CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Cyber Risk Assessment to Empower Cyber Insurance Markets

Jay P. Kesan, Ph.D., J.D.

Professor and H. Ross & Helen Workman Research Scholar
University of Illinois at Urbana-Champaign

kesan@illinois.edu

Linfeng Zhang

Research Associate
University of Illinois at Urbana-Champaign

lzhang18@illinois.edu

Background:

What problems are we addressing?

- Lack of sound cyber risk assessment – data, analyses, and metrics
- Large understanding gaps between directors and managers within organizations and between insured and insurers re. cyber risk
- Difficult for organizations to create optimal risk management plans or consider cyber insurance as a feasible risk management solution
- Organizations are often underprepared for cyber incidents
- Development of cyber insurance market is hindered

Background (cont'd):

How are we approaching it, and what makes our approach unique?

- Gathering extensive public and private data regarding known cyber incidents from multiple sources
- Performing extensive analyses on every important aspect of cyber risk, such as economic, financial, reputational and legal impact, to get more insights into cyber risk
- Uniqueness: Comprehensiveness of the multiple datasets we are building. Allows us to carry out research on important topics like the financial impact of cyber incidents that no prior studies have covered.

Background (cont'd):

Objectives/goals of the research:

- Develop data-driven cyber risk and resilience scoring metrics that enable cyber insurance carriers to both measure and improve risk and resilience associated with underwriting cyber liabilities
- Improve the resilience of infrastructure to known and unknown cyber attacks through the expansion of insurance coverage, but also by highlighting best practices for cyber risk mitigation as well as developing insights into the assessment and perception of cyber risks.

Cyber Risk Definition

- "operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems".
- Leading to various types of Incidents caused by different perils

1. Cyber Extortion
2. Data - Malicious Breach
3. Data - Physically Lost or Stolen
4. Data - Unintentional Disclosure
5. Denial of Service (DDOS)/System Disruption
6. Digital Breach/Identity Theft
7. Identity - Fraudulent Use/Account Access
8. Industrial Controls & Operations
9. IT - Configuration/Implementation Errors
10. IT - Processing Errors
11. Network/Website Disruption
12. Phishing, Spoofing, Social Engineering
13. Privacy - Unauthorized Contact or Disclosure
14. Privacy - Unauthorized Data Collection
15. Skimming, Physical Tampering

Cybersecurity Concern

- Cybersecurity is tied to the health of the U.S. economy. Malicious cyberattacks could throw the financial industry into chaos.
  - The World Economic Forum (based on McKinsey Report) estimates that ineffective cybersecurity may cost the world's economy $3 trillion in aggregate impact by 2020
- Cybersecurity is also national security. Critical infrastructure systems, from transportation to nuclear power, are vulnerable to cyberattacks.
  - Hospitals and police departments have been targeted with ransomware that severs access to vital information.
- Proper risk assessment and management can improve companies' resilience against cyber risks through market-based solutions
- The primary focus of our work is the private sector and on improving cyber security in the private sector through market-oriented solutions.

Cyber Incident Analysis

Better understanding of cyber risk

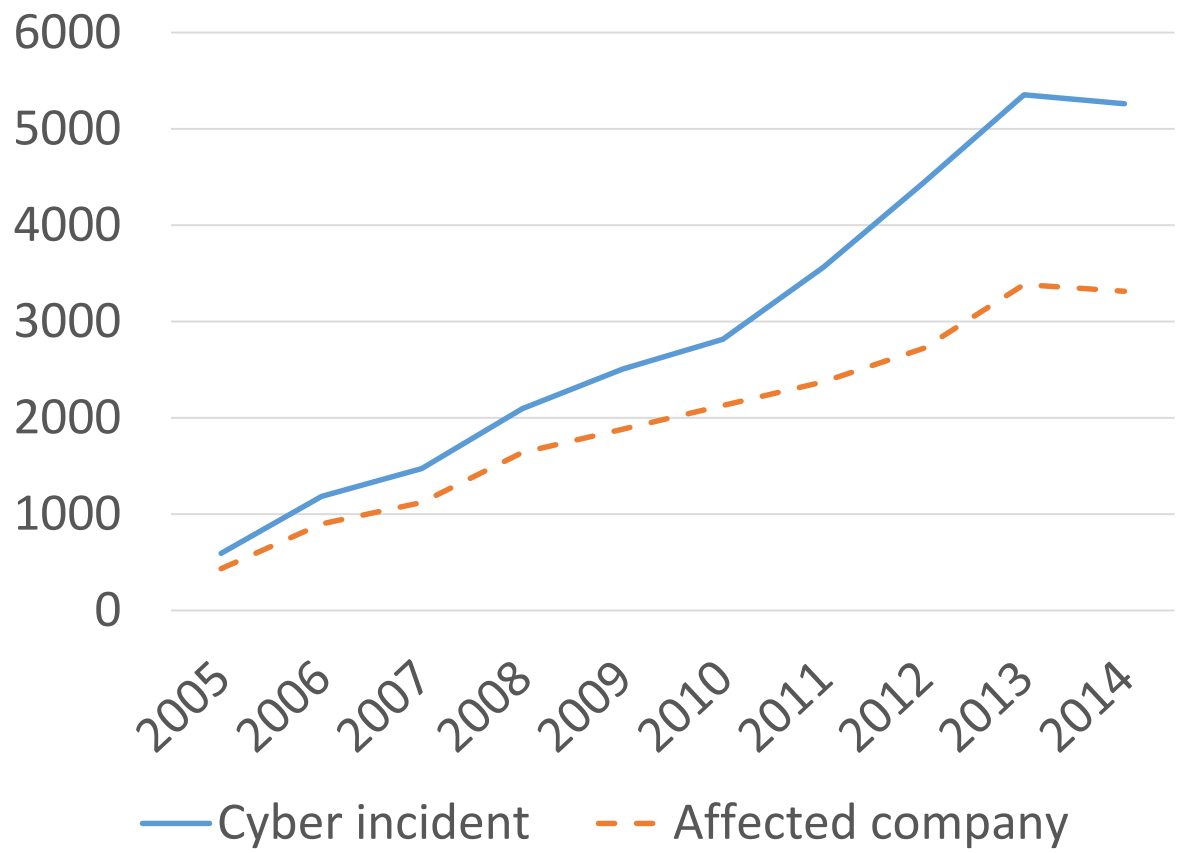
Data

- Analyzing over 40,000+ cyber incident records drawn from public data and private data (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

