

Analyzing Cyber insurance as a Market Based Solution for Cyber Resiliency

Sachin Shetty, Ph.D.

Associate Professor

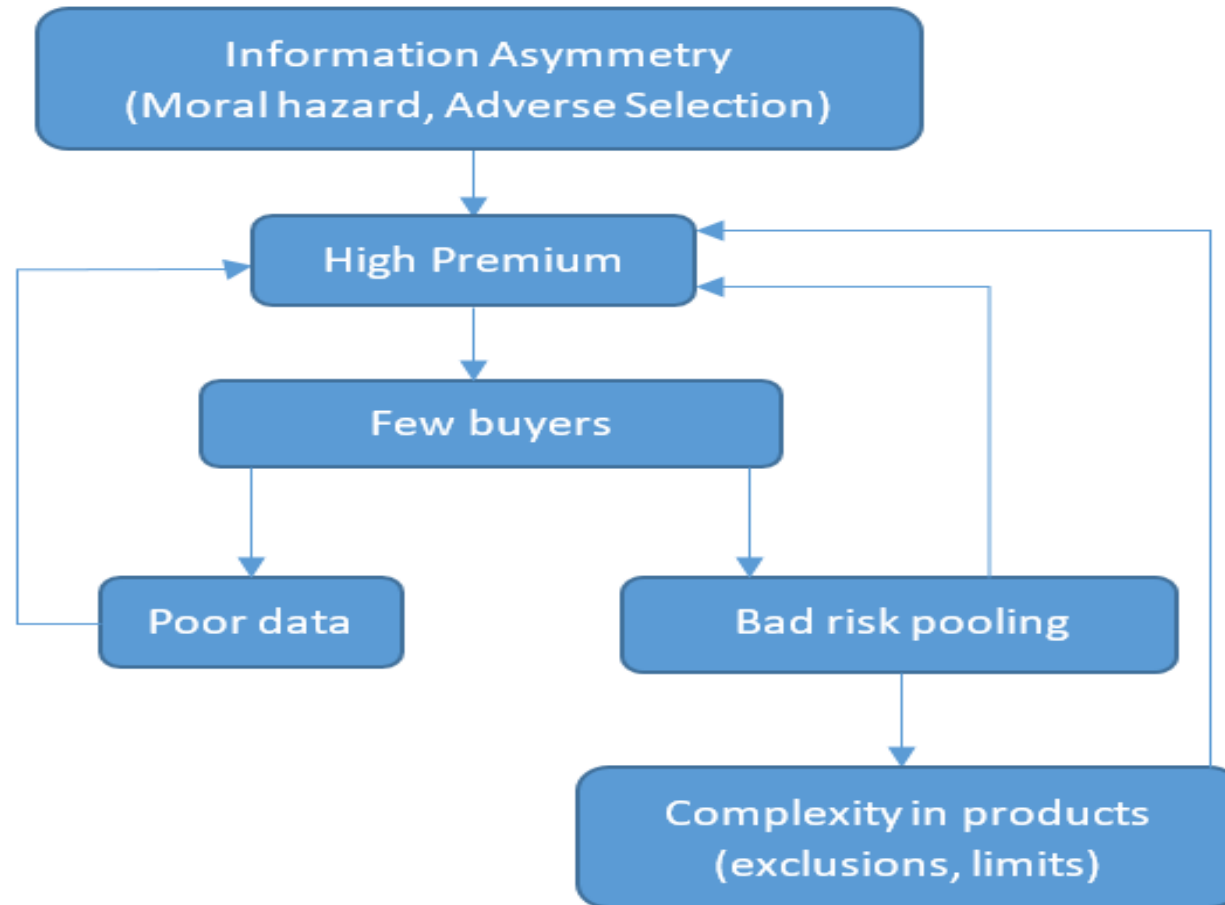
Virginia Modeling, Analysis and Simulation Center

Collaborator: Jay Kesan (UIUC)

Why Cyber Insurance?

- **Cyber Insurance Is A Private Market Solution**
 - Insurance allows risk shifting, but the risks of data-based injuries are often unknown.
 - A more developed cyber insurance market could incentivize the adoption of better security practices by requiring such practices as a condition of coverage.
- **Cyber Insurance Complements Government Action**
 - Government agencies can establish recommended standards of conduct, like the NIST Cybersecurity Framework, but their oversight ability is limited.
 - Insurance companies have a financial interest in (1) having a lot of policy holders, and (2) having policy holders whose networks are secure.
 - Government collaboration can turn the vicious circle of bad coverage and high premiums into a virtuous circle of good coverage and affordable premiums.

Feedback Loops in Cyber Insurance: A Vicious Circle

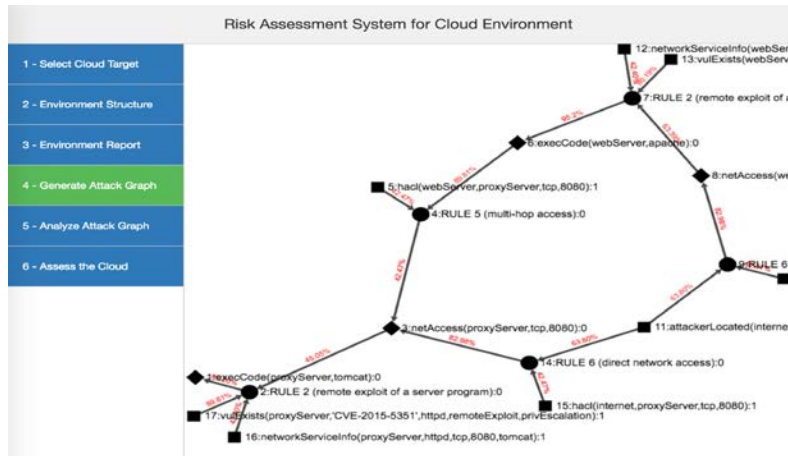


Risk Assessment is the Key

- The essential solution to the informational asymmetry problem is **better risk assessment**.
 - Narrow down the information gap between the insureds and the insurers.
 - Separate insureds with different risk levels and price policies more accurately.
 - Periodical risk assessment helps insurers monitor their risk exposures.
 - Better estimation of cost after losses.
- We can address this problem from several angles:
 - **Technological Risk (Cyber Risk Scoring and Mitigation (CRISM))**
 - **Portfolio Risk (Cyber Insurance Portfolio Analysis of Risk (CIPAR))**
 - **Legal Risk (Cyber Litigation Analysis Database (CLAD))**

TECHNOLOGICAL RISK

Cyber Risk Scoring and Mitigation (CRISM©)



• Problem

- Need to **understand** and **quantify** the impacts of **threats** to **cyber systems and networks** in order to develop prioritized mitigation plan

• Approach

- Built over a platform optimized for **vulnerability detection, attack graph analysis, and risk assessment.**
- Provides quantitative risk assessment and **categorizes attack paths** based on the impact of vulnerabilities.

