The State of Cybersecurity and Opportunities for Cyber Insurance

Advisory Council on Employee Welfare and Pension Benefit Plans
Department of Labor

July 18, 2022

Sasha Romanosky, PhD
sromanos@rand.org

The views and opinions expressed in this presentation and statement are mine alone and do not reflect those of the RAND Corporation

The state of cyber security

After 20 years, we security professionals and researchers are still unable to effectively measure and communicate cyber risk

1. We are unable to objectively determine which security controls are most effective
   - This is especially problematic given new vulnerabilities and attacker techniques
   - It's a game of best guesses, and prediction -- estimating probability of attack, and therefore appropriate countermeasures

2. We don't know how much to spend on cyber security
   - There is some *optimal* (efficient) amount, but no one can tell you what that is
   - All we can do is exhaust our IT budget, and hope for the best

This reduces our ability to fully measure, communicate, and manage cyber risk

3. The connection between security metrics and risk is weak
   - Metrics reflect what is easy to measure, not what you want really to know (risk)
   - Generally, they track *outputs*, not *outcomes*
   - E.g. how many vulnerabilities you patched -- not whether you patched the right ones

4. We can't tell if we're more secure now, relative to last year
   - We have no proven way to measure this
   - And measurement can be misguided (see above)

Now, sometimes measurement is effective

- Security metrics are tangible ways to demonstrate progress
  - "You can't manage what you can't measure," Edwards Deming (or possibly Peter Drucker)

- Quantifying harms (losses) provides an objective assessment of an impact that doesn't rely on normative, values-based judgments

- From an economic standpoint, quantification helps regulators and courts make efficient rules and avoid:
  - under-deterrence: incentivizing excessively risky behavior
  - over-deterrence: imposing unnecessary regulation

But are we obsessing over data?

- Some costs and harms are unquantifiable
  - because they represent inalienable rights,
  - because they are fundamental to our person
  - e.g. disclosure of medical or sexual information

- Quantifying some harms causes others to be ignored
  - E.g. privacy

- This can also lead to bad behaviors
  - "The more any metric is used for decision-making, the more it will distort and corrupt the processes it is intended to monitor" — Campbell's Law
  - "When a measure becomes a target, it ceases to be a good measure" — Goodhart's Law

These issues are pervasive

- The Federal Trade Commission has held dozens of panels with experts to testify and discuss the issue of harm caused by firm cyber security and privacy behaviors

- In addition, U.S. courts address similar issues of harm in order to impose proper sanctions or grant appropriate redress

- So how can cyber insurance help?

Cyber Insurance

- In theory:
  - Carriers use their capabilities to *assess* and *differentiate* risk across firms
  - Carriers convince policy holders to apply risk-reducing techniques
  - Better information -> Fewer breaches -> happier consumers

- The catch:
  - We don't want firms to substitute security investment with insurance (moral hazard)
  - Carriers don't know which are the best risk-reducing controls (Romanosky et al 2019)

- So how could insurance help?
  - Merge application data with claims data
  - Analyzed these together and objectively measure the security controls that lead to fewer breaches

We collected 180+ policy dockets from NY, PA, CA

69

coverage & exclusions

44

security questionnaires

42

rate schedules

Romanosky, S., Ablon, L., Khuen, A., Jones, T. (2017) Content Analysis of Cyber Insurance Policies: How Do Insurance Companies Price Cyber Risk?, Journal of Cybersecurity, 5(1), 1-19.

COMMON COVERAGE & EXCLUSIONS

Coverage

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

Exclusions

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

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.”

RATE SCHEDULES

Three types of pricing strategies:

Flat rate
Same for everyone

Base rate
Based on firm's size and type

Information Security Pricing
Incorporates some security questions

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) Increase limits

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

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

Final Thought on Costs and Incentives

- Research has shown that data breaches aren't (typically) that costly for firms
  - Median cost is only $200k
- Moreover, consumers often don't suffer losses
- We may still want to ask: are firms investing in the proper amount of security
  - Yes, firms may already be doing this
  - Just because breaches occur, this isn't evidence that firms aren't behaving "appropriately"

- If policy makers want firms to manage cyber security like any other enterprise risk, they must accept that cyber security may be deprioritized (and that's okay)

References

Cyber Insurance

- Sasha Romanosky, Lillian Ablon, Andreas Kuehn, Therese Jones, Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?, *Journal of Cybersecurity*, Vol. 5, No. 1.2019, tyz002, https://doi.org/10.1093/cybsec/tyz002
- Mohammad Mahdi Khalili, Mingyan Liu, Sasha Romanosky, Embracing and Controlling Risk Dependency in Cyber-insurance Policy Underwriting, *Journal of Cybersecurity*, Vol. 5, No. 1, 2019, tyz010, https://doi.org/10.1093/cybsec/tyz010

Firm and Consumer Costs of Data Breaches

- Sasha Romanosky, Examining the Costs and Causes of Cyber Incidents, *Journal of Cybersecurity*, Vol. 2, No. 2, Dec. 2016, pp. 121–135, https://doi.org/10.1093/cybsec/tyw001
- Romanosky, S. & Acquisti, A. (2009). Privacy Costs and Personal Data Protection: The Economic and Legal Perspectives. Berkeley Technology Law Journal, 24(3).

Breach Litigation

- Romanosky, S., Hoffman, D., and Acquisti, A. (2014). Empirical Analysis of Data Breach Litigation. Journal of Empirical Legal Studies, 11(1), 74–104.

Questions?

✉ sromanos@rand.org

@SashaRomanosky