Trends in Cyber Risk

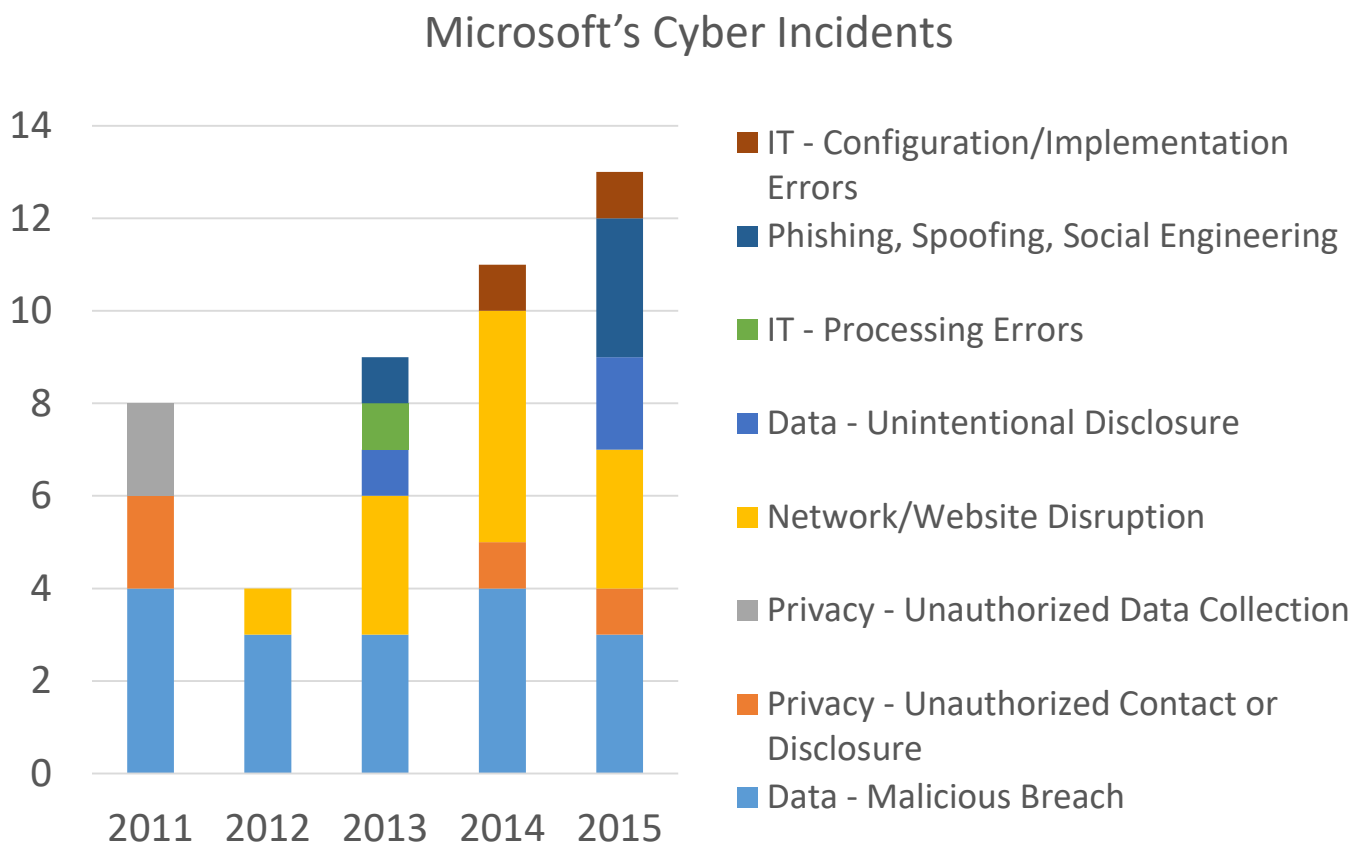
- During the 10-year period from 2005 to 2014:

1. Number of incidents have grown by 24.4% each year
2. Number of affected companies have increased by 22.5% each year
3. Incident/Company ratio has increased from 1.37 in 2005 to 1.59 in 2014, some companies are becoming more frequently affected by cyber incidents



Trends in Cyber Risk (cont'd)

- Investment in cybersecurity does not necessarily reduce the chance of having a incident
  - Microsoft Corporation spent $1 billion in cybersecurity in 2015, but the number of incidents it had in that year did not go down
  - Types of incidents are more diversified
  - More cyber risk derived from people risk (phishing, unintentional disclosure of data)



Cyber Risk Factors

- Three attributes of cyber risk
  - Hazards – what are the potential causes of incidents
  - Frequency – How often do cyber incidents occur
  - Severity – How large are the losses
- Hazards
  - Firms in different industries face different cyber threats, and firms in the same industry share similar risks
  - Industries having valuable data (e.g., financial industry) experience more data breaches
  - Firms in the same industry are vulnerable to similar attacks because of similar software or hardware setups (WannaCry and health care firms)

Cyber Risk Factors – Frequency

- Number of cyber incidents experienced by a firm in a certain time period
- Table shows data breach frequency experienced by individual firms from 2015 to 2017
- 1/10 of the firms had multiple incidents during the 3-year period
- Some firms are more frequently attacked than others

	All Companies	Companies with more than 1 incidents	Companies with more than 2 incidents
Count	1977	177	44
Incident (Malicious data breach) Number Descriptive Statistics			
Mean	1.1614	2.8023	5.2273
Standard Error	0.0216	0.2043	0.7107
Sample Variance	0.9228	7.3868	22.2262
Kurtosis	423.7810	54.6692	15.1725
Skewness	17.8550	6.8904	3.8503
Minimum	1	2	3
Maximum	26	26	26

Cyber Risk Factors – Frequency (cont'd)

- Dependent variable:
  - Number of data breaches experienced by individual firms during the 3-year period from 2015 to 2017
- Independent variable:
  - Firm size – log-scaled employee number as proxy
- Industry fix effects – 2-digit NAICS (North American Industry Classification System) code

	Estimate	Std. Error	t value	Pr(>|t|)	
log(employee)	0.0350	0.0076	4.6130	0.0000	***
(industry)11	0.8705	0.3594	2.4223	0.0155	*
(industry)21	0.7880	0.4762	1.6549	0.0981	.
(industry)22	0.7831	0.3384	2.3141	0.0208	***
(industry)51	1.4723	0.0903	16.3083	0.0000	***
(industry)52	0.9726	0.0775	12.5425	0.0000	***
…	…				
R^2	0.6094				
Degrees of Freedom	1929				

Cyber Risk Factors – Frequency (cont'd)

