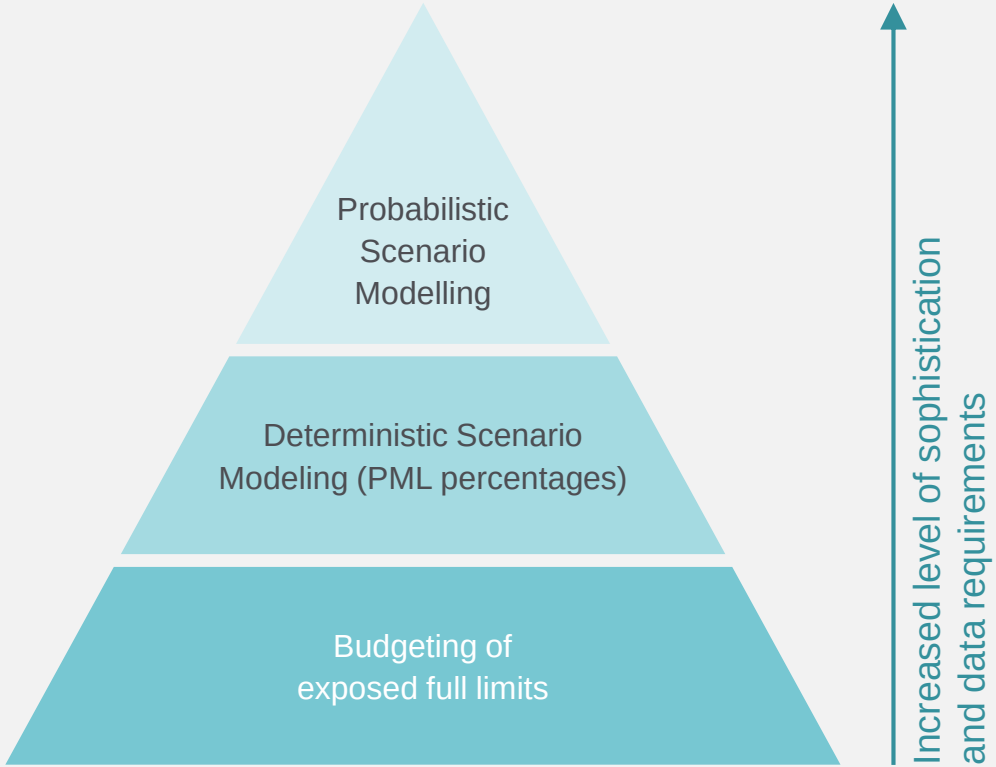


Source: SFKI 2011, Wikipedia, Siemens

Cyber Accumulation Event Timeline



Quantification approaches for cyber accumulations



General principles:

- Budgeting of full limits if no limiting feature exists or in case of non-availability of individual portfolio data
- Top-down estimate as an initial benchmark
- Probabilistic modelling ultimate goal but most challenging due to
  - Lack of loss history
  - Dynamic threat environment

Cyber risk

Quantifying accumulation exposure at Munich Re

1. We identify “single points of failure” that could result in widespread impact (business interruption and/or data breach losses), across thousands of businesses all at once
2. Munich Re develops and maintains its own frequency/severity PML models to quantify the most “extreme but plausible” (re)insurance losses it could face, from these threats.
3. These models use a Monte Carlo simulation approach, developed by mathematicians and actuaries working alongside cyber security specialists and cyber underwriters.
4. We are also in discussions with or license the leading cyber accumulation model vendors (RMS, Cyence, CyberCube and AIR), as well as other outside researchers, and refer to these outside views to help validate our own models.

Ransomware worm: NotPetya

Cyber accumulation model vendors

CYENCE

CyberCube

RMS

AIR WORLDWIDE
A VERISK ANALYTICS BUSINESS

State of the art risk management as true business enabler

Accumulation

Virus & Malware

Data breach

IT Service provider outage

Outage of external networks

Transparency – Do we write cyber?

