Cyber Risk and Assessment

An Insurance Industry and Market Perspective

CENTER FOR INSURANCE POLICY AND RESEARCH

NAIC 2023 FALL NATIONAL MEETING

SUNDAY, DECEMBER 3RD
2:00 PM – 3:30 PM (ET)

AGENDA

1) Broad assessment of insurance industry cybersecurity loss events over the past decade (20 minutes)

    (CIPR)

2) Discuss insurance industry loss events in wider context as well as ongoing NAIC initiatives and best practices aimed at curbing the frequency and impact of such cybersecurity loss events (30 minutes)

    (Jim Blinn, Zywave)

    (Cynthia Amann, Missouri Department of Commerce & Insurance)

---

3) Cyber modeling landscape and application (30 minutes)

    (Rebecca Bole, CyberCube)

    (Shaveta Gupta, NAIC CAT COE)

CYBER HEADLINES

Arthur J. Gallagher targeted in class action lawsuit based on 2020 ransomware attack

Chubb hit by a Maze ransomware attack in March 2020

Geico reported in April 2021, customer stolen license numbers possibly used to apply for fraudulent unemployment benefits

CNA paid $40 million in late March 2021 to hackers

(Source: Insurance Journal, Jan. 5, 2022, https://www.insurancejournal.com/news/2022/01/05/647530.htm)

Alleged Funeral Insurance Services Robocalls Gets Allstate Affiliate National General Into TCPA Hot Water

(Source: https://www.natlawreview.com/article/tcpaworld-after-dark-alleged-funeral-insurance-services-robocalls-gets-allstate)

Health Insurance Associates agreed to pay $990,000 to resolve claims that it violated the Telephone Consumer Protection Act (TCPA) with unsolicited telemarketing calls.

(Source: https://topclassactions.com/lawsuit-settlements/closed-settlements/health-insurance-associates-telemarketing-calls-990k-class-action-settlement/

MORE CYBER HEADLINES

The long list of companies hit by the global MOVEit hack has grown further with the addition of insurance provider Genworth, whose millions of customers and agents combined are affected – up to 2.7 million individuals affected.

https://www.insurancebusinessmag.com/us/news/cyber/genworth-outlines-massive-hit-from-global-moveit-hack-450435.aspx

Other 2023 high profile incidents:

Managed Care of North America (MCNA) Dental– March data breach that compromised data of almost nine million patients;

Progressive – May, one of its third-party vendors has fallen victim to a data breach that impacted about 347,000 customers;

CareSource – May, more than three million customers to have their personal data compromised;

Prudential & New York Life– May, more than 345,000 customer accounts were impacted by MOVEit hack;

American Family – October cyberattack shutting down IT systems;

https://www.insurancebusinessmag.com/us/guides/the-insurance-industry-cyber-crime-report-recent-attacks-on-insurance-businesses-448429.aspx#:~:text=In%20a%20notification%20letter%20dated,personal%20information%20accessed%20by%20hackers.

RESEARCH OBJECTIVE

But what do we know about the objective cybersecurity risk across the entire insurance industry over time?

- Access and analyze industry recognized proprietary cyber loss dataset
- Merging NAIC data points and survey information to create a unique modeling set for descriptive and statistical analysis
- Share and leverage findings with NAIC regulators

MAIN RESULTS

- Between 2012 and 2022, over **541 insurance companies** suffered a known cyber loss event, with an **average of 233 cyber loss events** transpiring each year.
- Cyber events potentially impact **both market conduct and financial solvency** areas of regulation.
- The likelihood of experiencing a malicious cyber event increases as **firm visibility increases.**
- The likelihood of experiencing a malicious cyber event increases as **firm performance decreases.**

OUR DATA UNIVERSE - SOURCE

- **Data source: Zywave Data Set** (f/k/a Advisen)
- **Cyber loss events accessed from a variety of sources**

  Government: SEC, FTC, FCC, Homeland Security, State FOIA requests, Int'l sources

  Litigation: Official court records, plaintiff attorney websites, litigation sources