- 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

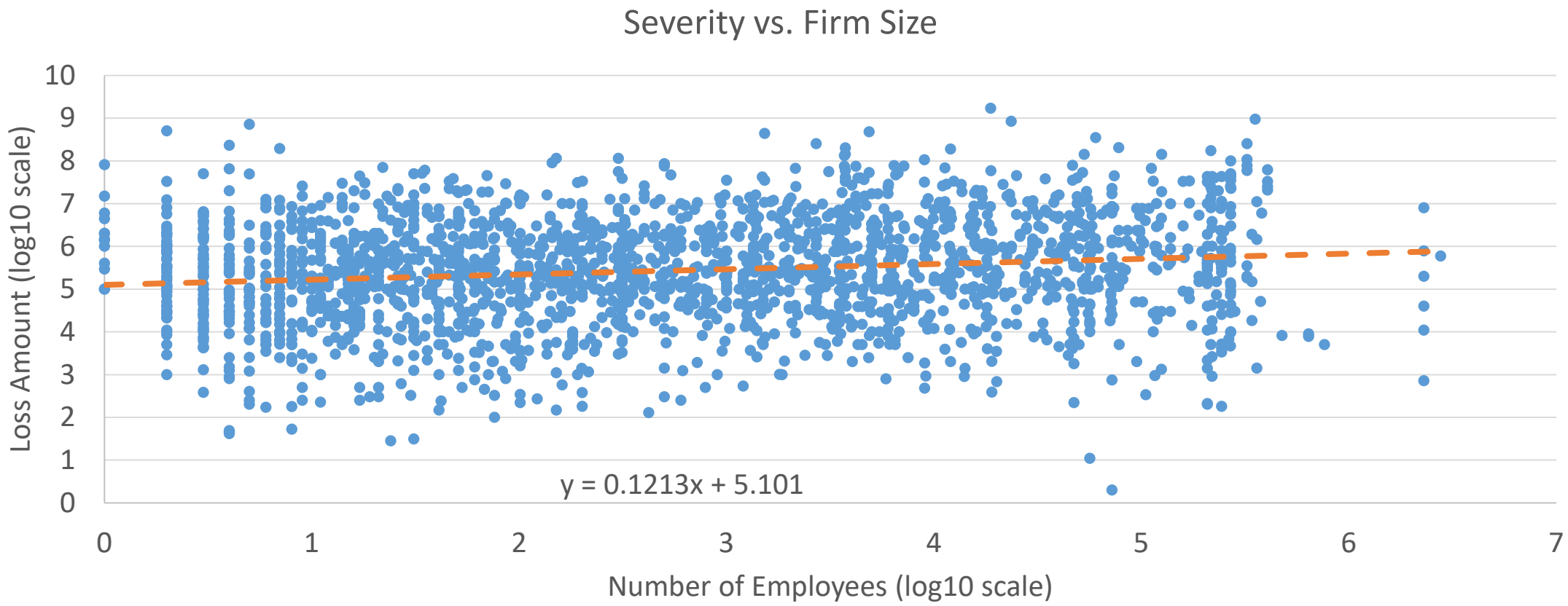
Industry	Coefficient	Standard Error
NAICS-51 Information	1.47	0.09
NAICS-52 Finance and Insurance	0.97	0.08

Cyber Risk Factors – Frequency (cont'd)

- Further analysis on how attack frequency varies across different industries
- Method: Pairwise t-test
- Most industries do not have different attack frequencies except industry-51 (Information Industry)
- Firms in information industry more often experience cyber incidents than firms in many 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	0.04	0.14	0.32	0.00	0.00	0.17	0.13	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	1.00	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	1.00	1	1	1							
56	1	1	1	1	1	1	1	1	1	1	1	1	0.01	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	0.98	1	1	1	1	1	1	1			
72	1	1	1	1	1	1	1	1	1	1	1	1	0.01	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	
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

Cyber Risk Factors – Severity



Cyber Risk Factors – Severity (cont'd)

- Data:
  - 8,413 malicious data breach incidents from 2001 to 2017
- Dependent variable
  - Severity – log10-scaled number of records breached in a data breach incident as proxy
- Independent variable
  - Firms size – log10-scaled employee number
- Control for industry-year fixed effects

	Estimate	Std. Error	t value	Pr(>|t|)	
log10(company_size)	0.1627	0.0144	11.322	0.0000	***
R^2	0.7047				
Degrees of Freedom	8090				

Cyber Risk Factors – Severity (cont'd)

- Firm size has a statistically significant coefficient of 0.1627
- In the same year and same industry, larger firms breach more records
- 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	
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

Bridging Causes and Outcomes

Cyber Incident Outcomes

- Firms with certain characteristics are more vulnerable to some attacks, how does it imply what outcomes to expect
- 15 types of cyber incidents caused by different perils
- Leading to various types of outcomes

First party losses	Third party liabilities
• Properties damaged or lost in cyber incidents • Direct financial damages (e.g., paid ransom) • Defense costs in lawsuits • Fines and penalties, which are paid by the company for violating regulations.	• Physical injuries • Property damage • Loss of assets other than property • Loss of wages • Loss of business income • Loss of life • Pain and suffering • Plaintiff legal fees generated from lawsuits

More Foreseeable Outcomes

- Given the fact that although some incidents have different causes, they are similar in terms of the types of losses that they result in, we try to group together different incident types with such similarities
- Creating larger samples
  - Very small sample sizes for some categories in original dataset, (e.g., only 8 records for DDoS incidents), is impractical for statistical analysis
- Generating a clearer path from cause of cyber incident to the outcome
  - Helping firms determining which cyber insurance coverages to buy
  - Making losses more foreseeable for insurers

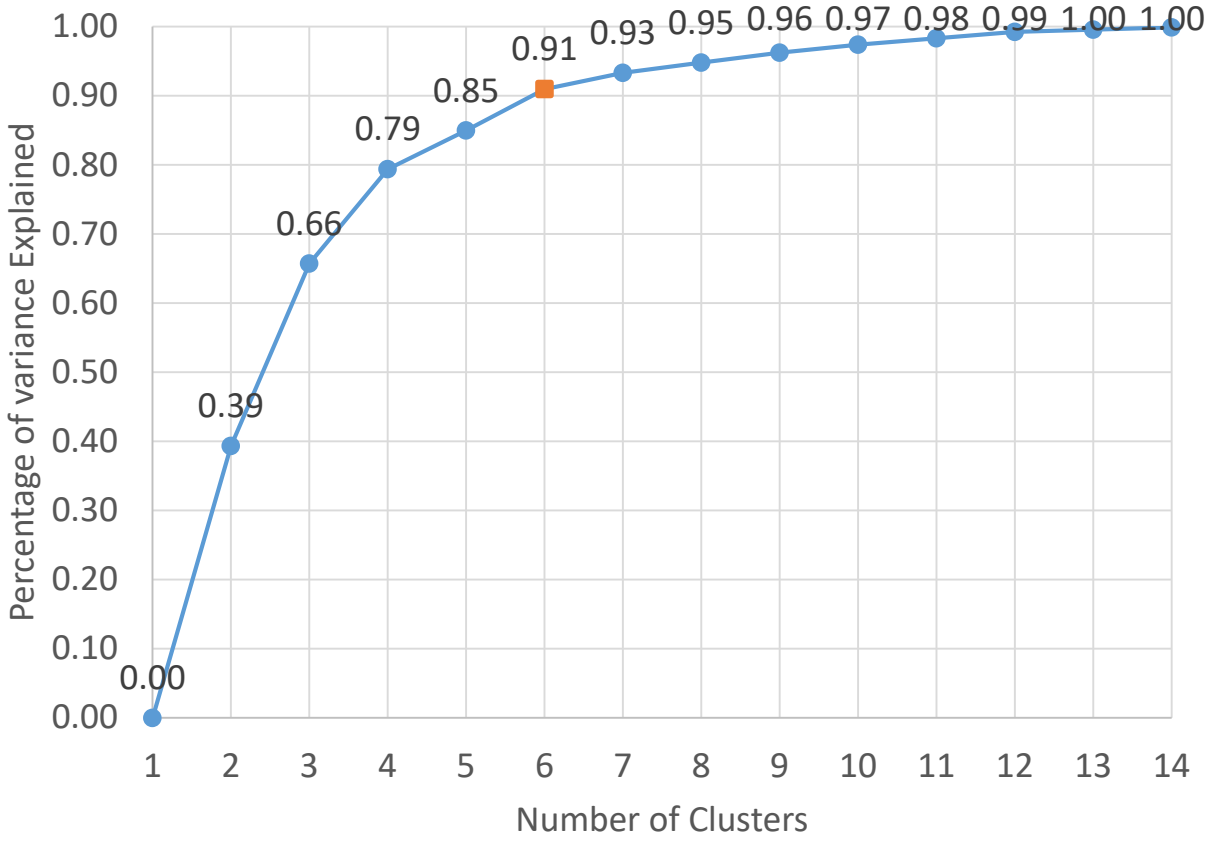
Incident Type Clustering

- First, we calculate the frequencies of different outcomes for each type of incident
- As an example, for malicious data breach incidents
  - 57.10% of them cause financial damages
  - 0.63% of them cause 3rd party property damages
  - Etc.

