

Content Analysis of Cyber Insurance Policies

Sasha Romanosky, Lillian Ablon, Andreas Kuehn, Therese Jones

Motivation

- Since at least 2013 (EO 13636, PPD-21), the USG has sought to induce the private sector, and critical infrastructure, to better protect their computing systems
 - NIST's cyber security framework was an important (voluntary) milestone
 - Market-driven solutions, like cyber-insurance are key potential solutions
- But there are challenges:
 - Insuring against loss can backfire (moral hazard)
 - Requires that insurance companies are able to assess, and differentiate risk between firms

Research Questions

- What is the current state of cyber insurance policies, and
- How do insurance carriers price cyber risk?
- We collected a dataset of cyber insurance contracts, and systematically examined their 3 components:
 - Coverage and Exclusions
 - Application Questionnaires
 - Rate Schedules

Current Market

- Total US premiums estimated between \$1b - \$2b annually
 - projected to reach \$20b by 2020
 - offered by ~500 firms
- However, this only makes up <1% of all corporate US insurance
- Avg. premiums between \$10k-\$25k, with limits between \$10m-\$25m, and towers up to \$100m

Data Collection

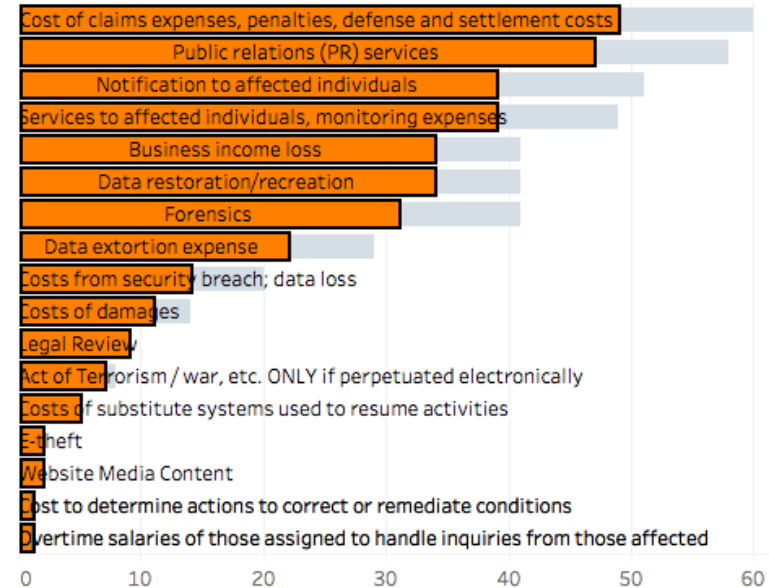
- Acquired 180+ policy dockets and hundreds of files from NY, PA, CA state insurance commissioners, in addition to large carrier websites
- Chose these states because of their size, geographic variation
- Policies cover years 2007 - 2017
- After data cleaning, we are left with:
 - Coverage and Exclusions: $n = 69$
 - Applications Questionnaires: $n = 44$
 - Rate Schedules: $n = 42$

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

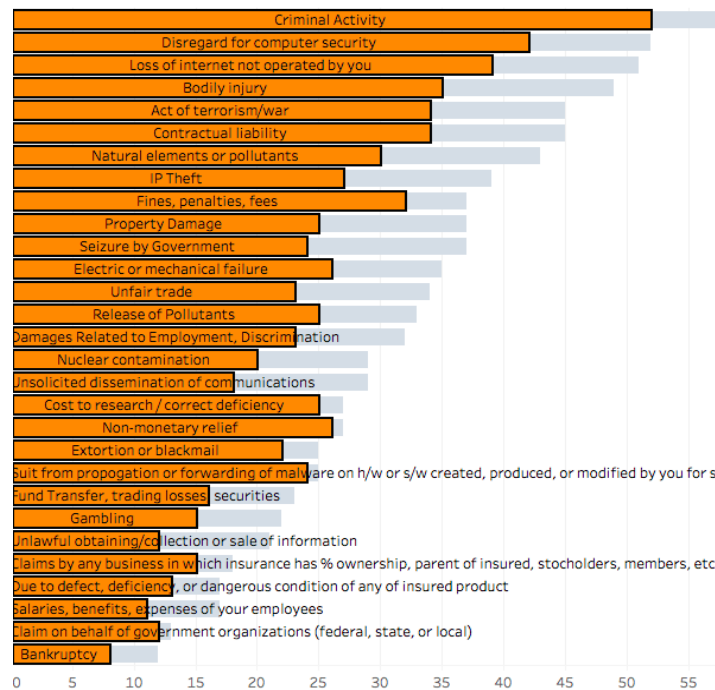
Part 1: Which Losses are Commonly Covered?