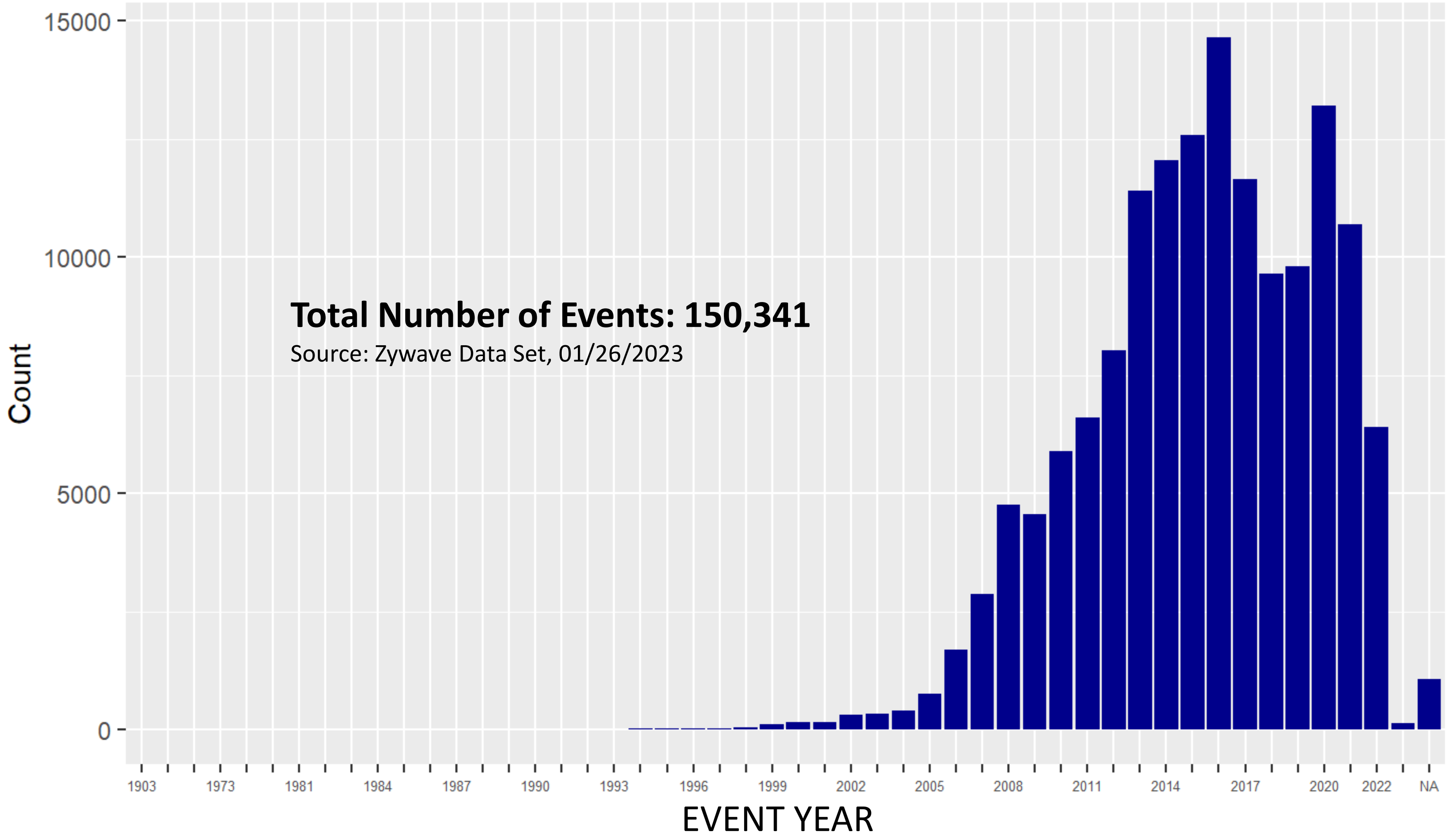
  News: Key-word based alerts

  Company: S&P, D&B

- **Timeframe**
  - Events range from 1953 – 2022
  - Analysis range from 2012 – 2022
  - Lag time from event creation and case updates can be considerable

HISTORICAL VIEW OF EVENTS - ALL GLOBAL COMPANIES

All Event Counts, All Years



Total Number of Events: 150,341

Source: Zywave Data Set, 01/26/2023

OUR DATA UNIVERSE – LOSS EVENTS

What is being tracked?

Events –An event is any risk of financial or physical loss, disruption of services, privacy violation, or damage to the assets or reputation of an organization through **either** a failure of its information or technology systems, **or** a malicious act affecting their information or technology systems.

Events may result in significant financial loss to or judgments against corporate entities.

- Data-- Unintentional Disclosure
- Data– Physically Lost or Stolen
- IT Configuration, Implementation Errors
- Privacy Unauthorized Contact or Disclosure
- Phishing, Spoofing, Social Engineering
- Data– Malicious Breach

ISOLATING U.S. INSURANCE COMPANIES

All U.S.