Data - Malicious Breach	
Outcomes	Frequency
Financial damages	57.10%
Property 3rd party	0.63%
Loss of assets	2.37%
Loss of business income	2.37%
Other	14.83%
Other fines penalties	22.56%
Pain and suffering	0.16%
Plaintiff legal fees expenses	6.47%
Property 1st party	1.42%
Punitive exemplary damages	0.63%
Other expenses	0.00%
Other multiplied damages	0.00%
Defense costs	0.00%
Loss of life	0.00%
Loss of wages	0.00%

Incident Type Clustering (cont'd)

- We use k-means clustering method based on Euclidean distance
- We group together incident types rather than incidents themselves because we need to preserve the cause information
- The elbow method suggests a cluster number of 6 would be sufficient
  - 91% of within-cluster variance explained (PoVE)
  - Slow increase in PoVE after 6



6 Types of outcomes

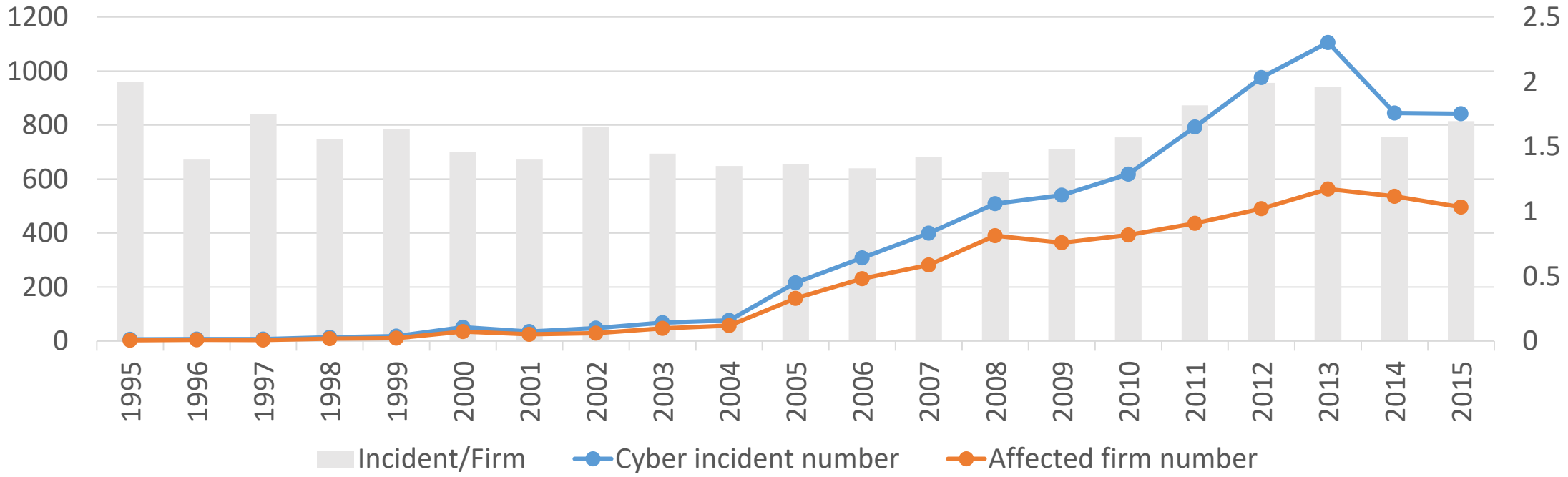
- 5-level scale indicating likelihood of having the type of loss

