



Managing Risks of Cloud Computing Services: Risk Management Issues and Aspects Of Insurability

Presentation at the annual conference 2014 of the DVfVW

Stuttgart, Germany

Andreas Haas, University of Hohenheim

Prof. Dr. Annette Hofmann, HSBA Hamburg School of Business Administration



- 1. Background & Motivation**
2. Research questions
3. Key results
4. Further research and discussion

- The term '**Cloud Computing**' refers to an **outsourcing model** that enables on-demand access to the IT resources of data centers, with the potential to transform business landscapes
- IT resources become a **tradable good**, that is offered online...

standardized

fully automatic

on-demand

cost-efficient

nearly infinite

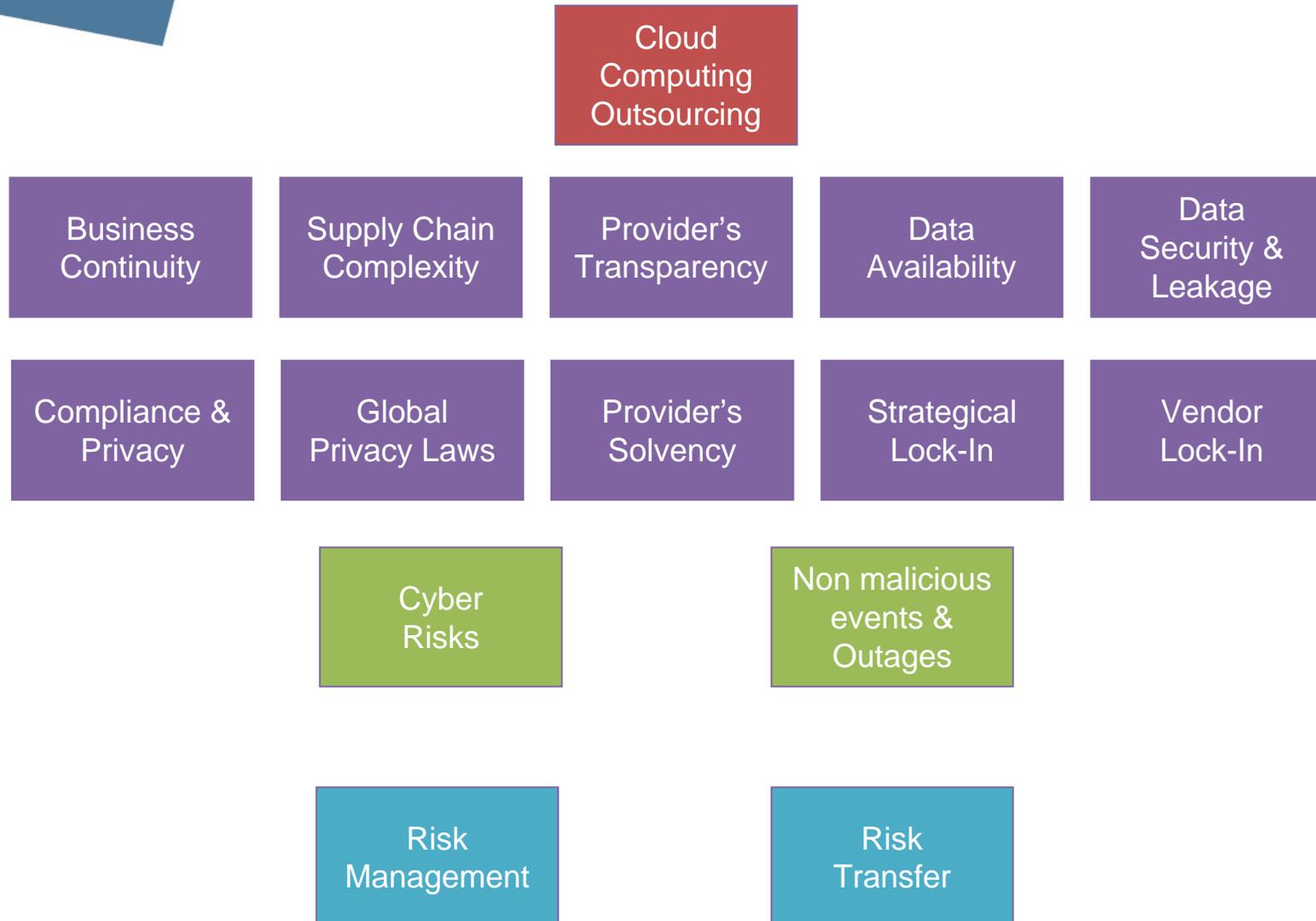
- Cloud Computing is used to replace complete in-house IT infrastructure and is the **enabling technology** for popular services like



