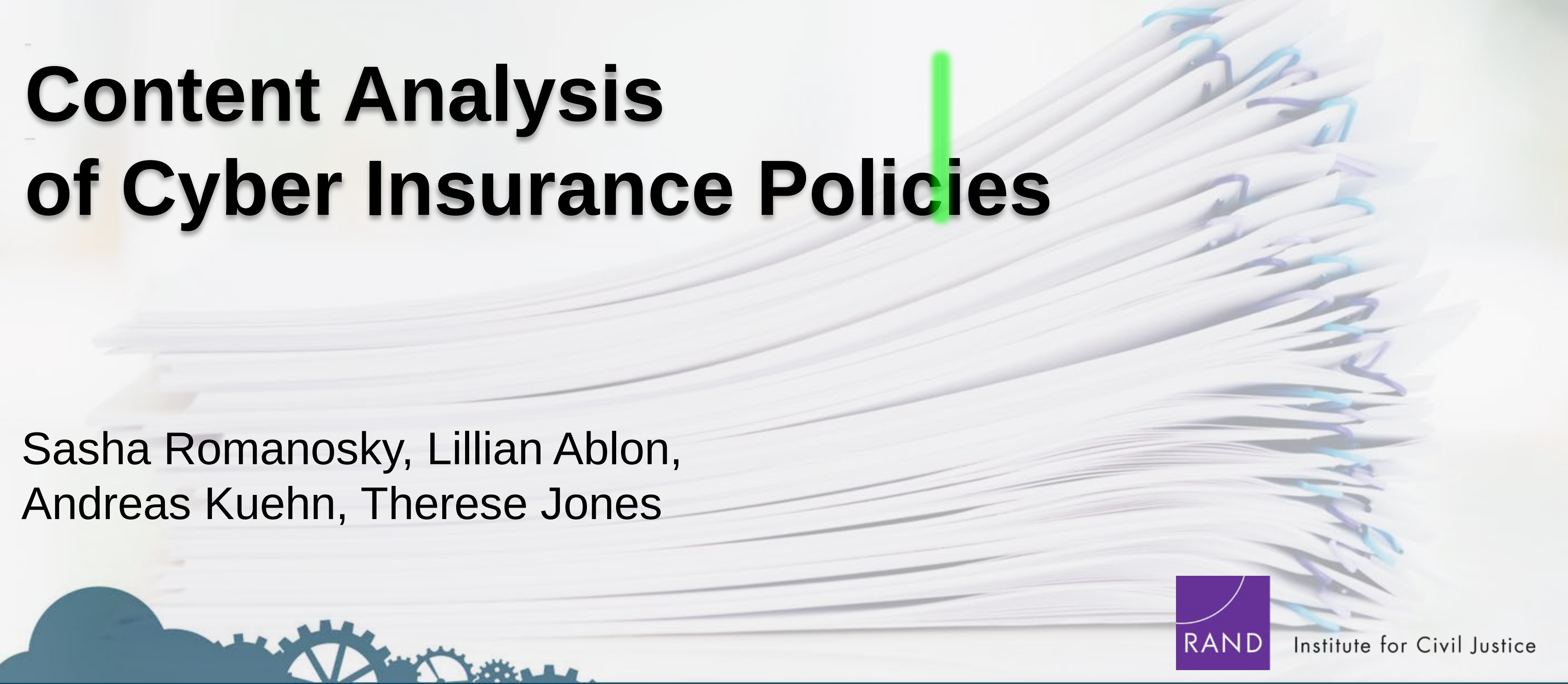


Content Analysis of Cyber Insurance Policies

Sasha Romanosky, Lillian Ablon,
Andreas Kuehn, Therese Jones

RAND Institute for Civil Justice

PRIVACYCON

Can insurance help decrease privacy risk?

- U.S. seeks to induce companies and critical infrastructure to better protect computers
  - NIST cyber security framework
  - Market solutions like cyber insurance have potential

- Challenges
  - Insuring can backfire (moral hazard)
  - Can insurers differentiate risk between client firms?

Research Questions

- What is the current state of cyber insurance policies?

- How do insurance carriers price cyber and privacy risks?

Current Market

- Total US premiums approximately $2b annually
- However, this makes up <1% of all corp. US insurance
- Typical:
  - premiums between $10k - $25k
  - limits between $10m - $25m
  - and towers of hundreds of millions

Policies collected from State Insurance Commissioners

180+ dockets
from NY, PA, CA, and large carriers (2007–2017)

69
coverage &
exclusions

44
security
questionnaires

96
rate
schedules

What is covered?