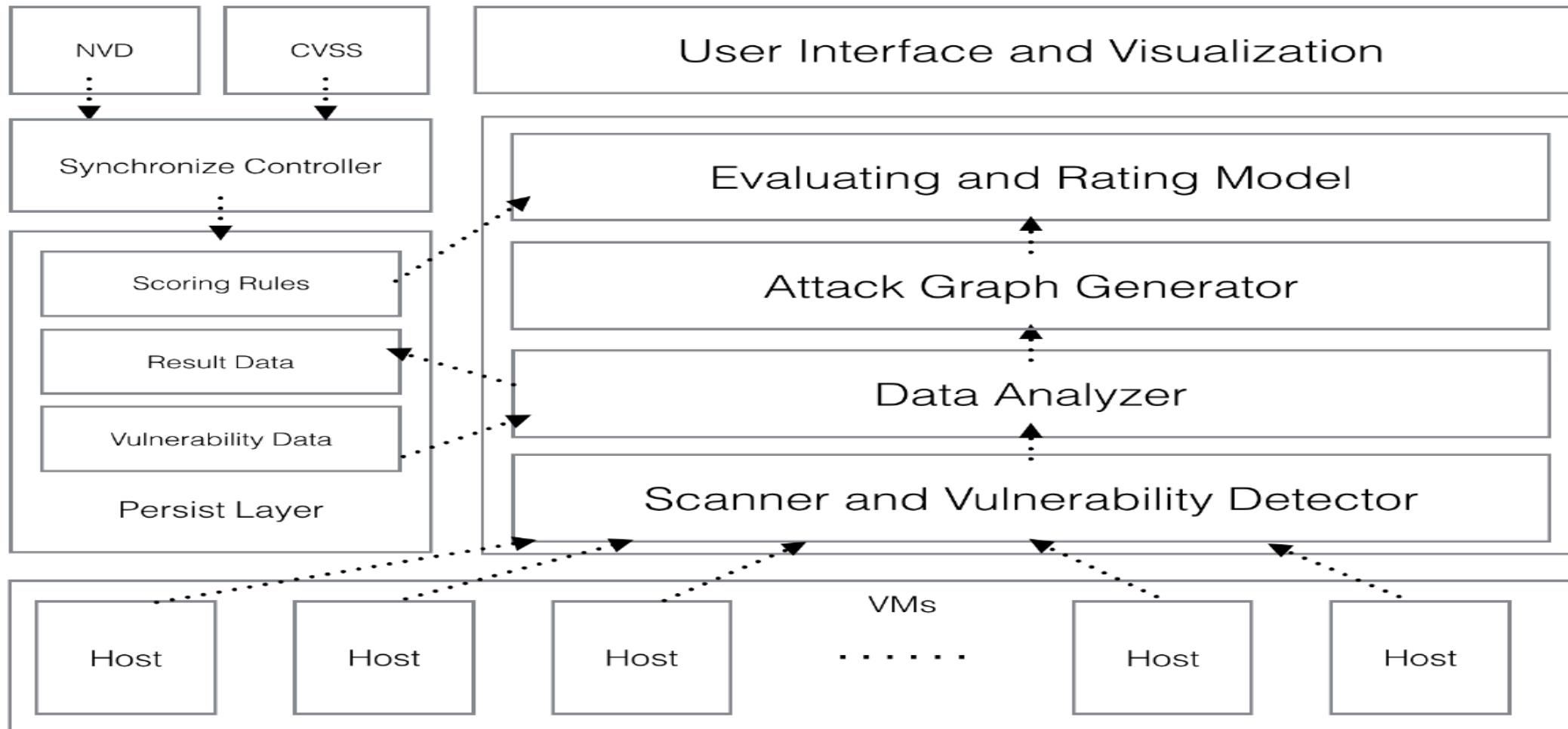
• Technology Transition

- Cyber Risk Scoring and Mitigation (CRISM) tool
- Software License
- Provisional Patent application filed

Measuring Security Risk

Challenges	Solutions
Identification of Attack Surfaces	Acquisition of vulnerability scores from live threat intelligence feeds and vulnerability databases
Identification of Exploitable Attack Paths	Network Vulnerability Tests and Attack graph generation
Modeling and assessing risk for cyber-insurance	Bayesian attack graph modeling techniques to categorize attack paths by impact, cost and degree of difficulty
On demand and real-time access to quantifiable cyber risks	Cloud based risk assessment tool

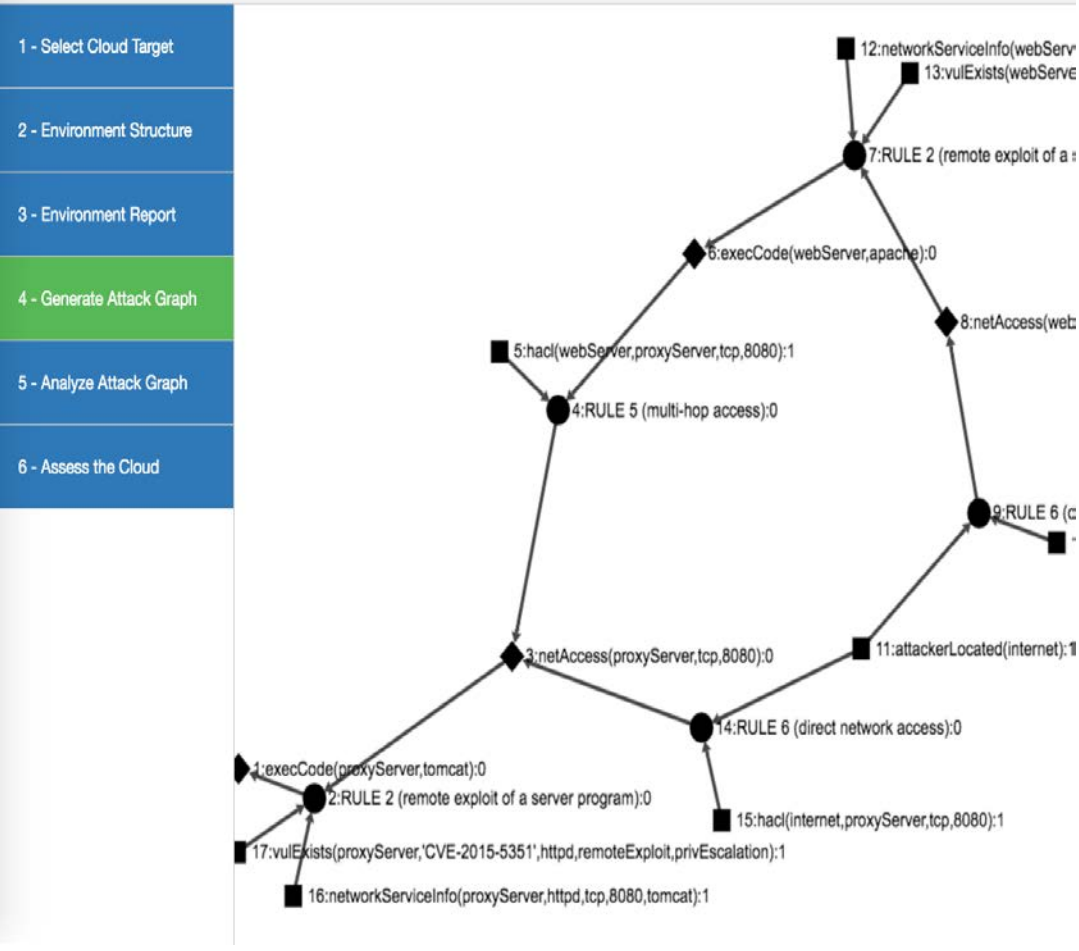
Cyber Risk Scoring and Mitigation (CRISM©)