- Almost every conventional non-life policy can be exposed to cyber risk
- Silent Cyber exposure is potentially significant, but it presents also a nearly untapped area of business opportunities

Action required

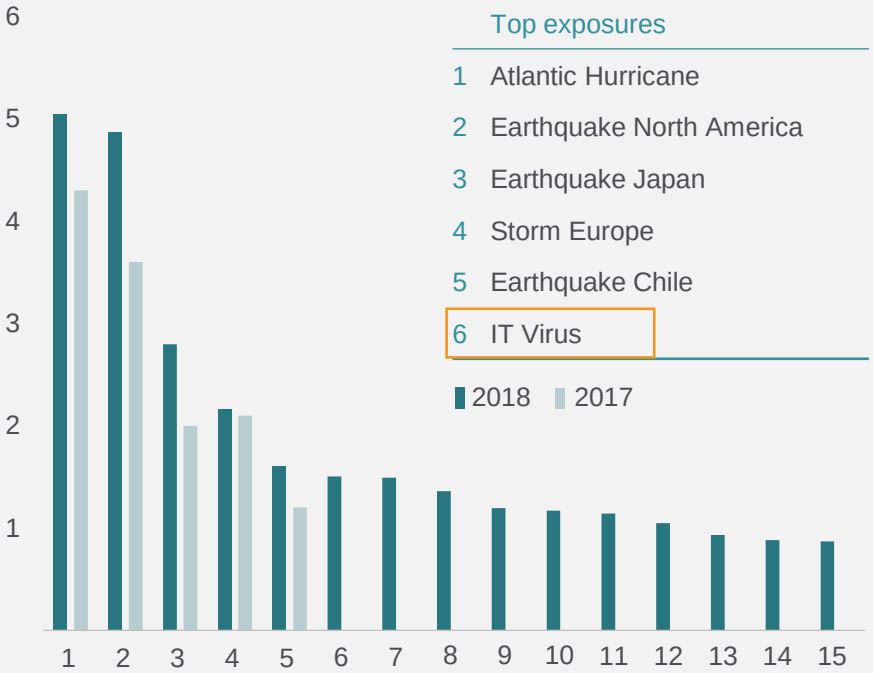
- Achieve transparency of the inherent exposure
- Turn the silent coverage into at least non-silent or even better affirmative coverage
- Risk assessment and pricing
- Accumulation control

Our biggest risk is the "strategic risk not to find any insurance solution for cyber".

Insurance risks are driven more by cyber:

Property-casualty risks

Top scenario exposures (net of retrocession) – AggVaR[1] €bn



SCR property-casualty €bn

	2018	2017
Basic losses	4.0	3.4
Major losses[2]	7.1	5.7
Diversification	-3.5	-2.8
Total	7.6	6.3

- Basic losses: Portfolio growth and material model update
- Major losses: Substantial growth as well in RI nat cat exposure in the course of 2018
- IT Virus: explicit reflection in the Group Internal Risk Model in 2018

1 Munich Re (Group). Return period 200 years, pre-tax. 2 Natural catastrophes, man-made (including terrorism and casualty accumulations) and major single losses.

Asses possible Cyber Risk exposure

Munich RE

Security and business continuity

- Asset analysis: critical systems/data
- Threat analysis: internal – external
- Cloud and outsourcing
- Crisis management
- Press and media
- Risk awareness

Underwriting and portfolio management

- Underwriting guidelines (exclusion clauses)
- Cyber loss scenarios
- Accumulation/ budget control
- Loss monitoring
- Product development

Cyber insurance

- Perform cyber risk assessment
- Transfer individual cyber exposure
- Pre-view and select professional advisor

Compliance and globalisation

- Compliance radar
- Check business partners/ service level agreements
- Legal protection (contractual penalties)
- Lobbying for global standards, co-operation,…

4 Future threats and trends

Cyber threats to be observed

Munich RE

=> Cyber-future

Connected critical infrastructure: concern for governments and societies (cyber terror/war)

Digital systems can cause human deaths (smart home/vehicles: volocopter)

Criminal cyber syndicates resembled to powerful multinational organisations

IT companies gain monopolistic power of information (e.g., Google, Amazon, Facebook, Apple)

Widely distributed and homogenous or old technologies increase (systemic) risks

New kinds of cyber risks emerge unexpectedly and develop fast:
From “Alexa” and ransomware to artificial intelligence and the singularity

Images: dpa Picture Alliance
Source: ISF Threat Horizon Report 2017

Thank you for your attention!

Heidi A. Strauß 

Dr. Michael Spreitzenbarth 

Munich RE