- The **market volume** of cloud computing 2013 reaches **\$155 billion** worldwide with a CAGR of 17% in the next five years



Risk Context of Cloud Computing



- Datacenters of **reputable Cloud Providers** like Amazon or Google, accredited to ISO and industry standards, meet **higher security standards** than most other IT infrastructures of small- and medium businesses
 - (Public) Clouds are usually distributed **worldwide**, storing data **redundant** on several datacenters and being able to **deliver software** services to employees and users worldwide without any considerable delay
 - The (low) monthly usage fee on a **pay-per-use basis** - instead of high investments in own datacenters and its maintenance - may **reduce** the **financial risk** of a company
 - Flexible **(de)provisioning of cloud services** allows to respond faster to (un)predictable swings in the business's demand for IT resources, e.g. in case of new business opportunities, new business locations or providing IT for new business units or startups → can **reduce capital costs**
- Cloud Computing can be an important element of **(cyber) risk management**

- Recurring **outages** (and data losses) at Microsoft, Amazon and other cloud providers in the last years show that clouds are not perfect
 - Cloud Computing risks are a (sub-)category of **cyber risks** and can lead to loss of income, higher operating expenses, business interruptions, data loss, reputational loss or 3rd party liability
 - Cloud providers restrict their liability for **business interruptions** and **data loss** to a minimum by standardized Service Level Agreements (SLAs)
 - Surveys & market data show, that the willingness to store and process even **sensitive data** on these outsourced IT infrastructures rises
- ➔ Cloud Computing as a risk management approach should also involve managing the risks of cloud computing

	ACE	AIG	Allianz	AON	Chartis	Chubb	HDI Gerling	Hiscox	Zurich
Covered damages and losses	Data Protect	Cyber Edge	Cyber Protect	Risk Solution	Cyber Edge	Cyber Security	Cyber+	Data Risks	Cyber & Data Protect.
Data Theft or Extortion	Green	Green	Green	Green	Green	Green	Green	Green	Green
Business Interruption	Green	Orange	Green	Green	Green	Green	Green	Green	Green
Reputational Loss	Orange	Orange	Orange	Orange	Orange	Orange	Orange	Orange	Orange
Crisis Management	Red	Green	Green	Green	Red	Green	Green	Green	Green
Forensic Actions	Green	Green	Green	Green	Green	Green	Green	Green	Green
3 rd Party Liability	Red	Orange	Green	Green	Green	Green	Orange	Green	Green
3 rd Party Loss of Income	Red	Red	Orange	Orange	Red	Red	Orange	Red	Orange
Violation of Privacy (Laws)	Orange	Green	Red	Orange	Green	Red	Orange	Red	Orange
....