Cyber Risk Scoring and Mitigation (CRISM©)

Bayesian Attack Graph

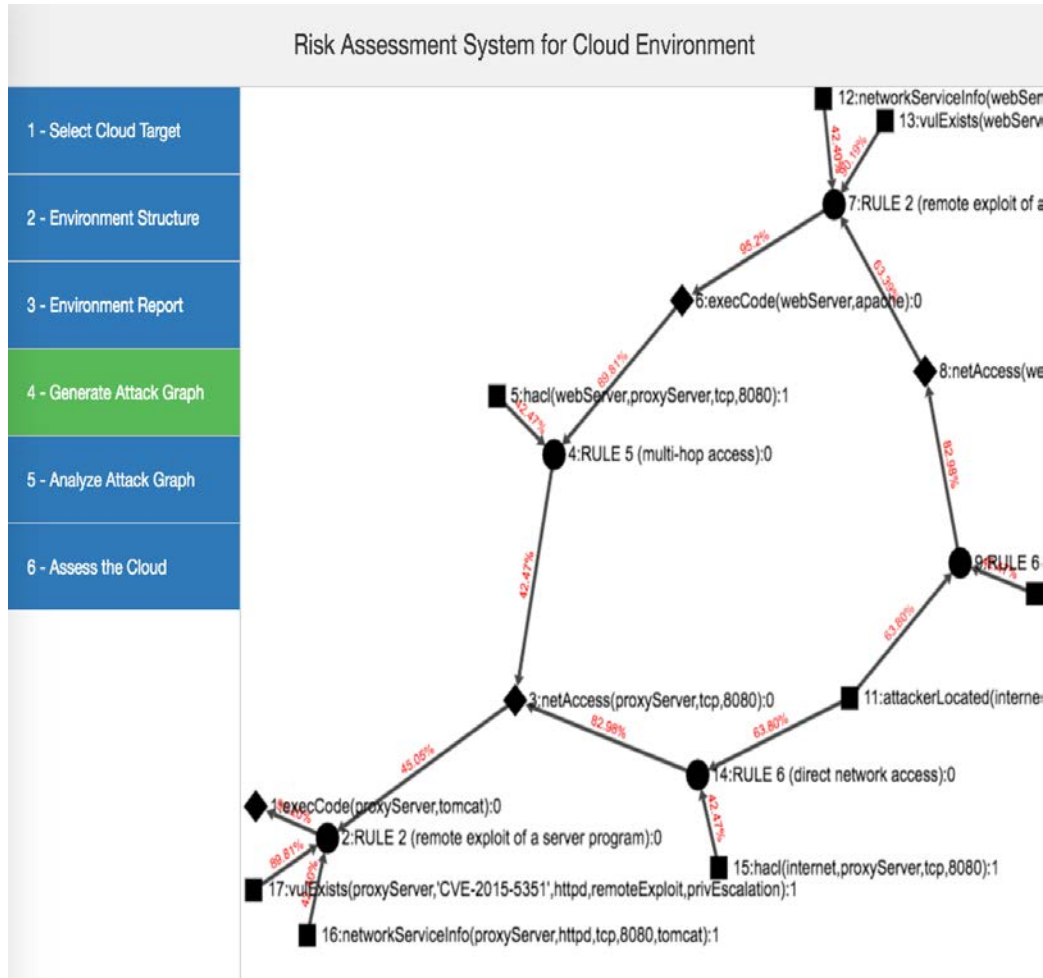
Risk Assessment System for Cloud Environment



- Extract topology and vulnerability information for enterprise systems and network from scanning, vulnerability tests and vulnerability databases
- Generation of attack graph to model security state of enterprise system and network
- Developed probabilistic security metric using Bayesian Networks by leveraging attack graph
- Encoding contribution of different security conditions during system compromise.

Cyber Risk Scoring and Mitigation (CRISM©)

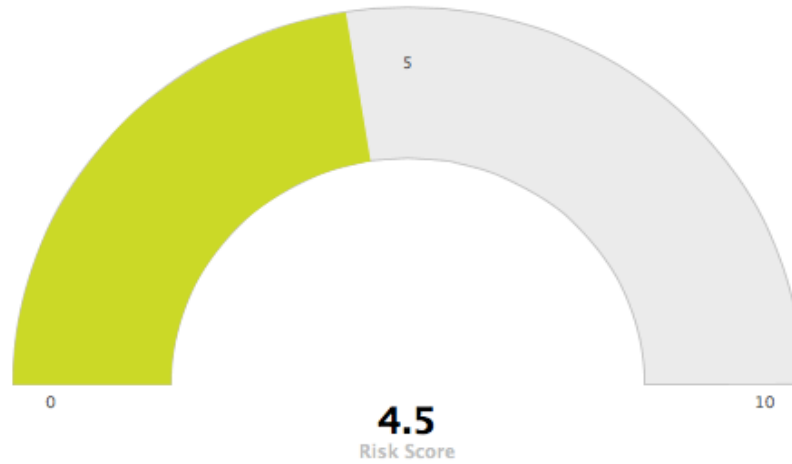
Bayesian Attack Graph Analysis



- Examples of vulnerabilities-
 - Unsafe security policy, corrupted file, memory access permission, unsafe firewall properties, unauthorized access
- System and network states represented as attributes and modeled using Bernoulli distribution
- Attacker success to reach goal depends on state of attributes
- Bayesian Attack Graph captures cause-consequence relationships between attributes

Cyber Risk Scoring and Mitigation (CRISM©)

- 2 - Environment Structure
- 3 - Environment Report
- 4 - Generate Attack Graph
- 5 - Analyze Attack Graph
- 6 - Assess the Cloud



Risk scores of the components in your cloud environment
Click the columns to view vulnerability details.