124,589
events

TIME PERIOD:
2012 - 2022

All U.S. Insurance Related*

2,050
Zywave companies

All U.S. Insurance Related*

4,475
events

***SIC Codes 63 & 64**

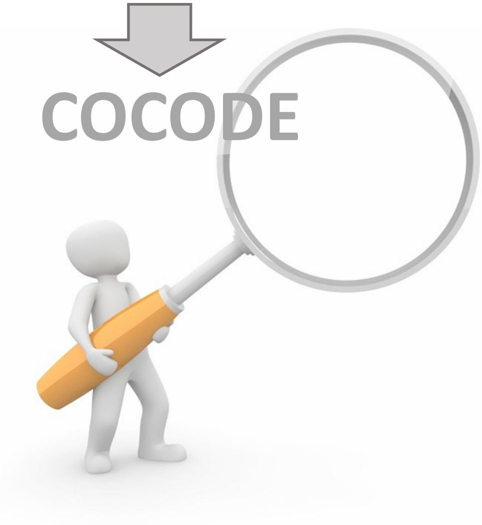
Zywave ID

↓

FEIN / Name / Event Description /State of Domicile

↓

COCODE



NAIC Matched Insurers

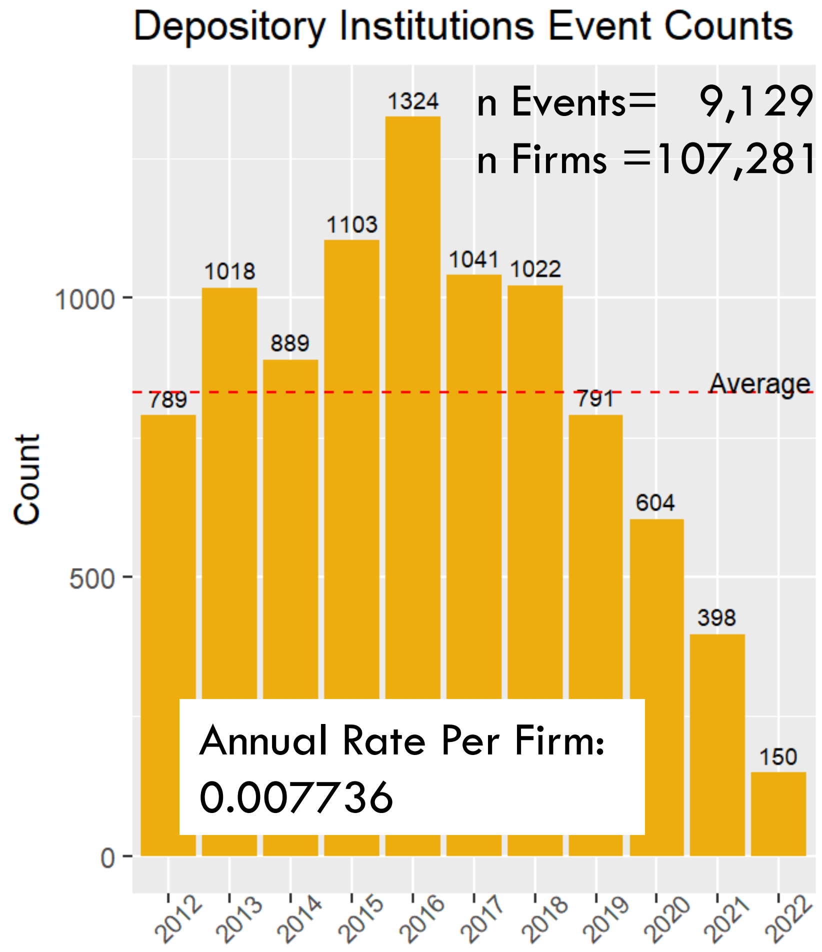
541
NAIC companies

NAIC Matched Insurers

2,566
events

Source: **Zywave data set, Jan 26, 2023**
NAIC FDR

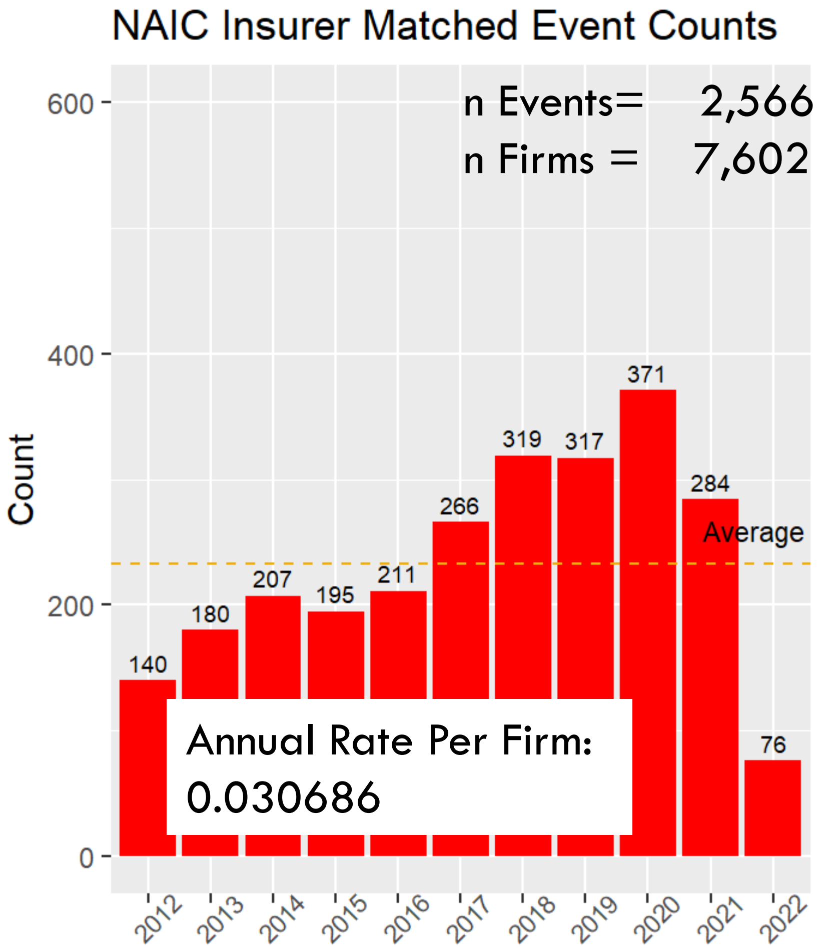
INSURANCE EVENTS OVER TIME (2012-2022)