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

Industry-wise Cyber Risk Assessment

Maritime Industry

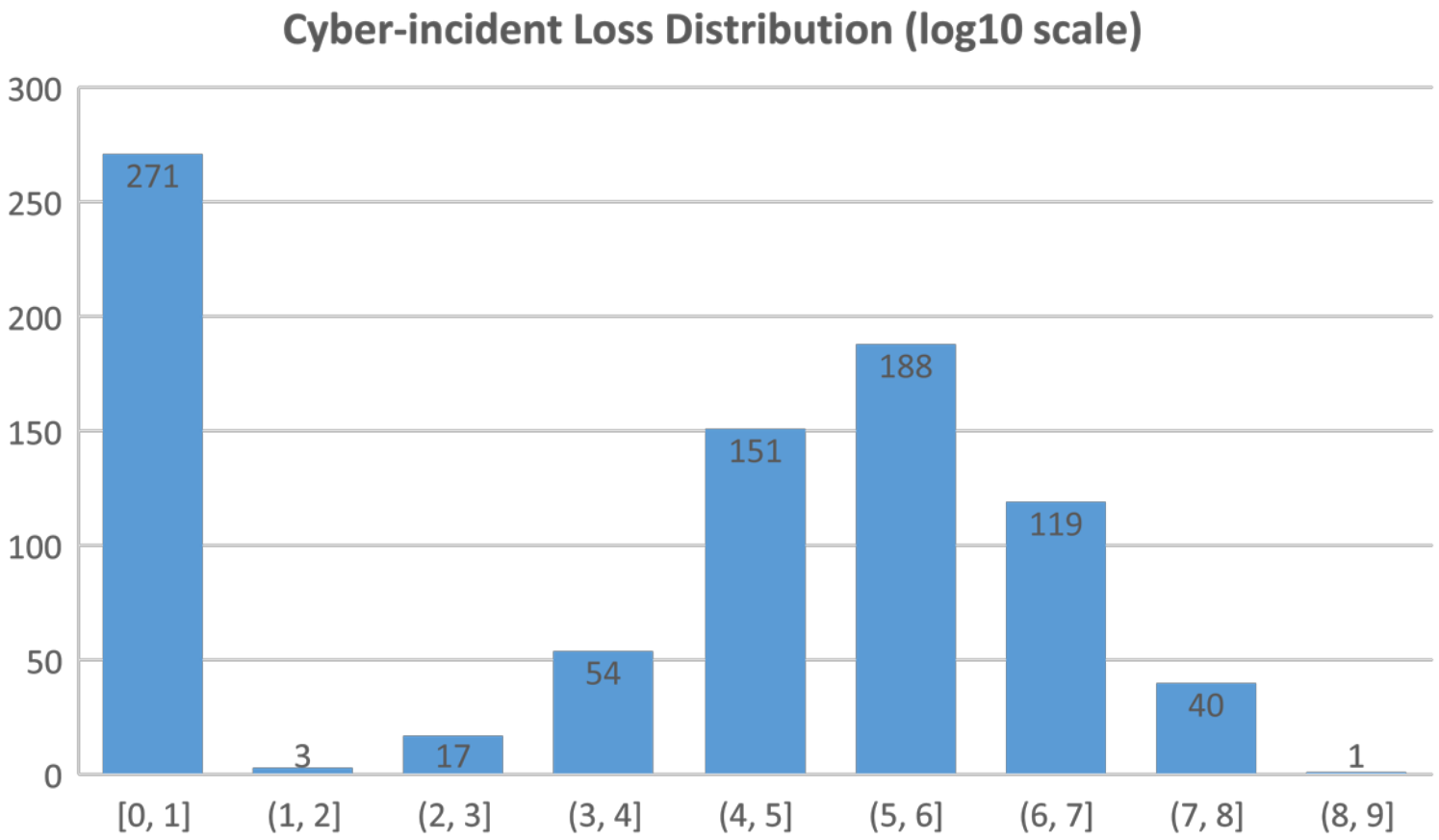
Cyber Risk over Time



- Both number of cyber-incidents and number of affected firms are growing
- Incident/firm ratio is relatively stable over time (i.e. cyber risk within individual firms is not increasing)

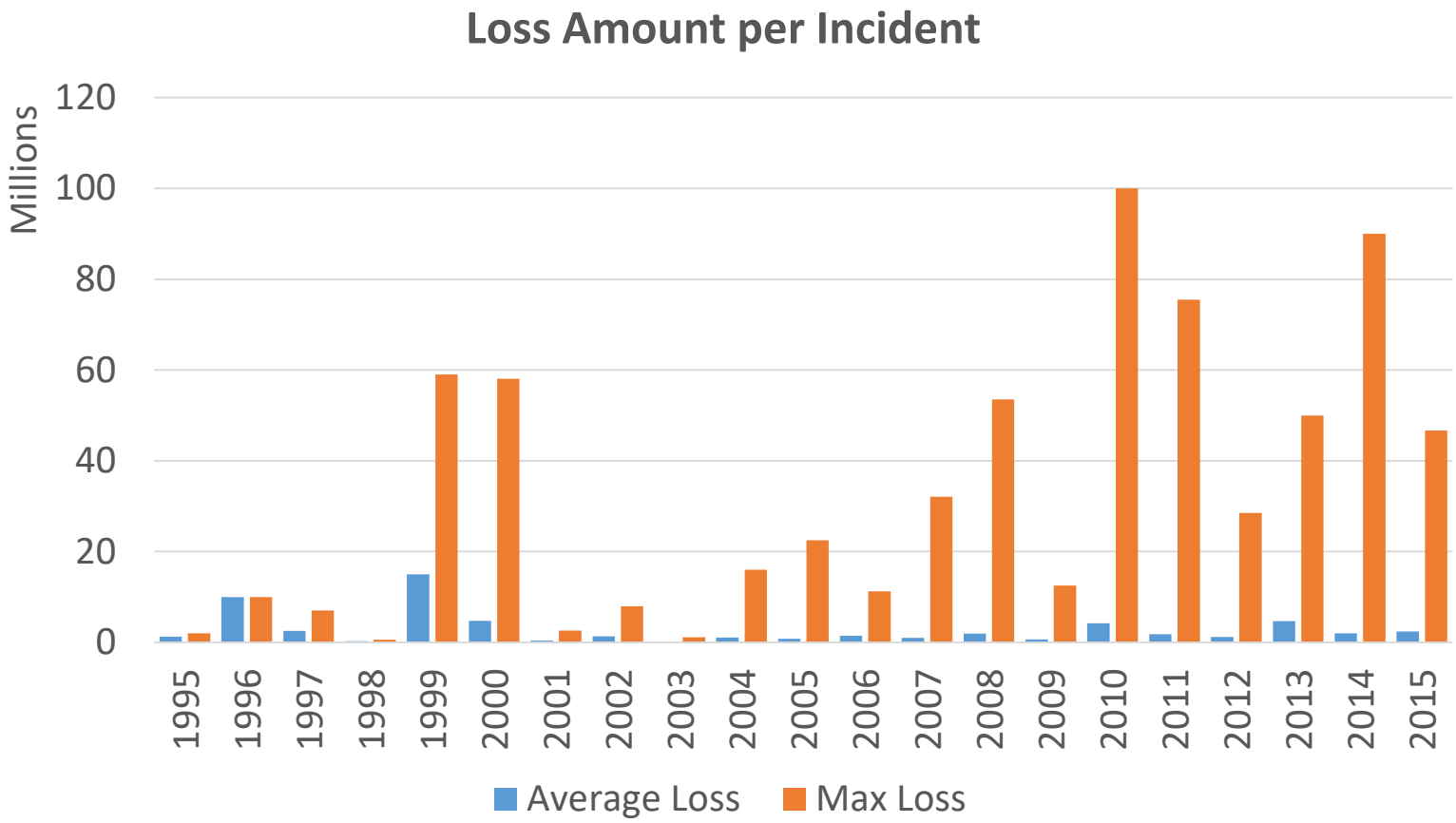
Cyber Incident Losses

- The average loss amount of all cyber-incidents is 2.15 million
- Around 1/3 (271/844) of the cyber-incidents in maritime industry do not result in losses.
- The losses typically range from 10 thousand to 10 million
- Losses can be as large as 100 million