Portfolio RISK

CIPAR—Cyber Insurance Portfolio Analysis of Risk

- A web-based cyber risk assessment tool built on our data and analyses
- Gives firms from all market segments an easy way to estimate their exposure to cyber risk
- Help cyber insurance carriers manage portfolio risk more efficiently and improve product pricing
- Key features:
 - Cyber incident lookup
 - Cyber risk data visualization
 - Cyber risk scores based on firm characteristics
- [Demo](#)

Cyber Insurance Portfolio Analysis of Risk (CIPAR)

- CIPAR improves cyber insurance pricing and underwriting by:
 - **Using cyber incident data more efficiently**
 - Mitigate the data scarcity problem
 - **Improving risk modeling**
 - Make companies with different risk level distinguishable
- CIPAR provides insights into cyber losses based on Advisen's cyber incident database
- Integrates corporate finance data from ComputStat to provide relation between company characteristics and cyber incidents
- Computes quantified risk indicators and outputs a risk map based on company characteristics.

Data

- Analyzing over 40,000+ cyber incident records from public sources (WHID, VCDB) and from Advisen, Ltd., a leading provider of data for the commercial property and casualty insurance market
- Each record has:
 - Timeline (first notice date, report data, etc.)
 - Case characteristics (case type, causes, etc.)
 - Legal information (juris trigger, court, etc.)
 - Outcome (Loss amounts, injuries, etc.)
 - Victim company information (name, sector, size, etc.)
 - Detailed incident description from news media

Improving Efficiency in Data Usage

- Given the scarcity of cyber incident data, we must consider the trade-off between partition and abstraction
 - Abstraction removes excessive information
 - Partition gives more details, but breaks data into small pieces
 - 15 incident types in Advisen's dataset, some have very few observations making it hard to study these incident types
 - May need an abstraction by grouping together some incident types
- When we determine the optimal level of partition, we think about attributes of an incident that are the most important to insurers:
 - Cause – whether a peril is covered by policy
 - Loss (first-party damage, third-party liability, etc.) – whether a loss is covered

Cyber Risk Factors – Frequency

- Firm size variable has a statistically significant coefficient of 0.035
 - In the same industry, larger firms experience cyber attacks more frequently than smaller firms in a given period
 - Because firm size variable is log scaled, the attack frequency for smaller firms is more sensitive to firm size changes
 - From 100 employees to 200 employees, ~3-year incident number goes up 0.024
 - From 1000 employees to 1100 employees, ~3-year incident number goes up 0.003
- Coefficient varies across different industries
 - Firms in some industries are more often attacked than the others

Industry	Coefficient	Standard Error
NAICS-51 Information	1.47	0.09
NAICS-52 Finance and Insurance	0.97	0.08

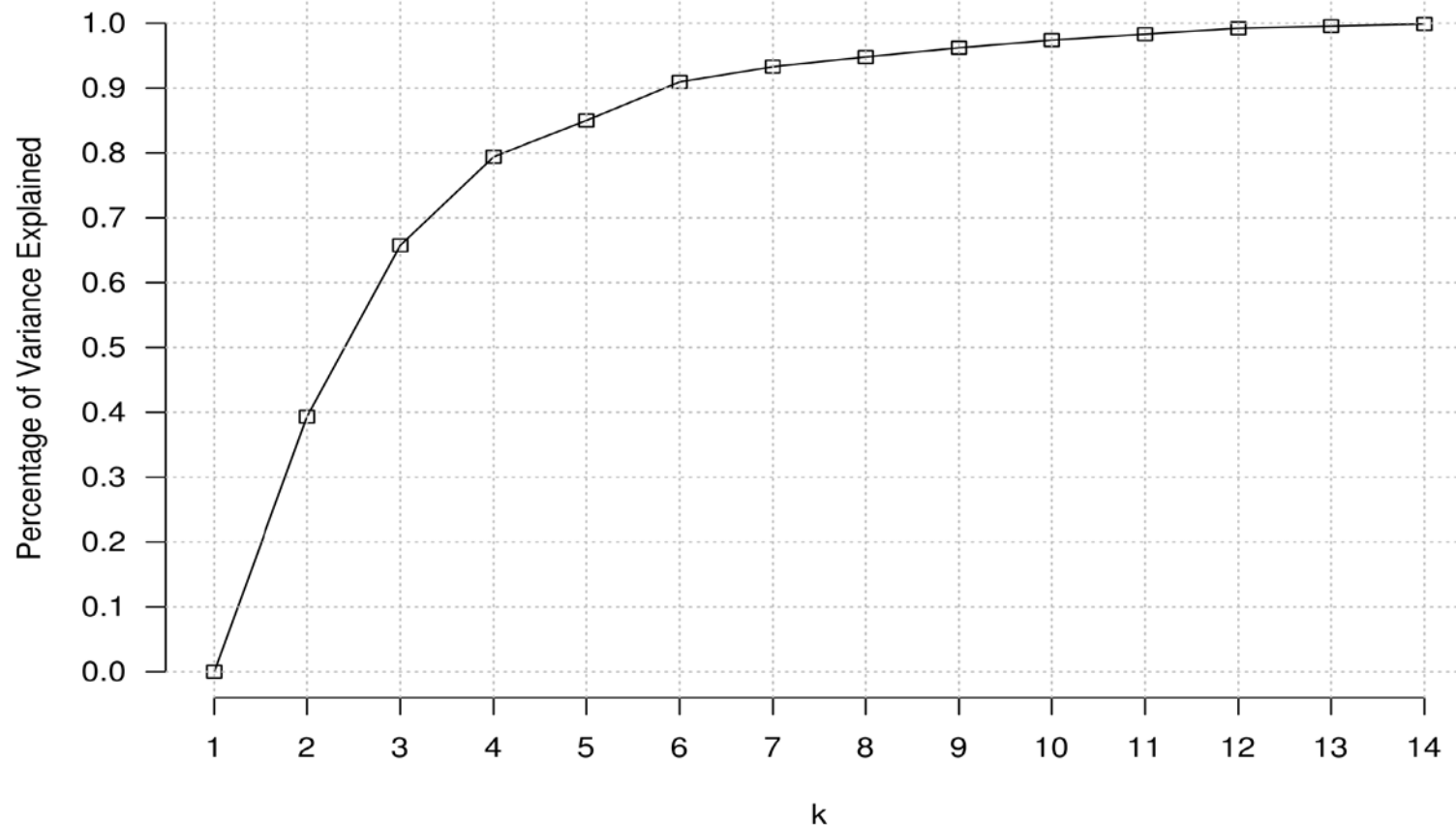
Cyber Risk Factors – Severity

- Firm size has a statistically significant coefficient of 0.1627
- In the same year and same industry, larger firms suffer more breaches
- Again, pairwise t-test suggests that firms in industry-51 (information industry) experience more severe data breaches than firms in other industries