- Commonly covered losses:
 - Cost of legal claims, penalties
 - Public relations services
 - Consumer notification, monitoring
 - Business income loss
 - Forensic investigation
 - Data restoration
- Rarely covered losses:
 - Ransomware
 - Act of terrorism



Which Losses are Commonly Excluded?

- Common exclusions:
 - Criminal activity
 - Property damage and bodily injury
 - Acts of war or terrorism
 - Intentional disregard for computer security
 - Seizure or destruction by government
- Others:
 - Caused by a named virus
 - Outsourcing of data processing
 - Reputational injury



Part 2: Security Questionnaires

- Ostensibly used to help assess an applicant's security posture (e.g technical and management practices)
- We identified 98 different topics, reduced to 4 main categories:
 - Organizational (32 topics)
 - Technical (16)
 - Policies and Procedures (40)
 - Legal and Compliance (10)

Organizational, and Technical

- Organizational (32)
 - Industry, revenues, current insurance coverage
 - Loss history
 - Budget allocation among: prevention, detection, and response controls
- Technical (16)
 - Number of computing devices, or IP addresses; network segmentation
 - Measures to protect against data theft and intrusions such as AV, IDS/IPS
 - Controls to enforce secure user access, and access revocation

Policies and procedures, and Legal

- Policies and procedures (40)
 - Does the applicant sell or share sensitive information (i.e., PII)?
 - Does the applicant perform a privacy/security assessment of 3rd parties?
 - Does the Applicant run vulnerability scans or penetration tests against all parts of the Applicant's network? If "yes" how often are the tests run?
- Legal (10)
 - Compliance with HIPPA, PCI/DSS, GLBA

Part 3: How do carriers price cyber risk?

- Answer: Poorly
- *“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” – we're guessing*
- *“The rates for the above-mentioned coverages have been developed by analyzing the rates of the main competitors” – we're using someone else's guess*

Carriers also borrow from other lines of business

- *"...factors are taken from our Miscellaneous Professional Liability product."*
- *"...factors were based on currently filed Errors and Omissions and Internet Liability rates."*
- *"...we chose to use Fiduciary liability data because it has a similar limit profile and expected development pattern [as cyber losses]."*

Pricing Strategy #1: Flat Rate

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

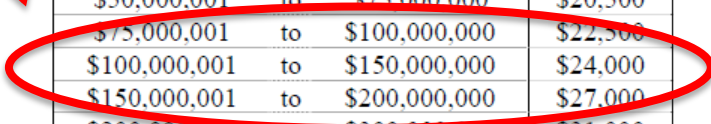


- Carriers use data from industry, and academic reports
- No variation by firm, industry, or risk
- Targeted toward small businesses

Pricing Strategy #2: Base Rate


1) Determine revenue

2) Base premium

3) Modify limits up/down



Annual Revenue			Base Rate
	to	\$5,000,000	\$5,000
\$5,000,001	to	\$10,000,000	\$7,500
\$10,000,001	to	\$25,000,000	\$11,500
\$25,000,001	to	\$50,000,000	\$16,500
\$50,000,001	to	\$75,000,000	\$20,500
\$75,000,001	to	\$100,000,000	\$22,500
\$100,000,001	to	\$150,000,000	\$24,000
\$150,000,001	to	\$200,000,000	\$27,000
\$200,000,001	to	\$300,000,000	\$31,000
\$300,000,001	to	\$400,000,000	\$33,500
\$400,000,001	to	\$500,000,000	\$37,000
\$500,000,001	to	\$750,000,000	\$40,000
\$750,000,001	to	\$1,000,000,000	\$43,500



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

Section 2: Industry Factors: The appropriate factor should be applied multiplicatively.

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

Labor Management Trusts	1.00
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
Municipalities (Local, County, State)	1.20

Pricing Strategy #3: Security Questions

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

2. **Laptop Security Policy:**

Does the insured have a laptop security policy?	Factor
Yes	0.80 to 0.90
N/A (insured does not use laptops)	1.00
No	1.10 to 1.20

3. **Website Third Party Service 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?

Answer YES to	Factor
---------------	--------

How are final premiums calculated?

The Cyber Liability premium is calculated as follows:

(Section 1 Base Rate) x (Section 2 Industry Factor) x (Section 3.1 ILF) x (Section 3.2 Retention Factor)
x (Section 3.3 Coinsurance Factor) x (Section 6 Third-Party Modifier Factors)

V. **Final Premium Calculation**

(Third Party Liability Base Rate) + (First Party Costs 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 (Endorsements Factor, if applicable) = **Final Premium**

What have we learned, and where do we go?

- 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 do not appear to have advanced capabilities for assessing risk
- Future work:
 - empirical analysis of premium pricing

Questions?

sromanos@rand.org