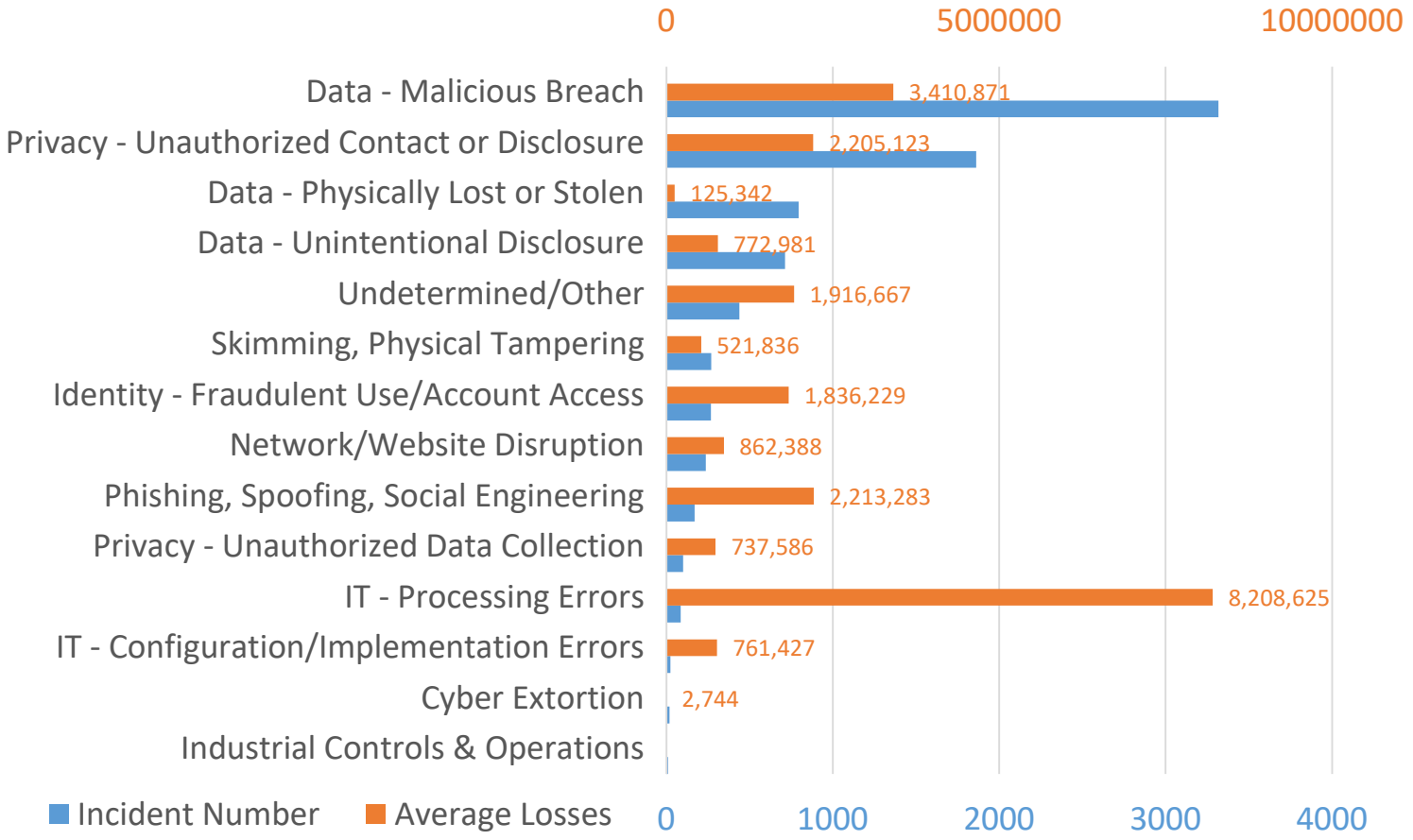
Cyber Incident Losses (cont'd)

- 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



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



Highlights of Cyber Risk in Maritime Industry

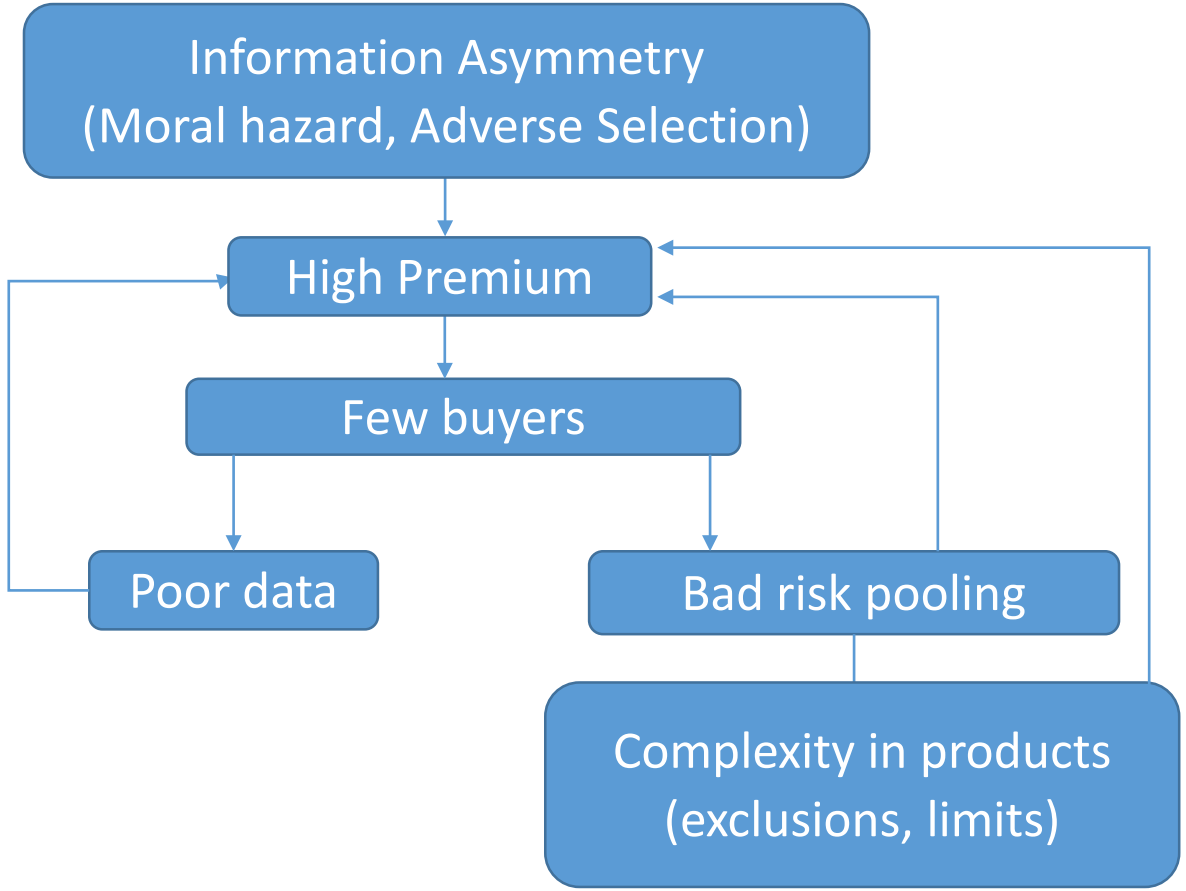
- From previous analyses of cyber risk in maritime industry, we find:
  - More firms are being affected by cyber incidents
  - Malicious data breach is the biggest threat to this industry in terms of loss frequency and severity, and IT process errors can lead to very large losses
  - The incident frequency of individual firms roughly remains the same over the years, while the potential maximum loss from a single incident is getting higher
- 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

Insurance for Cyber Risk Management

Cyber Insurance

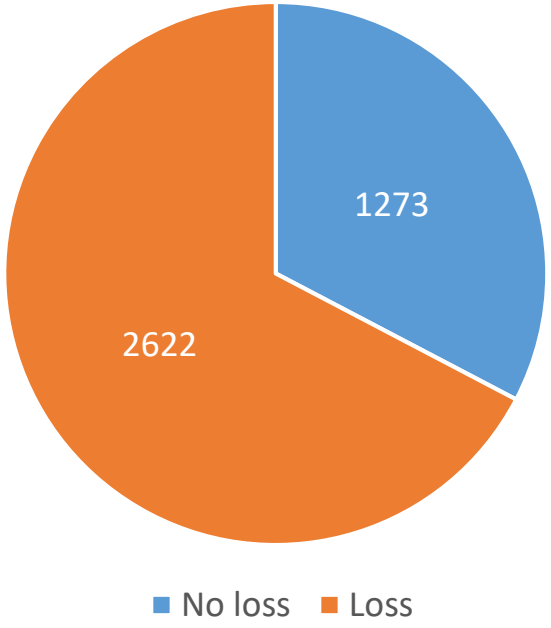
- Cyber insurance is a risk transference vehicle
  - Complement to cybersecurity enhancement
  - Help insured businesses quickly recover from cyber incidents
- The market is still in its infancy
  - U.S. penetration level of insureds is less than 15% (less than 1% in other regions)
  - Less than 5% of small and medium sized businesses purchase cyber insurance in the U.S.
- The market is growing fast
  - $1.7 billion written premium in 2015
  - 30% annual growth rate since 2011