Depository Institutions Event Counts

n Events= 9,129
n Firms =107,281

Annual Rate Per Firm:
0.007736



NAIC Insurer Matched Event Counts

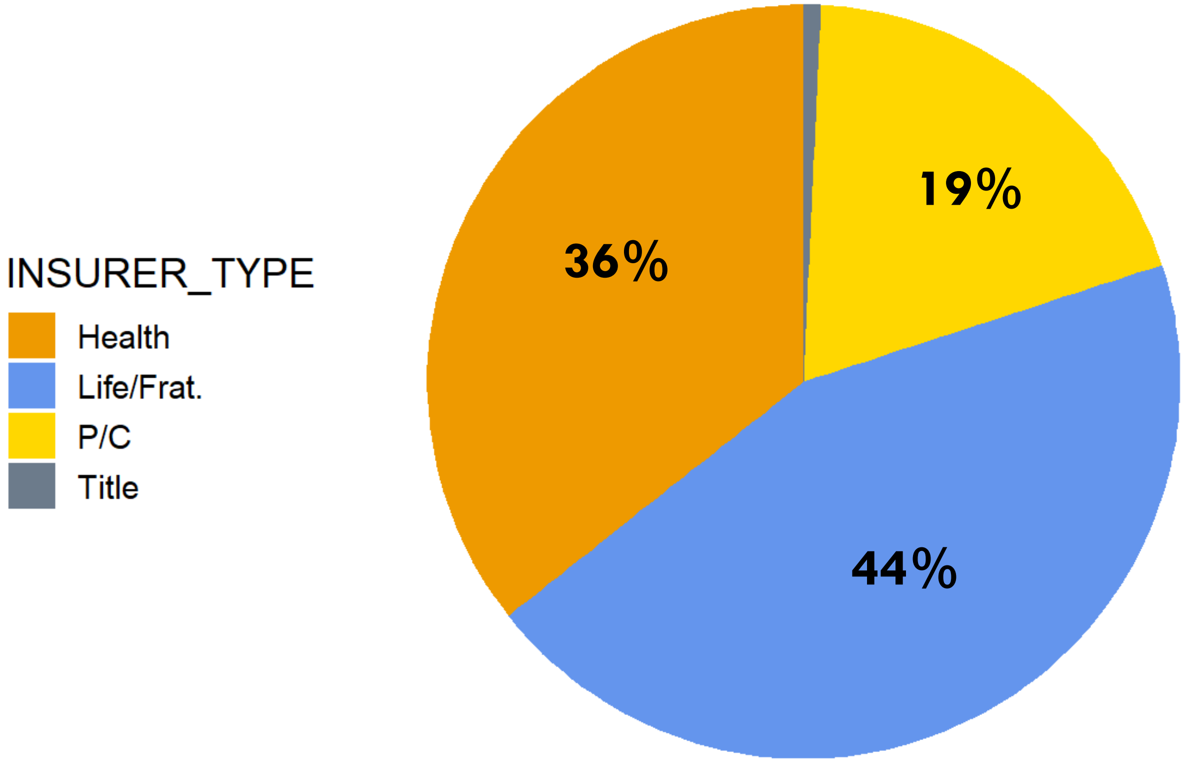
n Events= 2,566
n Firms = 7,602

Annual Rate Per Firm:
0.030686

Roughly, insurance companies are 4x more likely than a depository institution to experience a cyber event.