Common coverage areas

- Business income loss
- Forensic review
- Notification to affected individuals
- Monitoring expenses
- Public relations services
- Cost of claims, penalties, defense, and settlement

Rare, but notable

- E-theft (phishing)
- Website media content
- Act of terrorism (if electronic)

SECURITY and PRIVACY QUESTIONNAIRES

ORGANIZATIONAL

TECHNICAL

LEGAL & COMPLIANCE

POLICIES & PROCEDURES

SECURITY and PRIVACY QUESTIONNAIRES

ORGANIZATIONAL

- Data collection and handling
- Outsourcing
- Incident loss history
- IT security budget & spending

TECHNICAL

- Information technology and computing infrastructure
- Technical security measures
- Access control

LEGAL & COMPLIANCE

- Healthcare privacy
- Financial security regulation compliance/standards

POLICIES & PROCEDURES

- Information and data management
- Employee privacy
  and network security
- Organizational security policies and procedures

How do carriers price cyber risk? Suboptimally

“Limitations of available data have constrained the traditional actuarial methods used to support rates.”

Translation: ***“We don’t know.”***

“The base retentions were set at what we believe to be an appropriate level for the relative size of each insured.”

Translation: ***“We’re guessing.”***

“The rates for the above-mentioned coverages have been developed by analyzing the rates of the main competitors.”

Translation: ***“We’re using someone else’s guess.”***

Carriers base estimates on other insurance lines

“Loss trend was determined by examining 10 years of countrywide Fiduciary frequency and severity trends.”

“The Limit of Liability factors are taken from our Miscellaneous Professional Liability product.”

“Base rates for each module of this new product were developed based on currently filed Errors and Omissions and Internet Liability rates.”

Pricing strategy #1: Flat rate

Coverage	Frequency	Severity	Expected Loss	Profit	Premium
	*	=	(Lost Cost)	Load	
Computer Attack	0.20%	$49,800	$99.60	35%	$153
Network Liability	0.17%	$86,100	$147.23	35%	$227