	11	21	22	23	31	32	33	42	44	45	48	49	51	52	53	54	55	56	61	62	71	72	81	
21	1																							
22	1	1																						
23	1	1	1																					
31	1	1	1	1																				
32	1	1	1	1	1																			
33	1	1	1	1	1	1																		
42	1	1	1	1	1	1	1																	
44	1	1	1	1	1	1	1	1																
45	1	1	1	1	1	1	1	1	1															
48	1	1	1	1	1	1	1	1	1	1														
49	1	1	1	1	1	1	1	1	1	1	1													
51	1	1	1	1	0.06	0.03	0.00	0.00	0.00	0.00	0.16	1												
52	1	1	1	1	1	1	1	1	1	1	1	1	0.00											
53	1	1	1	1	1	1	1	1	1	1	1	1	0.35	1										
54	1	1	1	1	1	1	1	1	1	1	1	1	0.00	1	1									
55	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1								
56	1	1	1	1	1	1	1	1	1	1	1	1	0.00	1	1	1	1							
61	1	1	1	1	1	1	1	1	1	1	1	1	0.00	1	1	1	1	1						
62	1	1	1	1	1	1	1	1	1	1	1	1	0.00	1	1	1	1	1	1					
71	1	1	1	1	1	1	1	1	1	1	1	1	0.04	1	1	1	1	1	1	1				
72	1	1	1	1	1	1	1	1	1	1	1	1	0.00	1	1	1	1	1	1	1	1			
81	1	1	1	1	1	1	1	1	1	1	1	1	0.00	1	1	1	1	1	1	1	1	1	1	
92	1	1	1	1	1	1	1	1	1	1	1	1	0.00	1	1	1	1	1	1	1	1	1	1	1

Improving Efficiency in Data Usage (Cont.)

The Elbow Method



K-means clustering method is applied to group together incident types with similar loss profile

- Optimal number of clusters is determined by the Elbow method
 - Choosing the smallest number that makes the model have enough explanatory power
 - In this case, the optimal number is 6
- 6 clusters would be sufficient to explain 90% of in-cluster variance
- Indicating the original data having lots of unnecessary information (6 clusters vs 15 incident types)

6 Types of Outcomes

Group	Causes	Note
1	Privacy - Unauthorized Contact or Disclosure	Privacy Violation
	Privacy - Unauthorized Data Collection	
2	Denial of Service (DDOS)/System Disruption	Cyber disruptions that affect business operations
	Network/Website Disruption	
3	Industrial Controls & Operations	Industrial Controls & Operations
4	Cyber Extortion	Unauthorized access to information systems for financial gain
	Digital Breach/Identity Theft	
	Identity - Fraudulent Use/Account Access	
	Phishing, Spoofing, Social Engineering	
5	Skimming, Physical Tampering	Malicious data breach and IT failures
	Data - Malicious Breach	
	Data - Physically Lost or Stolen	
	IT - Configuration/Implementation Errors	
6	IT - Processing Errors	Unintentional data disclosure
	Data - Unintentional Disclosure	

Many types of incidents are similar based on the criteria of cause and loss

- Incidents in the same group tend to lead to same types of losses
- E.g. incidents in group 4 usually cause only first-party losses and rarely result in any third party liabilities
- They also share similarity in causes, which makes intuitive sense

