Cyber Risks
Threats – Trends – Mitigation

Nuremberg, 21st May 2019
Heidi A. Strauß, Dr. Michael Spreitzenbarth
Agenda

1. Introduction
2. Why is Cyber important?
3. Cyber business value chain
4. Future threats and trends
1880
Munich Re is founded on 19 April 1880 at the instigation of Carl von Thieme, Baron Theodor von Cramer-Klett and Wilhelm Finck.

1906
First major loss in the 20th century: The earthquake 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.

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.

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.

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.

Image: Munich Re / Marcus Buck
Image: Corbis
Image: ERGO Versicherungsgruppe
Image: Corbis
Image: Corbis
Image: Munich Re / Marcus Buck
Image: used under license from shutterstock.com
Image: Corbis
Key figures 2018

**REINSURANCE**
NET RESULT

€1.8–2.2bn
Guidance 2018

€1.9bn
2018

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

**ERGO**
NET RESULT

€250–300m
Guidance 2018

€412m
2018

Strong earnings contribution, even when adjusted for one-offs

**GROUP**
NET RESULT

€2.1–2.5bn
Guidance 2018

€2.3bn
2018

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

Digital transformation offers new opportunities for reinsurers

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

CREATING NEW STRATEGIC OPTIONS
- Reshuffling the value chain
- Expanding the boundaries of insurability
- Data-driven solutions

GROWTH AND EXCELLENCE

AI trends

Trends

Cyber Risks

21 May 2019
Cyber risks constitute one of the greatest threats we face.

Global reinsurance landscape
**Strong long-term growth in cyber (re)insurance expected**

Munich Re with leading-edge expertise and market presence

### GWP global cyber insurance market

- **RoW**
- **US**

<table>
<thead>
<tr>
<th>Year</th>
<th>RoW</th>
<th>US</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>2</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>2017</td>
<td>4</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>2018</td>
<td>5</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>2019</td>
<td>6</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td>2022</td>
<td>7</td>
<td>7</td>
<td>14</td>
</tr>
</tbody>
</table>

### GWP Munich Re cyber portfolio

- **PI**
- **RI**

<table>
<thead>
<tr>
<th>Year</th>
<th>PI</th>
<th>RI</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>100</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>2017</td>
<td>150</td>
<td>150</td>
<td>300</td>
</tr>
<tr>
<td>2018</td>
<td>200</td>
<td>200</td>
<td>400</td>
</tr>
<tr>
<td>2019</td>
<td>250</td>
<td>250</td>
<td>500</td>
</tr>
<tr>
<td>2022</td>
<td>300</td>
<td>300</td>
<td>600</td>
</tr>
</tbody>
</table>

---

**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
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.

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

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

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

- Intellectual property infringement
- Product/service failure
- Privacy violation
## Possible costs after an incident

**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’s cyber strategy

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

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

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

Already in the market

... first offerings

... not yet

Increasing exposure and complexity of coverages
Munich Re offers a fully fledged, market proven product with solutions for the whole value chain.
Cyber business value chain
**Cyber scenario chain**
A framework: From the technical incident to the insured consequence

- **Scenario party**
  - Government
  - Teenager
  - Terrorist
  - Rogue Employee
  - IT-Freak
  - Competitor
  - Activist Group

- **Scenario step**
  - Threat actor
  - Cyber threat
  - IT-components affected/
    point-of entry
  - Consequence/
    Economic loss

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

- **Target**
  - Industry
  - Market
  - Company size

- **(Re-) Insurance**
  - PI policy type
  - RI participation

- **Possible characteristics**
  - 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, …

- **Triggered insurance**
  - Property: Fire
  - Property: Engineering
  - Property: Other
  - Casualty: General Liab.
  - Casualty: Prof. Indemn.
  - Casualty: MedMal
  - Casualty: Financial lines
  - Casualty: Motor
  - Casualty: PA
  - Cyber
  - Marine
  - Aviation

- **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

- Risk assessment
- Pricing
- Wording
- Loss monitoring
Cyber risk management on UW level
Risk assessment: Incident resilience

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)

Risk assessment
Pricing
Worded
Loss monitoring

Cyber Security Threat Radar
Cyber Threat Platform
Cyber Loss Database

Risk Ratings

Insurance Terms & Conditions
Certainty

Cyber Threat Scenarios
Coverage Trigger Probabilities
Claims Severity Distributions
Monte Carlo Simulations
Expected Loss

Source: Cambridge Cyber Exposure Data Schema
… still differ a lot, depending on market, company, jurisdiction …
Cyber risk management on UW level

- Loss monitoring
- Risk assessment
- Pricing
- Wording

Source: CRO Forum – Cyber Working Group

Project **CIDER**: Cyber Incident Data Exchange Repository
A major driver, changing constantly

Regulatory requirements

Canada
- Broadening the Federal law "Personal Information Protection and Electronic Documents Act" (PIPEDA) following the US. Partly stricter federal state laws in force

Germany
- EU Guideline for Network- and Information security "IT-Sicherheitsgesetz"
- Liability of companies – e.g., § 93 Aktiengesetz, §43 GmbHG

Russia
- New "Data-localisation-law", effective since Sept. 2014. Collection of PII Data in Russia, these have to be stored in Russian data centers. Companies have to use Russian servers for data which was gathered in Russia

India
- The government gathers biometric data. Usage for those still has to be regulated. Otherwise EU-Regulation in regards of information- and Data-protection serves as role model

Brazil
- No Data Protection law. But several special laws that address data protection and security. Like in Chile, trends for data protection arising out of Brazil are expected to influence other South American countries. First debates about Data storage laws

South Africa
- Protection of Personal Information Act ("POPIA") 2013

Australia

Malaysia
- Personal data Protection Act 2010

Indonesia
- Electronic Information Transaction Act

Source: SFKI 2011, Wikipedia, Siemens
Cyber Accumulation Event Timeline

- Ukraine Power Plant Hack, December 2015
- Dyn DDoS attack, October 2016
- Amazon S3 Outage, February 2017
- WannaCry ransomware worm, May 2017
- NotPetya attack, June 2017
Quantification approaches for cyber accumulations

Increased level of sophistication and data requirements

Budgeting of exposed full limits

Deterministic Scenario Modeling (PML percentages)

Probabilistic Scenario Modelling

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
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.
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”.

Accumulation

<table>
<thead>
<tr>
<th>Virus &amp; Malware</th>
<th>Data breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Service provider outage</td>
<td>Outage of external networks</td>
</tr>
</tbody>
</table>
Insurance risks are driven more by cyber: 
Property-casualty risks

Top scenario exposures (net of retrocession) – AggVaR¹ €bn

<table>
<thead>
<tr>
<th>Top exposures</th>
<th>2018</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Atlantic Hurricane</td>
<td>4.0</td>
<td>3.4</td>
</tr>
<tr>
<td>2 Earthquake North America</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Earthquake Japan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Storm Europe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Earthquake Chile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 IT Virus</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SCR property-casualty €bn

- 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.

Munich RE
Asses possible Cyber Risk exposure

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

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

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

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

21 May 2019
Cyber Risks
Future threats and trends
Cyber threats to be observed

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
Thank you for your attention!

Heidi A. Strauß

Dr. Michael Spreitzenbarth

© 2019 Münchener Rückversicherungs-Gesellschaft © 2019 Munich Reinsurance Company