Carriers use data from industry, and academic reports

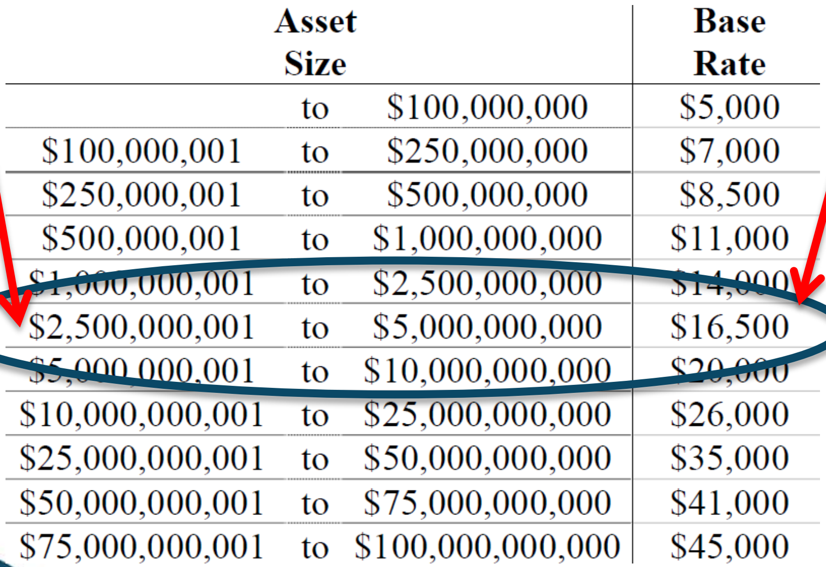
No variation by firm, industry, or risk

Targeted toward small businesses

Pricing strategy 2: base rate

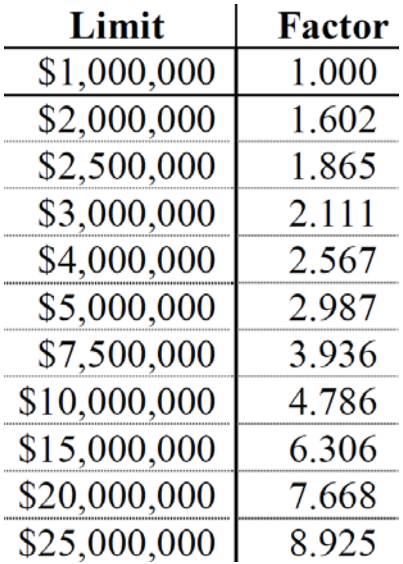
1) Determine revenue

2) Base premium



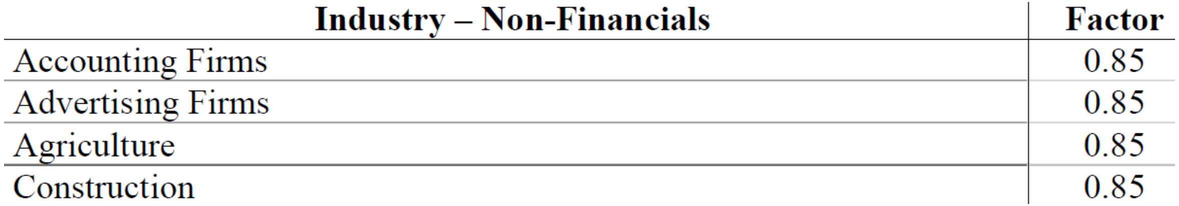
Asset Size			Base Rate
	to	$100,000,000	$5,000
$100,000,001	to	$250,000,000	$7,000
$250,000,001	to	$500,000,000	$8,500
$500,000,001	to	$1,000,000,000	$11,000
$1,000,000,001	to	$2,500,000,000	$14,000
$2,500,000,001	to	$5,000,000,000	$16,500
$5,000,000,001	to	$10,000,000,000	$20,000
$10,000,000,001	to	$25,000,000,000	$26,000
$25,000,000,001	to	$50,000,000,000	$35,000
$50,000,000,001	to	$75,000,000,000	$41,000
$75,000,000,001	to	$100,000,000,000	$45,000

3) Increase limits

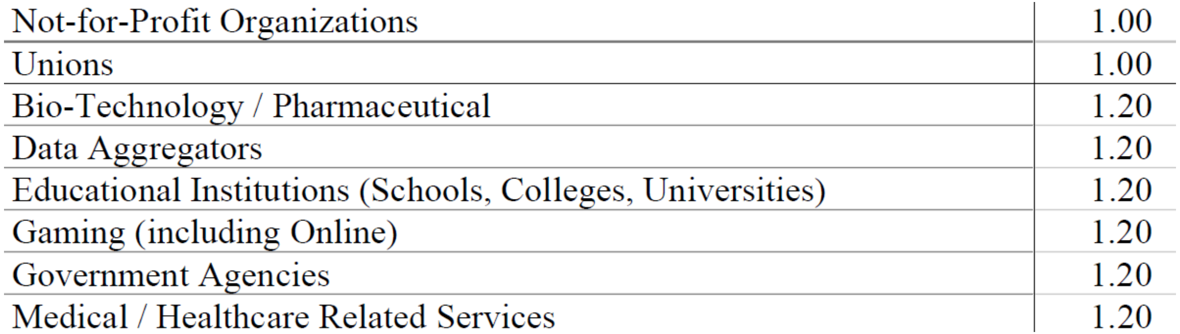


Limit	Factor
$1,000,000	1.000
$2,000,000	1.602
$2,500,000	1.865
$3,000,000	2.111
$4,000,000	2.567
$5,000,000	2.987
$7,500,000	3.936
$10,000,000	4.786
$15,000,000	6.306
$20,000,000	7.668
$25,000,000	8.925