Source: Zywave data set, Jan. 26, 2023; NAIC FDR; SICCODE.com

EVENT FREQUENCY BY STATEMENT TYPE

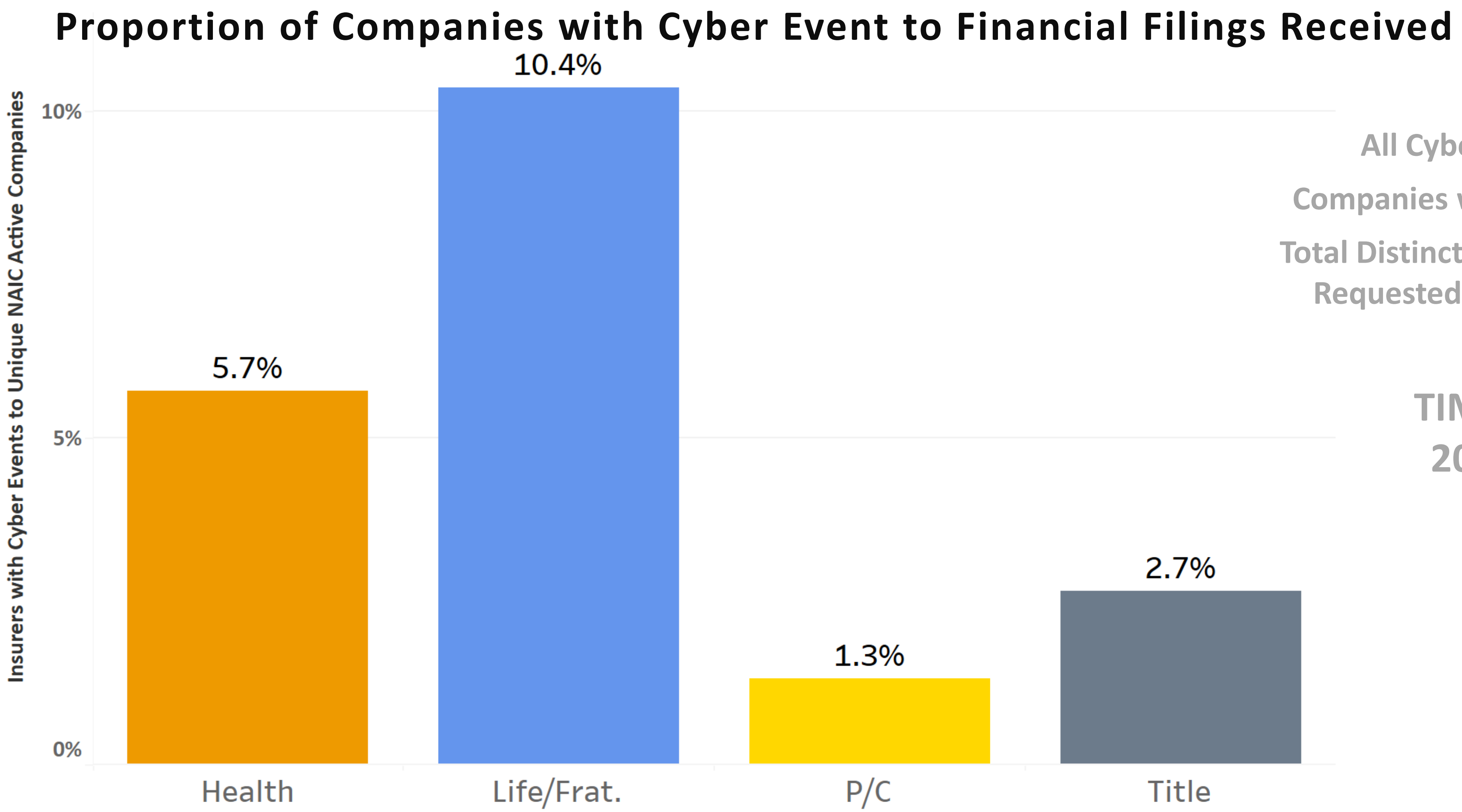


Matched NAIC Insurers

n Events=2,566

Source: Zywave data set, Jan 26, 2023

INSURER SECTOR INFLUENCE



All Cyber Events n = 2566

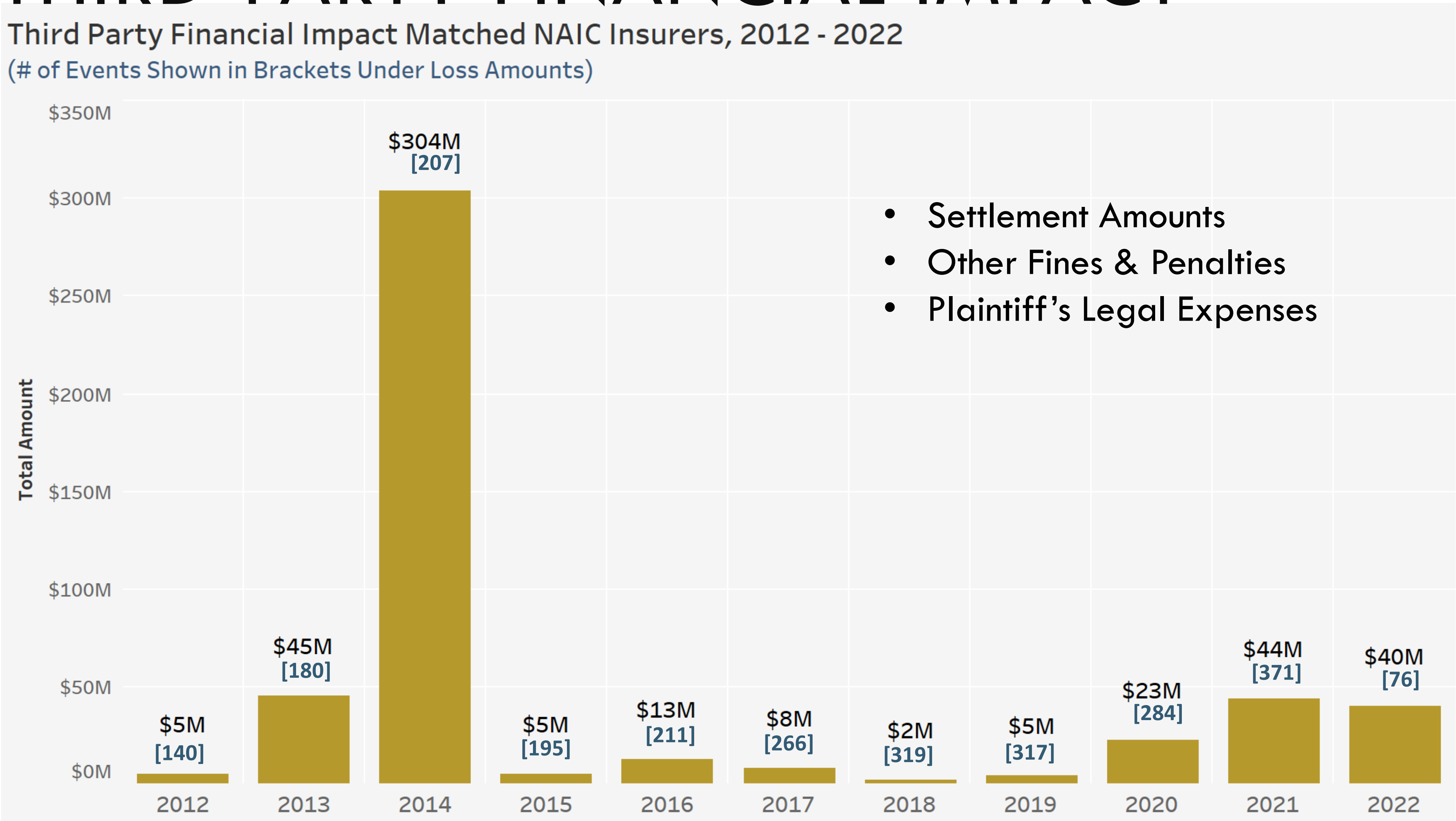
Companies w/ Cyber Event n = 526