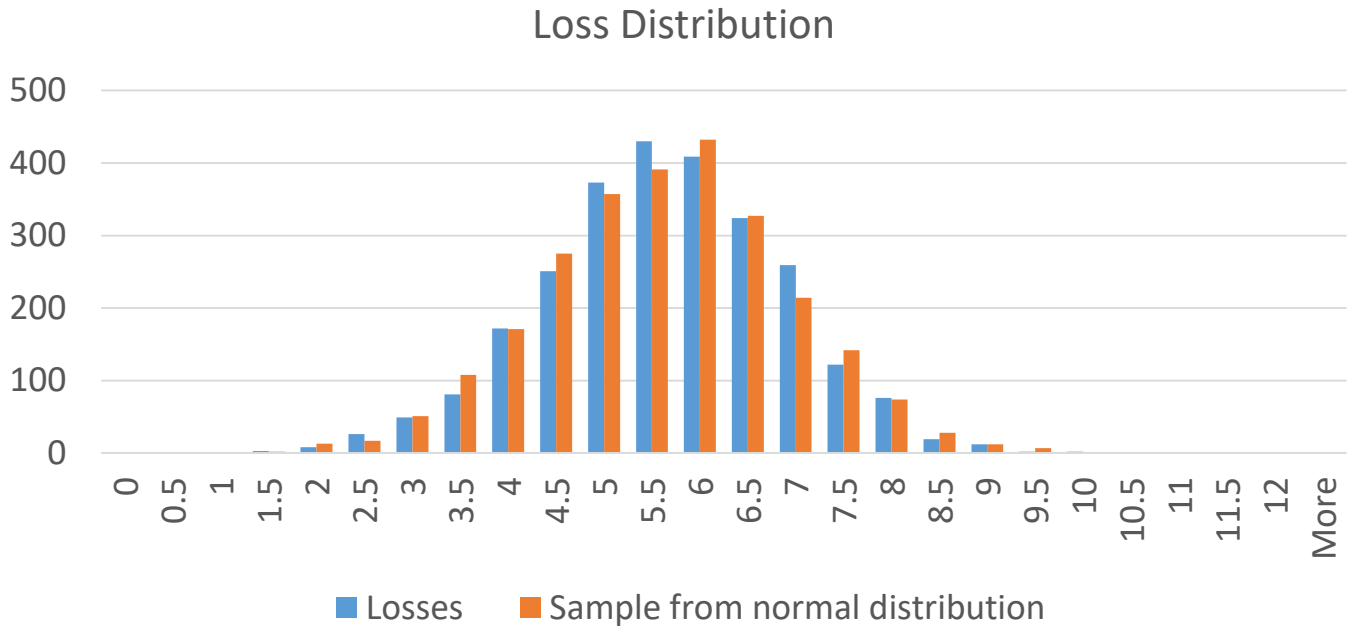
Issues with Cyber Insurance Market



Insurer's Portfolio Risk Assessment

Loss Distribution





- 3,895 loss amounts are recorded in Advisen's dataset
- About 1/3 (1273/3895 = 32.7%) of the cyber incidents do not result in any measurable losses
- The log10-scaled losses follows a normal distribution with mean 5.41 and standard deviation 1.25

Claim Rate Estimation

- Objective:
  - Estimate the cyber incident rate in a group of companies (i.e., number of cyber incidents per company in a given period)
  - In an insurance setting, number of possible claims arising from a pool of policyholders
- Assumptions:
  - Every incident results in a claim
  - Claims are all covered.
  - Portfolios are static (not changing in different years)
  - This analysis can be seen as the worst scenario; in actual insurer's portfolio, the rate is expected to be lower

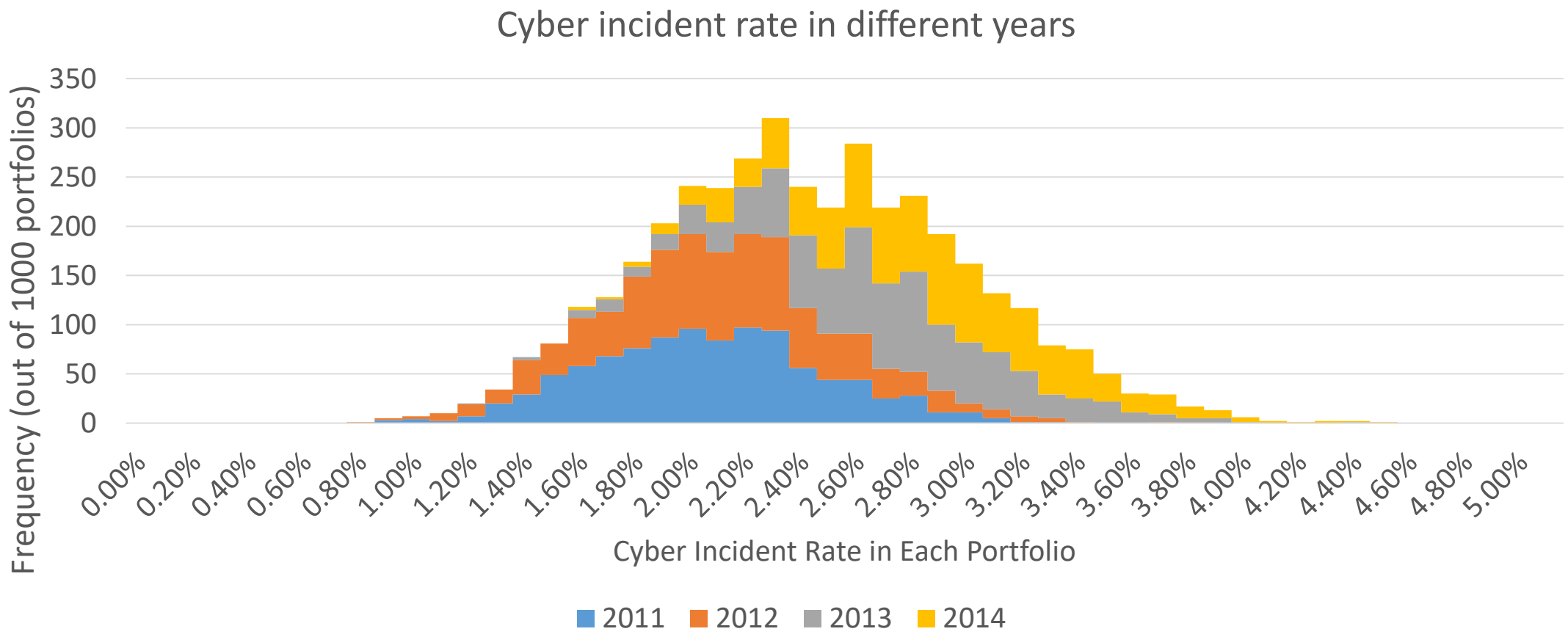
Claim Rate Estimation (cont'd)