Pricing strategy 2: base rate

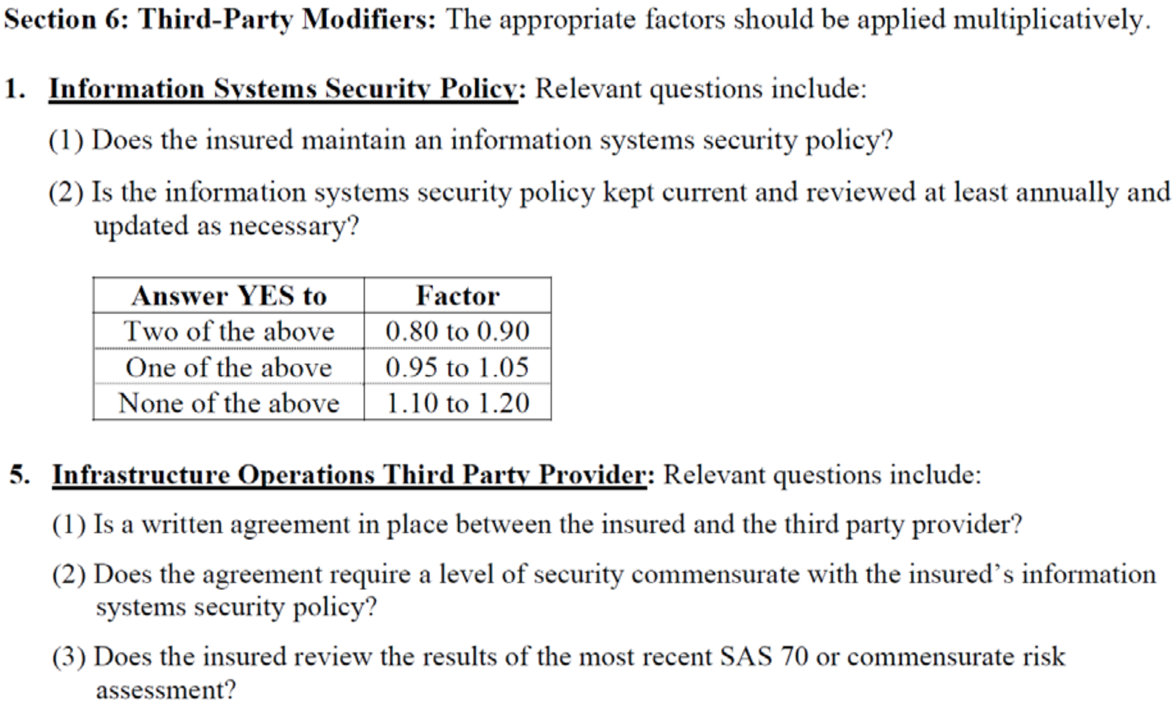


Industry – Non-Financials	Factor
Accounting Firms	0.85
Advertising Firms	0.85
Agriculture	0.85
Construction	0.85



Not-for-Profit Organizations	1.00
Unions	1.00
Bio-Technology / Pharmaceutical	1.20
Data Aggregators	1.20
Educational Institutions (Schools, Colleges, Universities)	1.20
Gaming (including Online)	1.20
Government Agencies	1.20
Medical / Healthcare Related Services	1.20

Pricing strategy 3: Security/Privacy questions



Section 6: Third-Party Modifiers: The appropriate factors should be applied multiplicatively.

1. **Information Systems Security Policy:** Relevant questions include:

   (1) Does the insured maintain an information systems security policy?

   (2) Is the information systems security policy kept current and reviewed at least annually and updated as necessary?

Answer YES to	Factor
Two of the above	0.80 to 0.90
One of the above	0.95 to 1.05
None of the above	1.10 to 1.20

5. **Infrastructure Operations Third Party Provider:** Relevant questions include:

   (1) Is a written agreement in place between the insured and the third party provider?

   (2) Does the agreement require a level of security commensurate with the insured's information systems security policy?

   (3) Does the insured review the results of the most recent SAS 70 or commensurate risk assessment?

Source: Policy questions from California insurer

How are final premiums calculated?

(Source: Final premium calculation from a California cyber insurance policy)

(Third party liability base rate) + (First party base rate if elected)
X (Limit factor)
X (Retention factor)
X (Data classification factor)
X (Security infrastructure factor)
X (Governance, risk and compliance factor)
X (Payment card controls factor)
X (Media controls factor)
X (Computer system interruption loss factor, if applicable)
X (Retroactive coverage factor) x (Claims/loss history factor)
X (Endorsement factor, if applicable)

Final Premium

✉ sromanos@rand.org

🐦 @SashaRomanosky

Research Methodology

We conducted a directed content methodology

- which enables us to identify and categorize themes and concepts, and derive meaning and insights across policies

Sample size was determined by purposive sampling, which relies on saturation:

- the point when new information produces no change to the codebook
- “As [the researcher] sees similar instances over and over again, [she] becomes empirically confident that a category is saturated”
- i.e. we want to saturate our codebook

What is excluded?

Common exclusions

- Criminal acts; trade law violation
- Acts of war or terrorism
- Theft of intellectual property, except when caused by breach
- Disregard for computer security

Rare, but notable

- Caused by a named virus
- Collateral damage
- Outsourcing of data processing

What did we learn about cyber insurance policies?

Coverage is available for most kinds of losses

- But pay attention to the exclusions

Security questionnaires appear to ask a reasonable set of questions

- Can there be improvements?

Despite suggestions, carriers <u>do not</u> appear to have advanced capabilities for assessing risk

Future work

- Empirical analysis of premium pricing