Total Distinct Companies with Filings Requested 2012 - 2022 n = 5876

TIME PERIOD:
2012 – 2022

Source: Zywave data set, Jan. 26, 2023; NAIC FDR

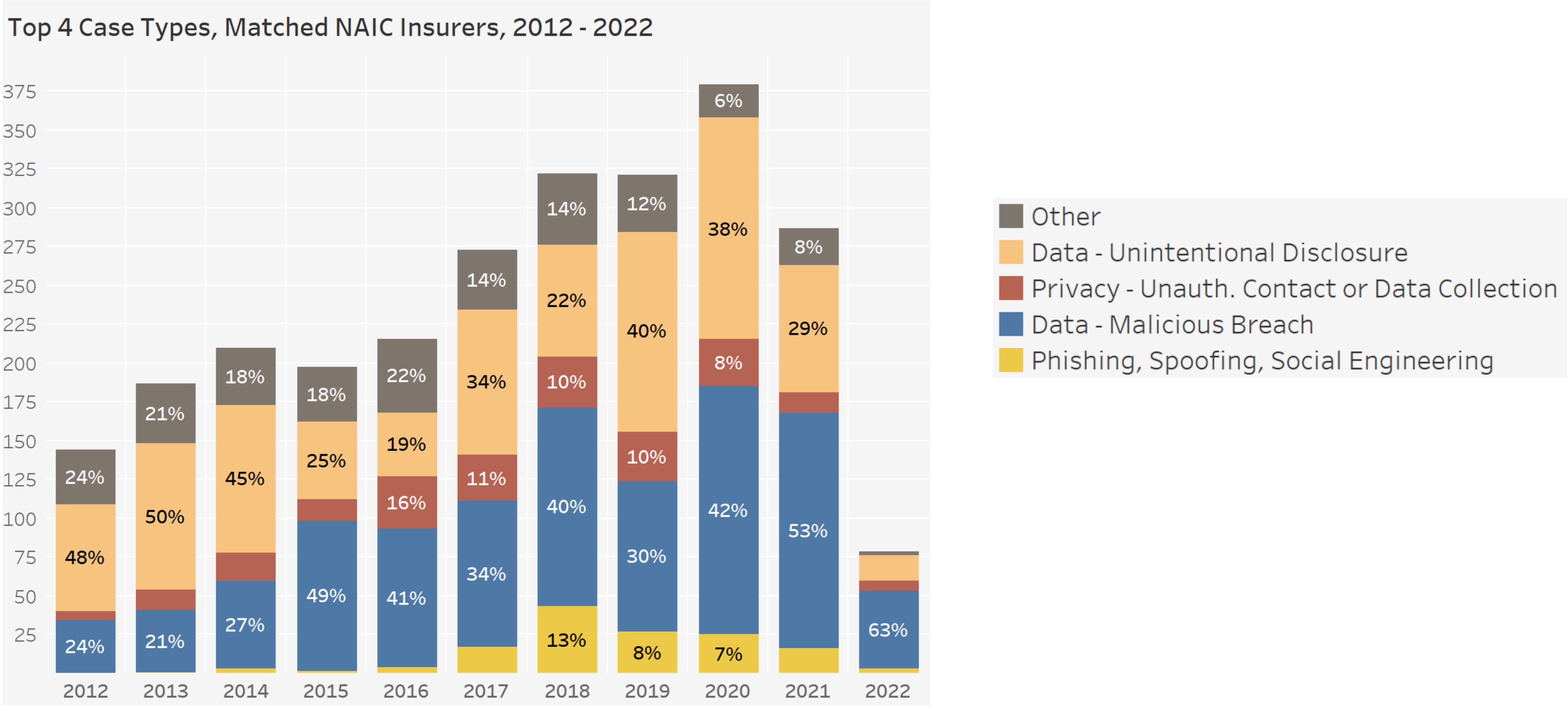
THIRD-PARTY FINANCIAL IMPACT



- Settlement Amounts
- Other Fines & Penalties
- Plaintiff’s Legal Expenses

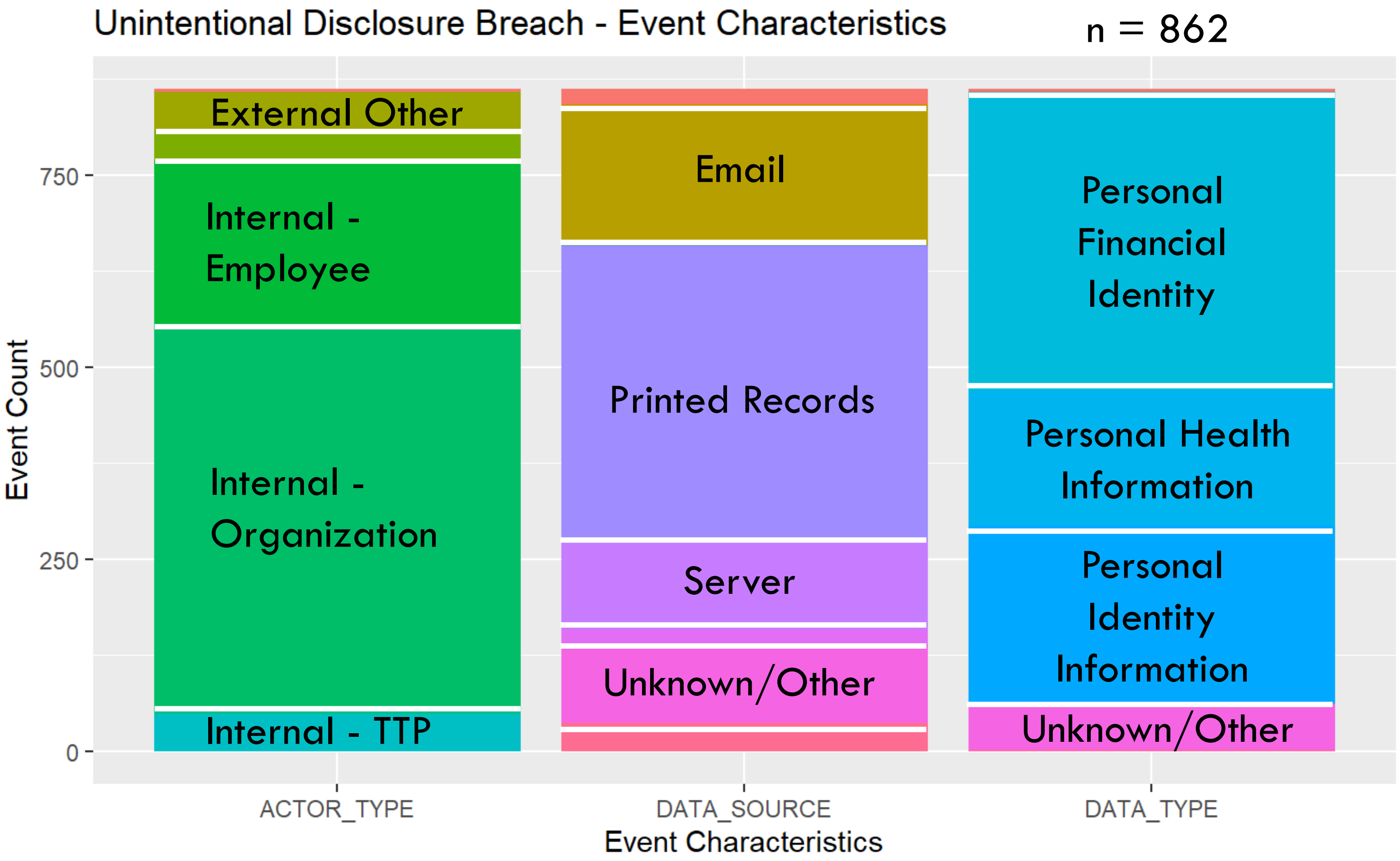
Source: Zywave data set, Jan 26, 2023