	ACE	AIG	Allianz	AON	Chartis	Chubb	HDI Gerling	Hiscox	Zurich
Covered damages and losses	Data Protect	Cyber Edge	Cyber Protect	Risk Solution	Cyber Edge	Cyber Security	Cyber+	Data Risks	Cyber & Data Protect.
Data Theft or Extortion	Green	Green	Green	Green	Green	Green	Green	Green	Green
Business Interruption	Green	Orange	Green	Green	Green	Green	Green	Green	Green
Reputational Loss	Orange	Orange	Orange	Orange	Orange	Orange	Orange	Orange	Orange
Crisis Management	Red	Green	Green	Green	Red	Green	Green	Green	Green
Forensic Actions	Green	Green	Green	Green	Green	Green	Green	Green	Green
3 rd Party Liability	Red	Orange	Green	Green	Green	Green	Orange	Green	Green
3 rd Party Loss of Income	Red	Red	Orange	Orange	Red	Red	Orange	Red	Orange
Violation of Privacy (Laws)	Orange	Green	Red	Orange	Green	Red	Orange	Red	Orange
....
Cloud coverage	Red	Red	Diagonal	Diagonal	Diagonal	Red	Red	Red	Diagonal



1. Background & Motivation
2. Research questions
3. Key results
4. Further research and discussion

Motivation

- Number of cyber attacks worldwide is **rising steadily**
- Cloud Computing is one of the most important IT trends, with a continuous growth
- The willingness to outsource even **sensitive data** to public cloud infrastructures rises, despite significant loss events
- We have to assume that currently **self insurance** is the main risk transfer instrument as cloud providers restrict their liability by SLAs and insurance products are lacking

Research questions

- (1) Why are risks out of cloud computing as a subcategory of cyber risks **not covered** by cyber insurance products?
- (2) What is the **impact** of cloud computing on the cyber insurance market?



1. **Background & Motivation**
2. **Research questions**
3. **Key results**
4. **Further research and discussion**

- The technical and legal risk landscape of cloud computing is **more differentiated** than of traditional IT outsourcing:
 - several legal frameworks affected, as worldwide distributed
 - standardized SLA in contrast to individual contract design
 - users share IT resources instead of dedicated server allocation
- The **required cooperation** between several cloud providers leads to a high risk **interdependency** and causing supply chains disruption in case of a malfunction
- Large Cloud Providers are an attractive target for hacker attacks
- Lacking opportunities for risk diversification as a change of the provider is currently not technically possible; strong lock-in-effects occur

The following criteria have to be fulfilled to make a risk insurable (Karten, 1972):

- **Randomness:** The occurrence of an insured event needs to be random
- **Unambiguousness:** Events have to be clear and distinct
- **Predictability:** The loss event needs to be predictable
- **Independence:** Insured risks need to be independent from each other
- **Possible maximum loss:** The maximum loss needs to be assessable

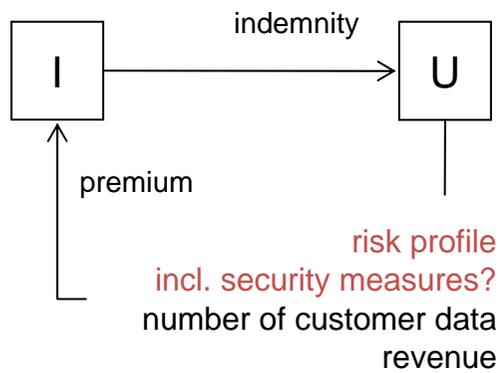
Independence

- The criterion independence of a potential damage is a major challenge for cloud portfolios
- Due to interdependent supply network structures, any service interruption or a deliberate malicious attack will affect a large number of individual risks simultaneously
- Risk accumulation is triggered by one company and a large number of clients is affected by one event, in case of a malfunction
- This **high risk of accumulation** is a new risk aspect for the (re-)insurance industry in terms of IT outsourcing and cyber risks