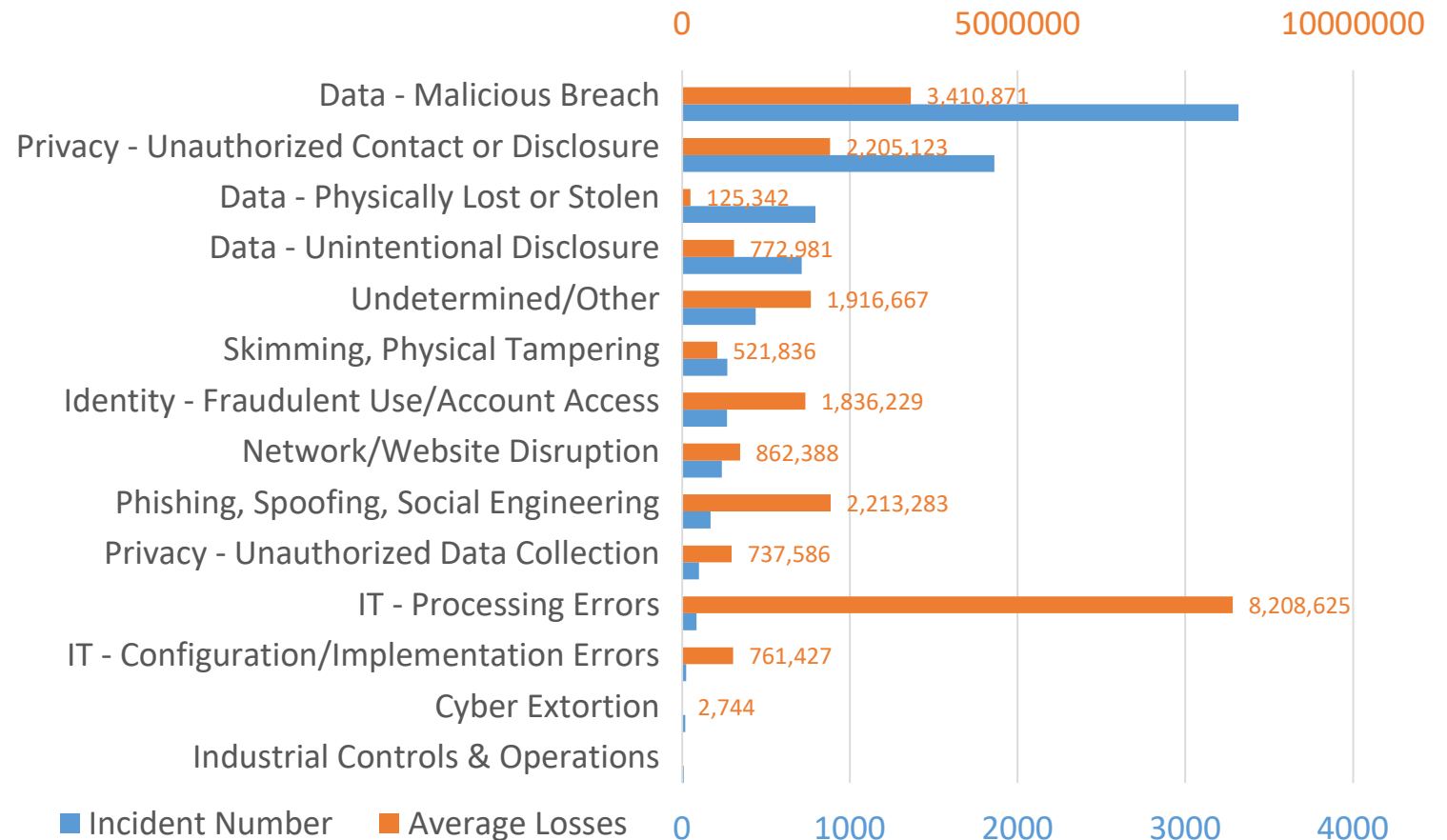
6 Types of Outcomes

- 5-level scale indicating likelihood of having the type of loss

Group	Cause	Financial Losses	Fines and Penalties	Plaintiff Legal Expenses	Other
1	Privacy - Unauthorized Contact or Disclosure	High	Low	Low	Very Low
	Privacy - Unauthorized Data Collection				
2	Denial of Service (DDOS)/System Disruption	High	Very Low	Very Low	Low
	Network/Website Disruption				
3	Industrial Controls & Operations	Low	Very Low	Very Low	High
4	Cyber Extortion	Very High	Very Low	Very Low	Very Low
	Digital Breach/Identity Theft				
	Identity - Fraudulent Use/Account Access				
	Phishing, Spoofing, Social Engineering Skimming, Physical Tampering				
5	Data - Malicious Breach	Medium	Low	Very Low	Very Low
	Data - Physically Lost or Stolen				
	IT - Configuration/Implementation Errors				
	IT - Processing Errors				
6	Data - Unintentional Disclosure	Low	Medium	Low	Very Low

Cyber Incident Types

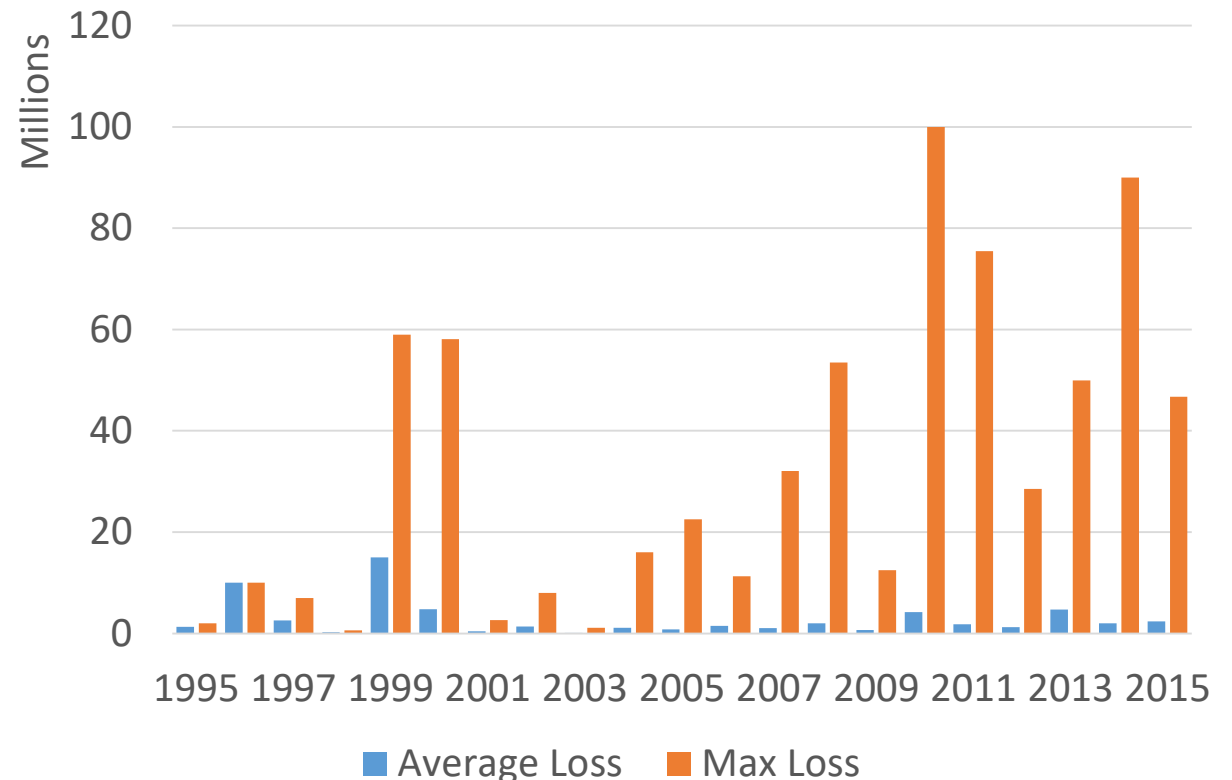
- Malicious data breach is the most common cyber-incident type in maritime industry, and it causes an average loss of 3.41 million per incident, which is also quite high compared to other incident types
- IT processing errors has a low occurrence frequency, but can cause large losses



Cyber Incident Losses

- The maximum possible loss in a single cyber incident is getting higher in recent years
- Average loss remains low, indicating that incidents with small losses are becoming more frequent
- Implications:
 - Firms in maritime industry should give data protection high priority when managing cyber risk, and take extra care to prevent IT process errors
 - Firms may want to transfer some risks (cyber insurance) since cyber risks are becoming more unretainable