INSURER TOP 4 EVENT TYPES OVER TIME



Source: Zywave data set, Jan 26, 2023

EVENT TYPES: NAIC MATCHED INSURERS



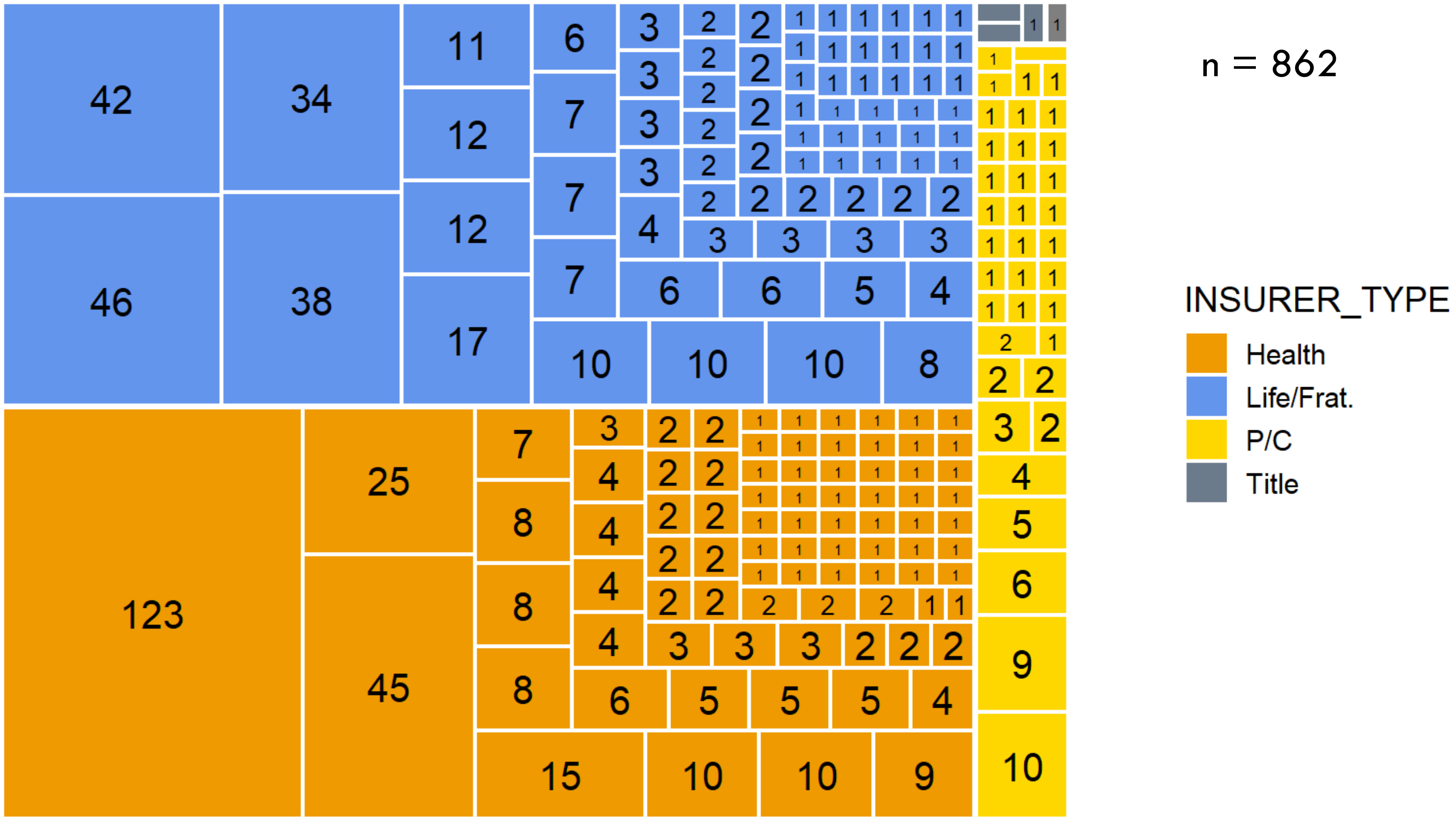
Unintentional Disclosure Example:

A policyholder ran a report that should have only shown their policy info, but instead included additional policyholders' info. Customer sent copy of report. Impacted over 1,000 policyholders.

