The 12th Geneva Association Annual Liability Regimes Conference

Session 2: Cyber Risks and Accumulation Issues

Munich, 17-18 November 2016
Maya Bundt
(Session Chair)
Head Cyber &
Digital Strategy,
Reinsurance
Swiss Re

Michael Bartsch
co-founder of
'Swiss Cyber
Experts' and
board member
of the
'Zukunftsforum
Öffentliche
Sicherheit'

Christian Biener
Project Manager
& Postdoctoral
Researcher
Institute of
Insurance
Economics (I.VW)
University of
St. Gallen

Eric Schuh
Head, Casualty
Centre Swiss Re
Accumulation
What ever that means in cyber?
Cyber in numbers: The Big Bang Theory

- **50/50** “There are only two types of companies: those that have been hacked, and those that will be.” Robert Mueller, FBI Director, 2012
- **51bn €** financial loss in 2015 through cybercrime and cyber espionage in Germany, Bitkom Report on Economic Security
- **100mio** lines of code in Windows 10 with Office 365 locally installed on each computer.
  - counting in all other applications: 250mio - 10bn lines of code on your computer.
- **7.73bn** mobile phones Statista 2016
- **3,425bn** direct internet connections Statista 2016
- **3,4·10^{38}** IPv6 addresses (340 Sextillion)
- **1998** IPv6 specification was designed and published as RFC2460

How much cybercrime was out there 18 years ago?
Insurances demand Risk Management

- Enterprise of 50,000 employees operates around 50,000 different applications, 100,000 Computers and Servers without peripherals and without SCADA and ICS-systems ➔ 1mio known attack vectors

- Can you really do risk management for Cyber:
  - criminals (money)
  - organized crime organization (more money)
  - states (espionage)
  - former employee – now he is mostly unfriendly (Revenge)
  - supplier (advantage, revenge)
  - competitor (advantage)
  - do gooder, do better, starry-eyed idealist (Attention)

Risk Management will always be affected by criminal intention!
Can you insure against cyber criminals?

An effective Cyberattack will misuse:

- Bugs in software and hardware
- Zero-day-exploits
- Configuration mistakes
- Or an unaware employee
- Or your entire (not well prepared) organization

**Imbalance:**
A company has to protect against ALL vulnerabilities but the criminal needs only ONE attack vector.
How to ensure Cybersecurity against these threats?

States:
- Around 70 States already developed cyber strategies (ENISA)
- EU- NIS Directive, German IT-Security Law, Regulation, cooperation models
  - Mandatory Notification for Critical Infrastructure and Digital Service Providers
  - Risk Management 😊
  - CERT (Incident Handling, Threats and Vulnerabilities, Information Exchange)
  - Crises Management
- NATO declared Cyber under Article 5 (collective defence)

Companies including SMEs:
- ???
Challenges:

• No one is owner of the internet - Attribution is quite difficult and nearly impossible.

• The complexity is to high:
  
  • We all use the internet everywhere, at home, on our mobile phone, at work, for fun, we do shopping, online banking, travel booking, mobile apps, etc.
  
  • The free services are paid by our data (data protection, who cares)

  • The rest we pay with an old fashioned credit card, prepaid cards, paypal, Apple Pay or with (digital) crypto-money (Bitcoin, Ether, etc.)

  • Have you ever heard about Ripple, DogeCoin, PeerCoin, LiteCoin, AuroraCoin and all the others?

  • States, banks and criminal organisations must be heavily involved – where is all the money - stolen through ransomware?

• Cyberattacks are a huge business case.

  Insurance companies have to insure someone against the business of another.
Questions I asked myself?

• Is Digitization itself an opportunity or a risk?
• Is a well known but insecure infrastructure insurable?
  **No CIO knows his infrastructure exactly!**
• Is cyber accumulation the end of the (insurance) food chain?
  **End of the day someone has to pay!**
• How can you do (accept) a risk assessment without knowing the real risks?
• How can you insure a company if you know that it will be easily attacked

**As a perpetrator I would see my new cyber-business-opportunity in attacking insurance companies.**

Either You pay me or I let you pay!
Thank you
for your
uninsurable attention!
....any more questions?

Michael Bartsch
Cybersecurity Expert
michael.bartsch@deutor.de
+49 171 324 3350
Cyber risk accumulation
Dr. Christian Biener
University of St. Gallen
Big risk and small insurance market: demand side frictions...

In 2015, only about 19% of US corporations had cyber coverage. “
Source: Aon & Ponemon, 2016

Reasons for small market...

“Exclusions”
“Limited coverage”
“High premiums”
“ Awareness”

GWP: Gross Written Premiums | Source: PWC, 2015
...caused by unresolved supply-driven insurability issues

- Limited product value…
  - “Exclusions”
  - “High Premiums”
  - “Limited Coverage”

- …because insurers are worried about tail risk

- Not observed – predictability
- Unknown correlations
- Maximum possible loss
- Moral hazard

[Diagram showing probability distribution with 95% VaR for “Normal” iid losses and “Extreme” non-iid losses]
Can we grasp cyber accumulation?