Loss Amount per Incident

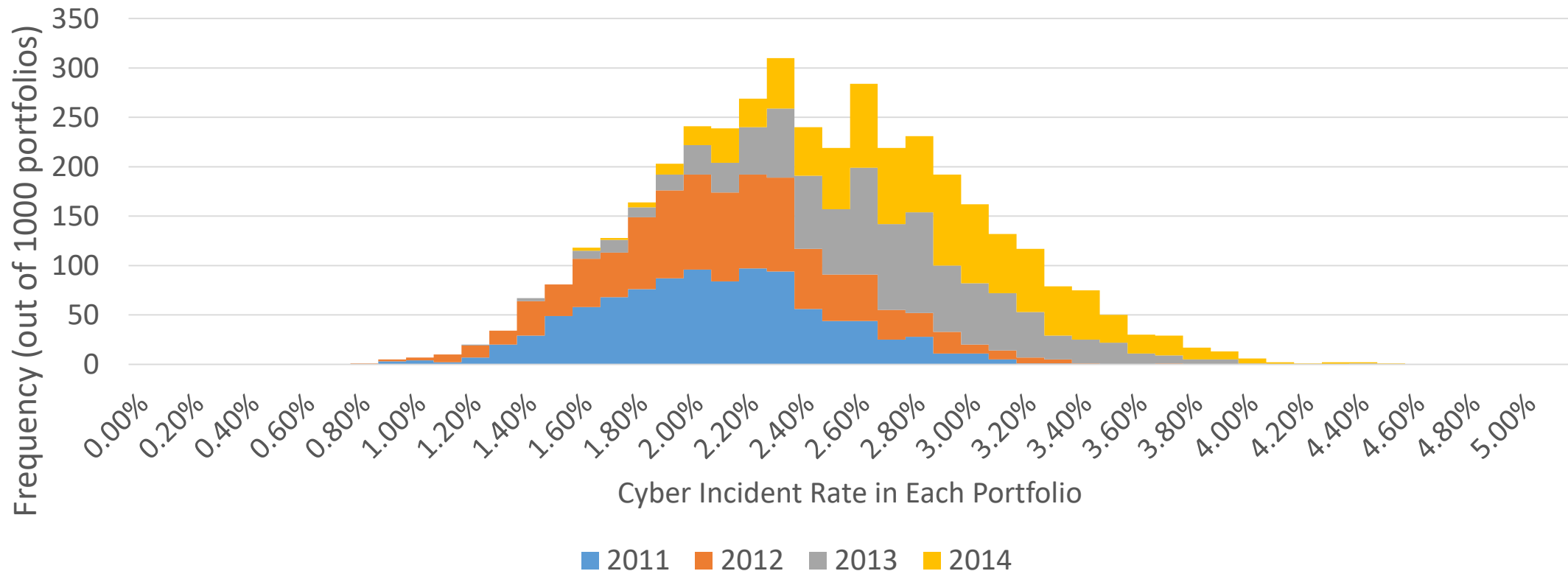


Claim Rate Estimation

- Methodology:
 - Randomly sampling 1,000 companies from the list to form a portfolio of policyholders
 - Assuming each company has the same likelihood of purchasing cyber-insurance
 - Repeat the process a 1,000 times to create 1,000 portfolios.
 - Looking up the companies from each portfolios in the Advisen's database to see how many of them have cyber incidents in a given year
 - We use data points from 2011 to 2014, since they have the best quality
 - Recording the cyber incident number for each portfolio. Since we have 1,000 portfolios in each year, we get a good distribution of portfolio risk in terms of claim counts.

Claim Rate Estimation – Results

Cyber incident rate in different years

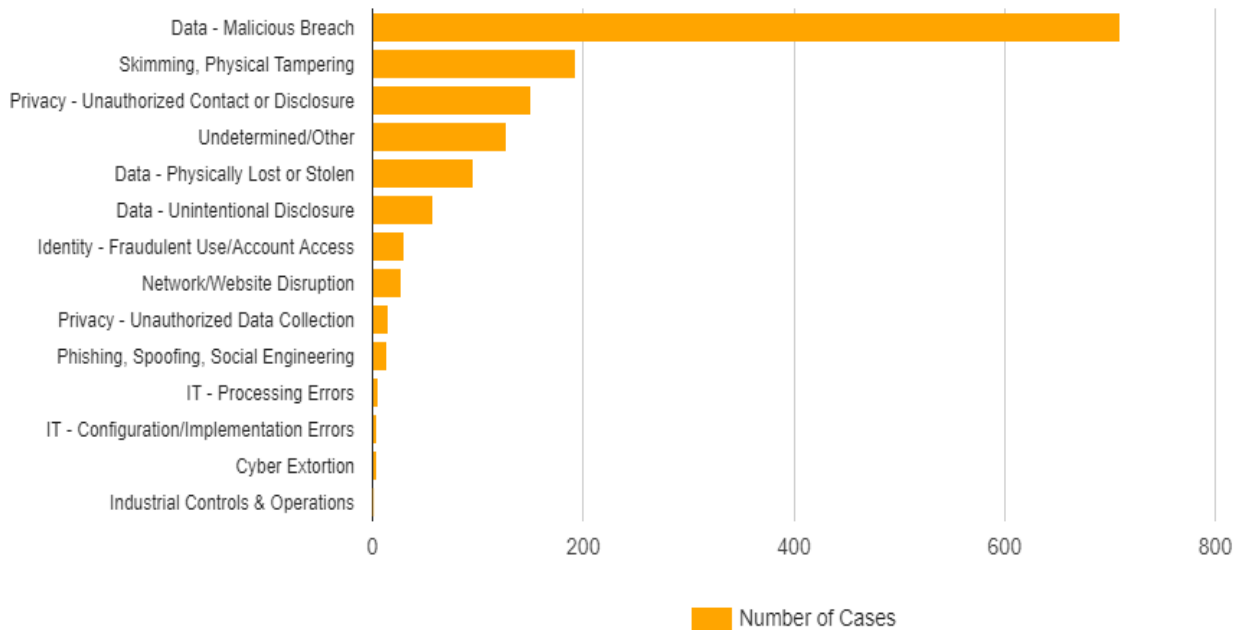


Claim Rate Estimation – Results (cont'd)

- Findings:
 - Portfolios typically have normally distributed claim rate
 - During the 4-year period from 2011 to 2014, the mean claim rate is 2.4% for public companies, and the standard deviation is 0.53%
 - The distribution is shifting to the right over time
 - 2% claim rate in 2011 vs. 3% in 2014
 - The variance is getting larger
 - 0.4% in 2011 vs. 0.47% in 2014
 - Insurer's portfolio risk is getting higher

Integrating CRISM with CIPAR

Cyber Incident Number in Food Sector across Different Incident Types



- Sector specific risk scores
- Exploitation of vulnerabilities are function of sector and company characteristics
- Update probabilities in CRISM's Bayesian attack graph with information of vulnerabilities exploited in targeted sectors
- Update portfolio risk profile in real time

Legal RISK

CLAD: Insurance Litigation

Analysis of Litigation Identifies the Current Legal Ambiguities

- Inconsistent legal standards aggravate the uncertainty within an already uncertain cyber insurance market.

Cyber Litigation Analytics Database (CLAD)

- Our research emphasized insurance litigation only
- We were able to collect more federal cases than state cases.

Duration	Federal	State
< 1 year	37	4
1-2 years	40	9
2-3 years	12	4
3-4 years	9	2
4+ years	4	2
N/A	2	5
Ongoing	14	2
Total	118	28

CLAD: Insurance Litigation (Cont.)

Frequently raised issues

- Issues raised by parties varied, but several occurred frequently. A majority of the cases involved exclusions, the duty to defend, and coverage for underlying litigation.