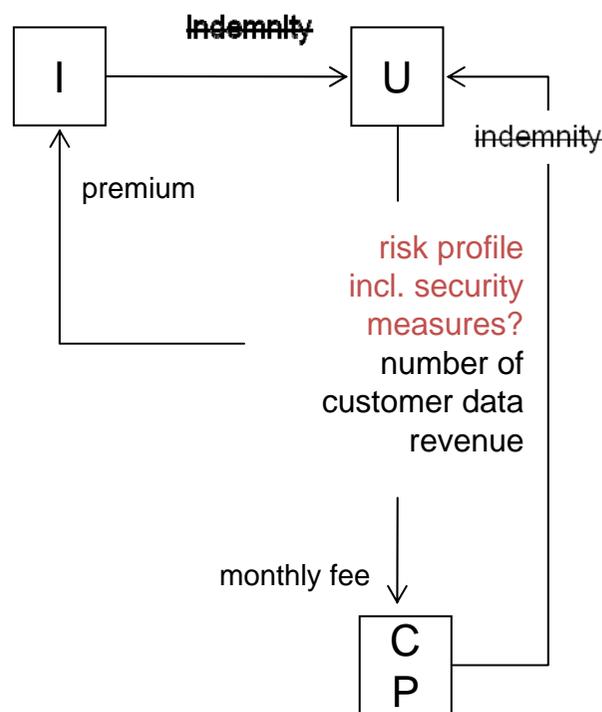
Key Results Insurability

- Randomness, Independence and Possible Maximum Loss are critical factors for insurers, especially because little re-insurance for cyber insurance is purchased

without
intermediation

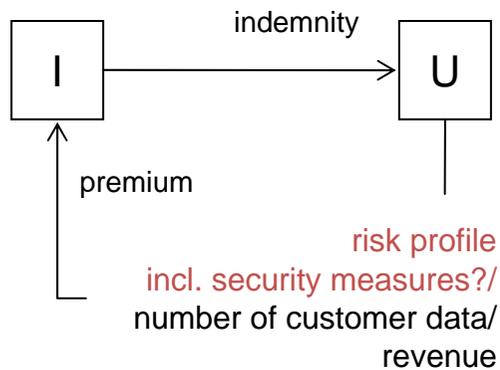


with cloud intermediation
current model



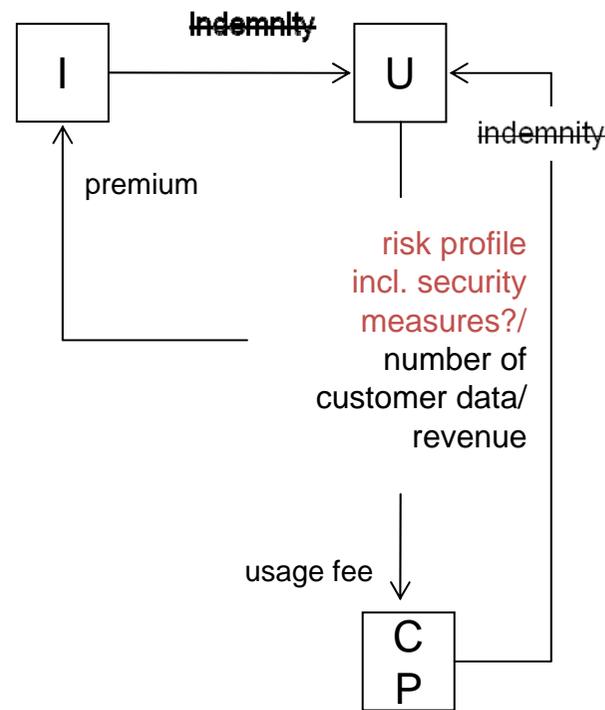
	ACE	AIG	Allianz	AON	Chartis	Chubb	HDI Gerling	Hiscox	Zurich
Covered damages and losses	Data Protect	Cyber Edge	Cyber Protect	Risk Solution	Cyber Edge	Cyber Security	Cyber+	Data Risks	Cyber & Data Protect.
Data Theft or Extortion	Green	Green	Green	Green	Green	Green	Green	Green	Green
Business Interruption	Green	Orange	Green	Green	Green	Green	Green	Green	Green
Reputational Loss	Orange	Orange	Orange	Orange	Orange	Orange	Orange	Orange	Orange
Crisis Management	Red	Green	Green	Green	Red	Green	Green	Green	Green
Forensic Actions	Green	Green	Green	Green	Green	Green	Green	Green	Green
3 rd Party Liability	Red	Orange	Green	Green	Green	Green	Orange	Green	Green
3 rd Party Loss of Income	Red	Red	Orange	Orange	Red	Red	Orange	Red	Orange
Violation of Privacy (Laws)	Orange	Green	Red	Orange	Green	Red	Orange	Red	Orange
....
Cloud coverage	Red	Red	Diagonal	Diagonal	Diagonal	Red	Red	Red	Diagonal