Addressing (some) actuarial issues
- Blending data (e.g., external data, data pool)
- Extreme value / threshold models
- Scenario analysis + exposure data
  - Backward-looking
  - Forward-looking (e.g., RMS / Cambridge)

Remaining issues
- Dynamic characteristics of underlying risk
- Arbitrariness of scenarios
- Scenario approaches have been shown to be inaccurate, e.g., in operational risk modeling

Ambiguity of tail distribution

Market development options
Increase capacity through collaboration:
- Data pool
- Insurance pool
- Alternative risk transfer (e.g., cyber cat bond)

Define the role of the government:
- Cyber risk management standards
- Reporting obligations
- Re-insurer of last resort for extreme losses
Cyber risk accumulation
Dr. Christian Biener
University of St. Gallen
The Challenges of Insuring New Technologies

Session 2 - Cyber Risk and Accumulation Issues

Annual Liability Regimes Conference- The Geneva Association
Munich 17th /18th November 2016
Topics

- **What** is the Insurance Industry doing in the so called ”cyber” space and **where** is/are the “cyber” Insurance product (s) directionally heading?

- **What** are the key threats, obstacles and **how** is the Industry currently managing those threats?

- **Is** there potential scope for Industry co-operation to improve risk quantification, improve liquidity in trading risk and deepen the market?
State of the Global Cyber Insurance market

Cyber /ˈsʌɪbə/ adjective: cyber relating to or characteristic of the culture of computers, information technology, and virtual reality "the cyber age“ Origin 1980s: abb. of cybernetics

- A beacon of growth for the industry but definitions are confusing
  - Cyber exposure embedded in most commercial lines of business - Passive
  - Current market focussed on loss of data, but morphing towards loss of control - Limited shift towards all lines cyber e.g. Ford Corp – Active

- Global Insurance market but overwhelmingly US-centric mirroring legal/statutory drivers
  - Circa $2bn DWP but anticipated to expand in size/geography as risk drivers evolve
  - Concentrated risk pools based on industry and size
  - Dominated by a handful of pioneering cyber writers

- To put this into context the Global cyber threat protection/consulting business is >30x $100bn
Prevailing dynamics, challenges and opportunities

- Underwriting results have (generally) been outstanding however, as market pivots towards *loss of control* prior results less meaningful

- Insurance buyers seeking/require broader protection for damage/ loss of digital assets/capability e.g. Business interruption, Contingent business interruption

- Nascent technical underwriting skills coupled with concerns about systemic accumulation, real-time mutation in underlying threats and fluid view on boundaries of coverage are constraining appetite and capacity in both primary and secondary markets

- Nature of risk inherently systemic but industry lacks both a coherent approach and a consistent framework for evaluating downside risk across the return period spectrum

- Some efforts by Third Party Vendor Model firms to provide limited scenario-based modelling support to their Insurance clients
Select aggregation perils

- **Digital**
  - Common vulnerabilities in cyber security programmes (or lack of)
  - Common shock vulnerabilities
  - Shared vendor/api infections leading to secondary/cascading cyber attacks across a shared network
  - Aggressive, calculated, maliciously motivated attacks on a series of linked companies
  - Malware infestation of shared data centre
  - Known common data software/patching failure leading to vulnerabilities
  - Malware infestation in internet provider services/nodes (data service centres, internet service centres and internet traffic satellites)

- **Physical**
  - Destruction of data service centres (explosion, fire, lightning, power outage etc.)
  - Destruction of internet cables (e.g. transoceanic submarine cables)
  - Destruction of internet service nodes (e.g. Crimean case study)

Andrew Coburn, director of the External Advisory Board of the University of Cambridge's Centre for Risk Studies - Based on a worst-case scenario, a series of unexplained information technology failures on “systemically important technology enterprises” (SITEs), such as Oracle Corp., International Business Machines Corp., Microsoft Corp., SAP AG/Sybase and Teradata Corp., could lead to a loss of $15 trillion in gross domestic output over five years, on a similar scale to the $18 trillion lost during the recent financial crisis.
Scope for improving market liquidity

- Modelling transformed Property Cat market - pre-hurricane Andrew, limited capacity but today multiple markets worldwide with increasing cross-over into wider capital markets, so **capacity per se** is not the issue

- Cyber represents extension to business interruption and CBI which Property Cat market able to cover provided it feels these risks are properly understood and underwritten

- Today’s market for cyber has similarities to pre-Andrew property cat market
  - AIR, RMS and other vendors racing to fill the modelling void, but not yet there
  - Challenge is harnessing data given the bewildering amount available in cyber-space, and need to create confidence that cyber aggregation can be quantified despite evolving nature of threats

- Once risks understood, models will gain credence and property cat roadmap suggests liquidity will follow