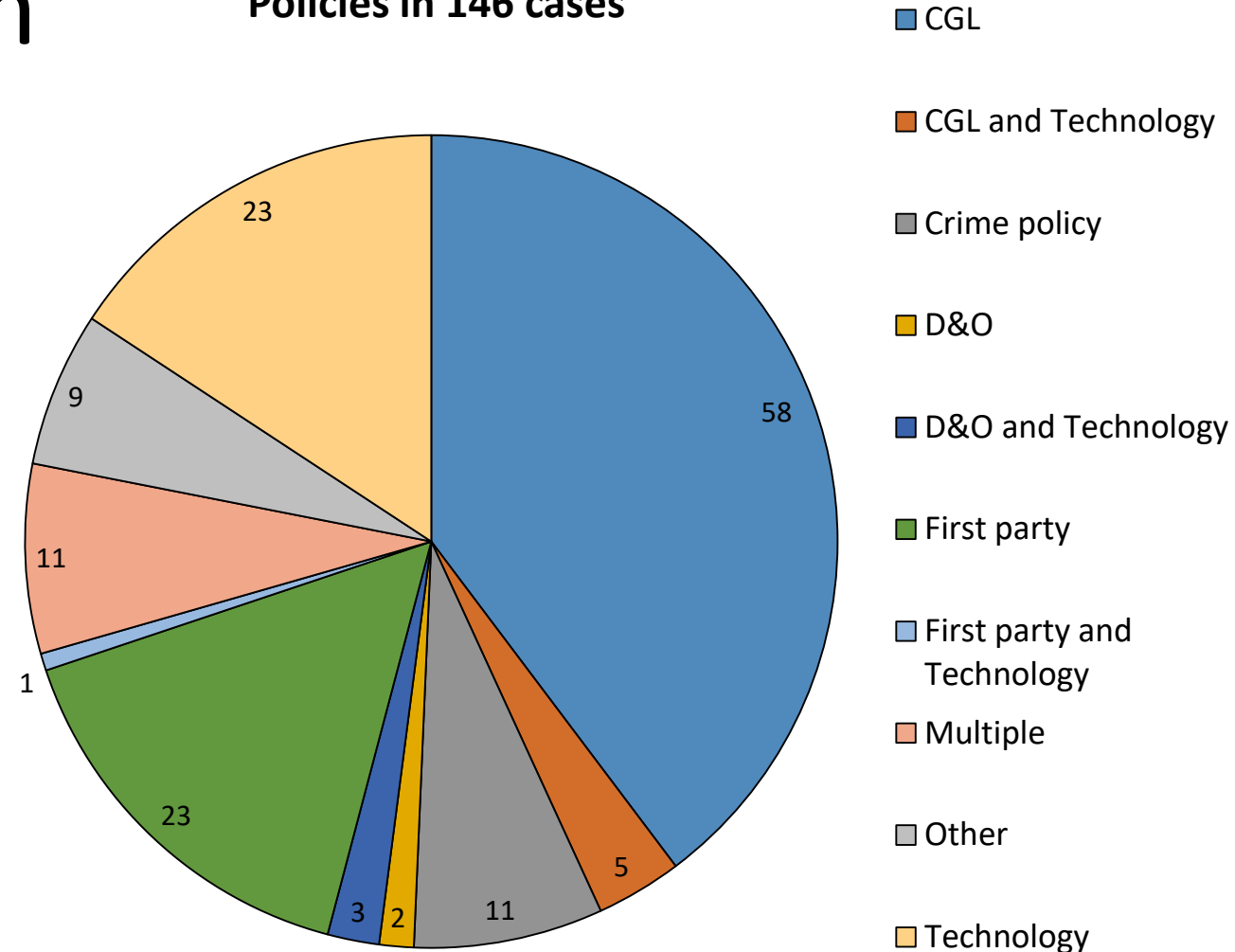
Jurisdiction	Exclusions Raised	Tangible Property and Damage	Occurrence	Causation	Duty to Defend	Publication	Presence of Underlying Suit
Federal	81	43	24	30	69	20	75
State	20	13	2	4	20	6	19
Total	101	56	26	34	89	26	94

CLAD: Insurance Litigation (Cont.)

Most of the Policies Were Not Cyber Policies

- A lot of the insurance litigation involved applying Commercial General Liability policies to digital harms.
- Many cases involved multiple policies.
- “Technology” policies included cyber insurance policies as well as technology errors and omissions.

Policies in 146 cases

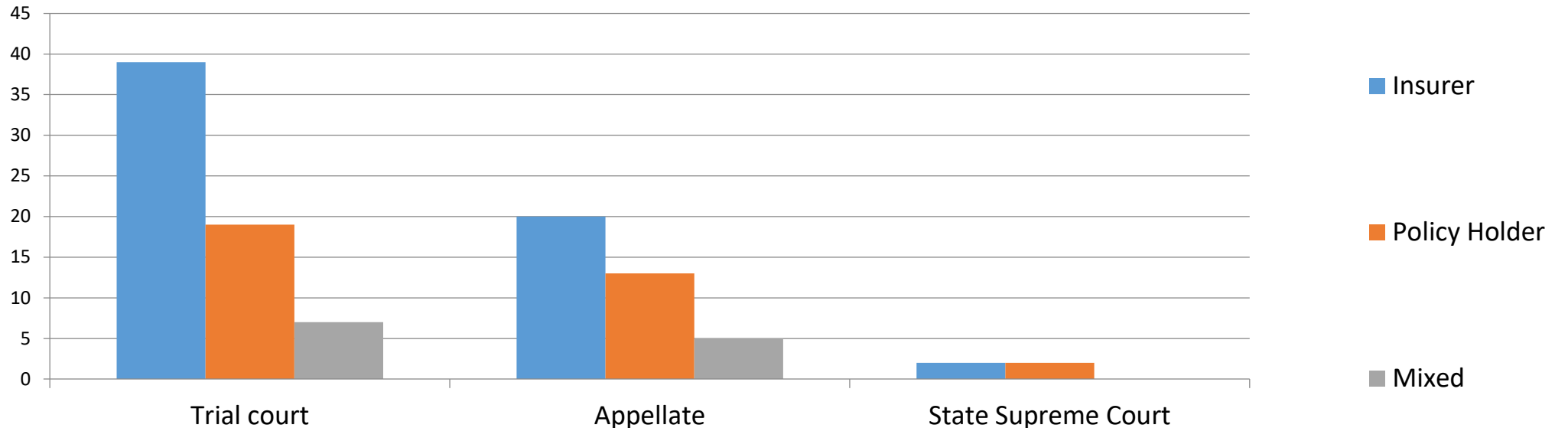


CLAD: Insurance Litigation (Cont.)

Insurers Prevail More Often at Trial Level

- But statistical regression analysis found that policy holders prevail more often on first party policies, while insurers prevail more often on third party policies
- 87% of cases which raised an issue about policy exclusions did not result in a settlement (p-value=0.03)

Outcomes by Court Level, n = 107



Future Research Topics

- How is a company's financial performance related to characteristics of the incident it experiences?
 - Positive correlation between the number of employees a company has and the magnitude of loss it suffers in a cyber incident.
 - More factors like this from the combined database (assets, revenues, etc.) can be examined
- How does a cyber incident affect a company's financial performance?
 - Changes in reputation, profitability, stock price and etc.
 - Changes in company's management style (risk management, investments in cybersecurity)
 - How long can the influence last

End User Engagement

- **Reliability First**
- **Sentara Health**

Thank You