without
intermediation

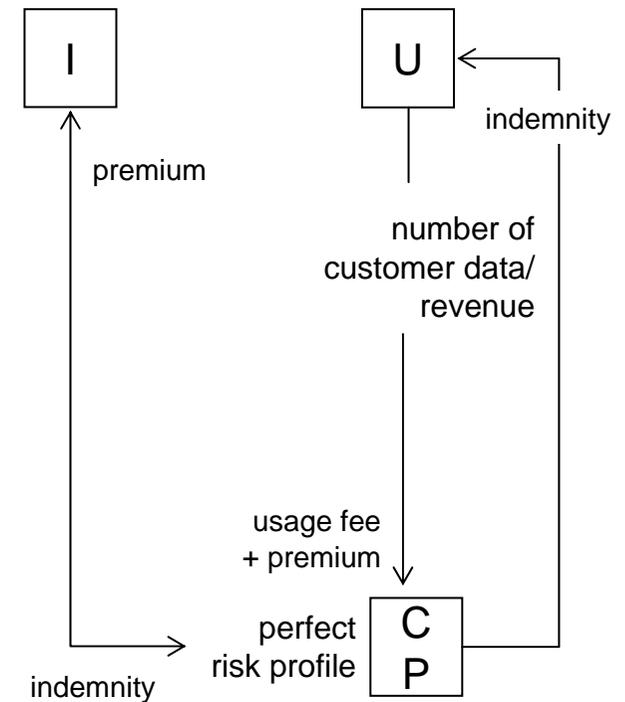


with cloud intermediation

current model



proposed model



ex ante	probability * loss
ex post	accident impact assessment

ex ante	probability * loss
ex post	accident impact assessment

- Cyber insurers should establish an **strategic cooperation** with cloud providers to offer cyber insurances to a mass market
- Solutions, like intensive IT security assessments and monitoring for larger companies are possible, but leading to high transaction costs on cyber insurance markets → too high premiums
- Cloud Computing can improve the situation of asymmetric information about security measures on cyber insurance markets, which is a major problem on these markets
- To calculate the possible maximum loss, information like the company's revenue, the number of employees or customer data can be sufficient to determine the insured sum
- Cloud Computing can be used as a distribution channel to offer cyber insurance products as cyber insurance markets in Germany reach only low market volume



1. **Background & Motivation**
2. **Research questions**
3. **Key results**
4. **Further research and discussion**

- We now focus on the impact of cloud computing on the cyber insurance market
- We propose a theoretical model to show that cloud computing providers are important intermediaries to reduce asymmetric information on cyber insurance markets, which is a major problem for cyber insurance markets



thank you

- Comparison of the U.S. and the German Cyber Insurance Market

market characteristics	U.S.	Germany
written premiums	\$ 1.3 billion	\$ 50 million
market penetration (% of companies)	30 %	5 %*
market growth	double digit growth available	double digit growth expected
market participants	> 30 insurers	< 10 insurers
insurance cover	up to \$ 350 million	up to \$ 250 million
main driver of demand	laws & legal provisions	-
popular coverage	liability & third party	business interruption