- Data:
  - Generate a list of publicly traded companies in the U.S.
  - We choose public companies because their information can be easily obtained, and we know the population size
  - Cyber insurance has a relatively higher penetration level among public companies, so in actual insurer's portfolios, we would expect to see lots of public companies as policyholders
  - Further research will be carried out on whether public and private companies have different risk characteristics in terms of cyber-security
  - Exchanges we considered include Nasdaq, NYSE and AMEX
  - 5,700+ companies in total after removing duplications
  - Different classes of stock or different divisions from the same company are seen as duplications.
  - 6,600+ companies before removal

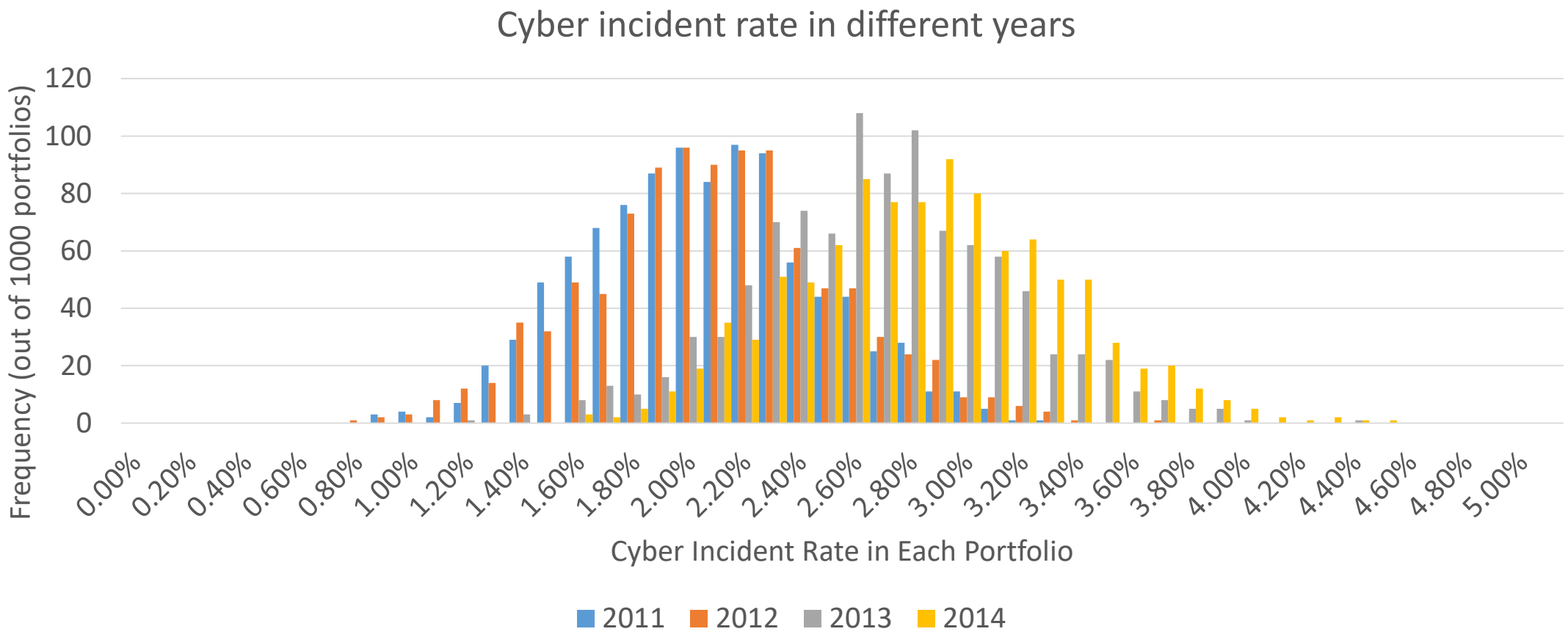
Claim Rate Estimation (cont'd)

- 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 1000 portfolios in each year, we get a good distribution of portfolio risk in terms of claim counts.

Claim Rate Estimation – Results



Claim Rate Estimation – Results (cont'd)



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

CIPAR

Cyber **I**nsurance **P**ortfolio **A**nalysis of **R**isk

CIPAR

- A web-based cyber risk assessment tool built upon our data and analyses
- Giving firms from all market segments an easy way to estimate their exposure to cyber risk
- Helping cyber insurance carriers manage portfolio risk more efficiently and improve product pricing
- Cyber incident look-up
- Key features:
  - Cyber incident lookup
  - Cyber risk data visualization
  - Cyber risk scores based on firm characteristics
- Demo

Cyber Incident and Corporate Finance

Combined Database

- We link cyber incident data with Compustat, a database widely used in corporate finance analysis
- Few studies try to explore the relation between cyber incidents and the fundamentals of victim firms
- With the combined data, we are going to study a number of interesting research questions
  - What corporate financial factors affect the frequency of cyber incidents?
  - Does it matter how a firm is positioned at the time of a cyber incident?
  - How big is the impact of cyber incidents on firms?
  - What are the types of impact – change in stock prices, loss of reputation, etc…
- Helping firms better prepare for cyber incidents and letting insurers better assess insureds' risks

Combined Database (cont'd)

- 4,820 records in data base
- Each record has:
  - Cyber incident information
  - All recorded quarterly financial statement items of the victim company
  - Stock price information
  - Each financial statement has two time stamps indicating:
    1. If it is prior to the incident occurrence date
    2. If it is prior to the first reported date of incident
- Ongoing research with the combined database:
  - The reputational loss after a data breach takes place

Studies on Reputational Losses

- Data:
  - 4,820 records in the combined database
  - Time stamp 2 (the date when an incident was first known to the public) is used
  - Based on these dates, we search for the last quarterly earnings before the incident, and subsequent quarterly earnings reports after the incident (discarding the ones with missing quarterly reports)
  - To have a better control on the length of time between the date of incident and the date of next earnings, we divide these incidents into three groups:
    - Taking place 2-3 months before the next earnings
    - Taking place 1-2 months before the next earnings
    - Taking place 0-1 months before the next earnings

Studies on Reputational Losses (cont'd)

- Methodology
  - Goodwill as the proxy for reputation:
    - Usually only has book value in mergers and acquisitions
    - Represents the amount of money that buyer is willing to pay for a company's good name
    - But we try to estimate it with excess earnings method, a common practice in accounting
    - Because we only care about the change value in goodwill, some issues with this method, such as choosing a proper capitalization rate is negligible
  - Other indicators as alternative references
    - Earnings quality & Market to book ratio
  - Control group – Other companies in the same industry which have similar characteristics but do not have cyber incidents in the same period
    - Industry-wise effects (e.g., holiday season in retail industry)

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

Recognizing the Team

Jay Kesan (PI)
Professor, Law & ECE,
University of Illinois

Linfeng Zhang
Res. Associate, University of Illinois

Carol Hayes
Postdoc, University of Illinois

Sachin Shetty (Co-PI)
Associate Professor, Virginia Modeling, Analysis and Simulation Center, Old Dominion University

David M. Nicol (Co-PI)
Professor, ECE, University of Illinois