Source: Zywave data set, Jan. 26, 2023

FREQUENCY BY COMPANY: 2012 - 2022

UNINTENTIONAL DISCLOSURE

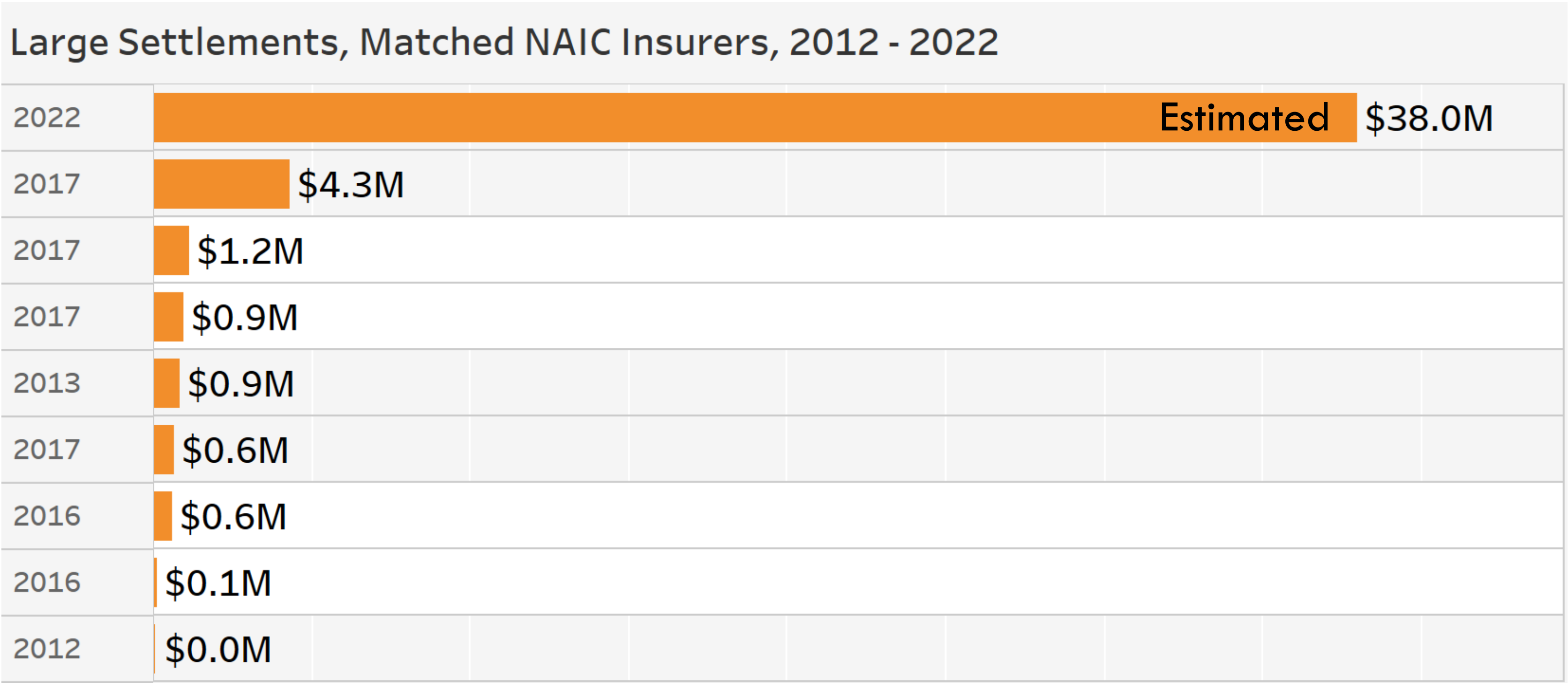


Source: Zywave data set, Jan 26, 2023

SEVERITY: 2012 - 2022

UNINTENTIONAL DISCLOSURE

n = 862

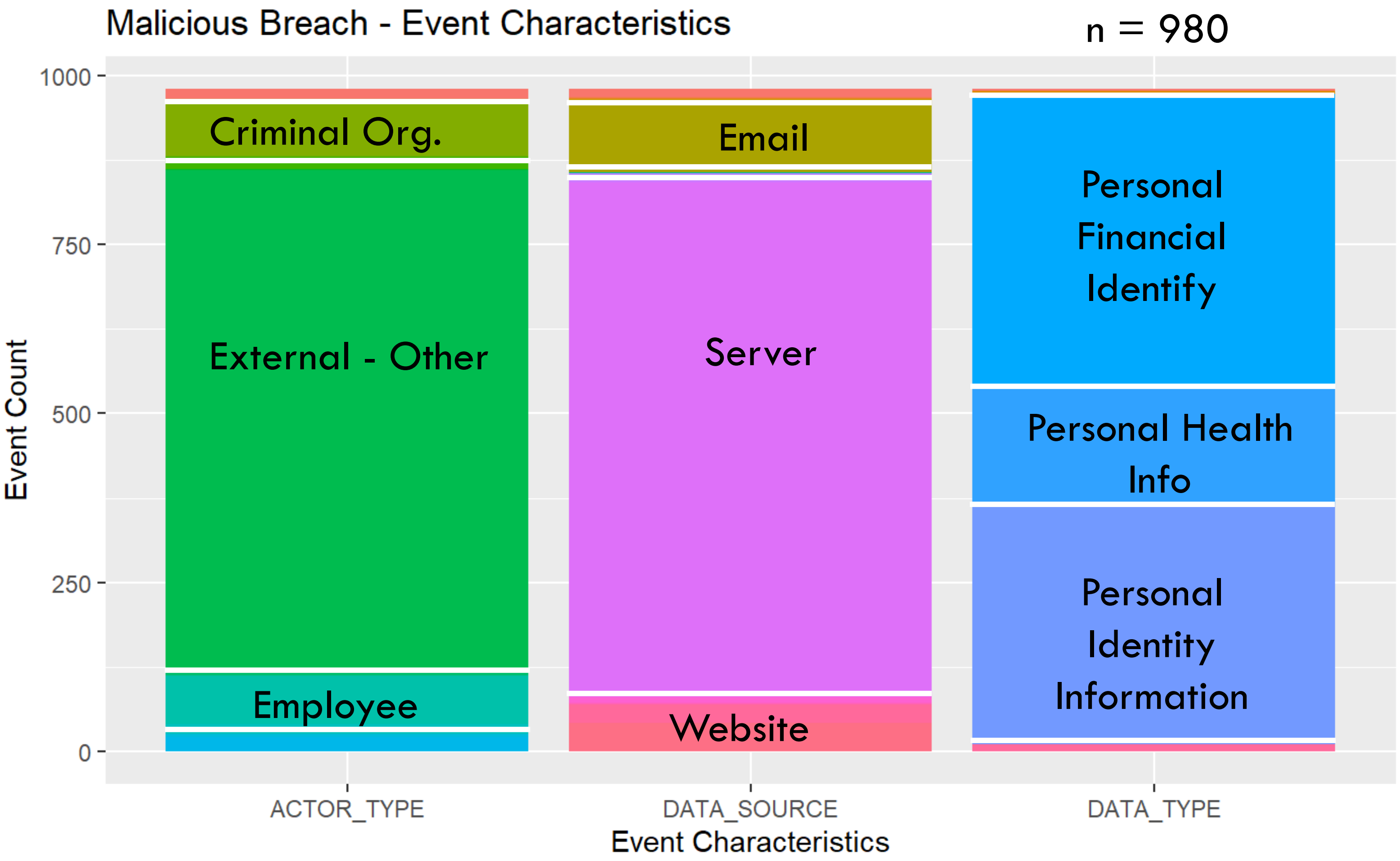

Large Settlements, Matched NAIC Insurers, 2012 - 2022

Event Percentile	Persons Affected
0%	1
10%	1
25%	1
50%	2
75%	103
90%	1,563
100%	15,000,000

% of Class Action Lawsuits: **.35%**

Source: Zywave data set, Jan 26, 2023

EVENT TYPES: NAIC MATCHED INSURERS



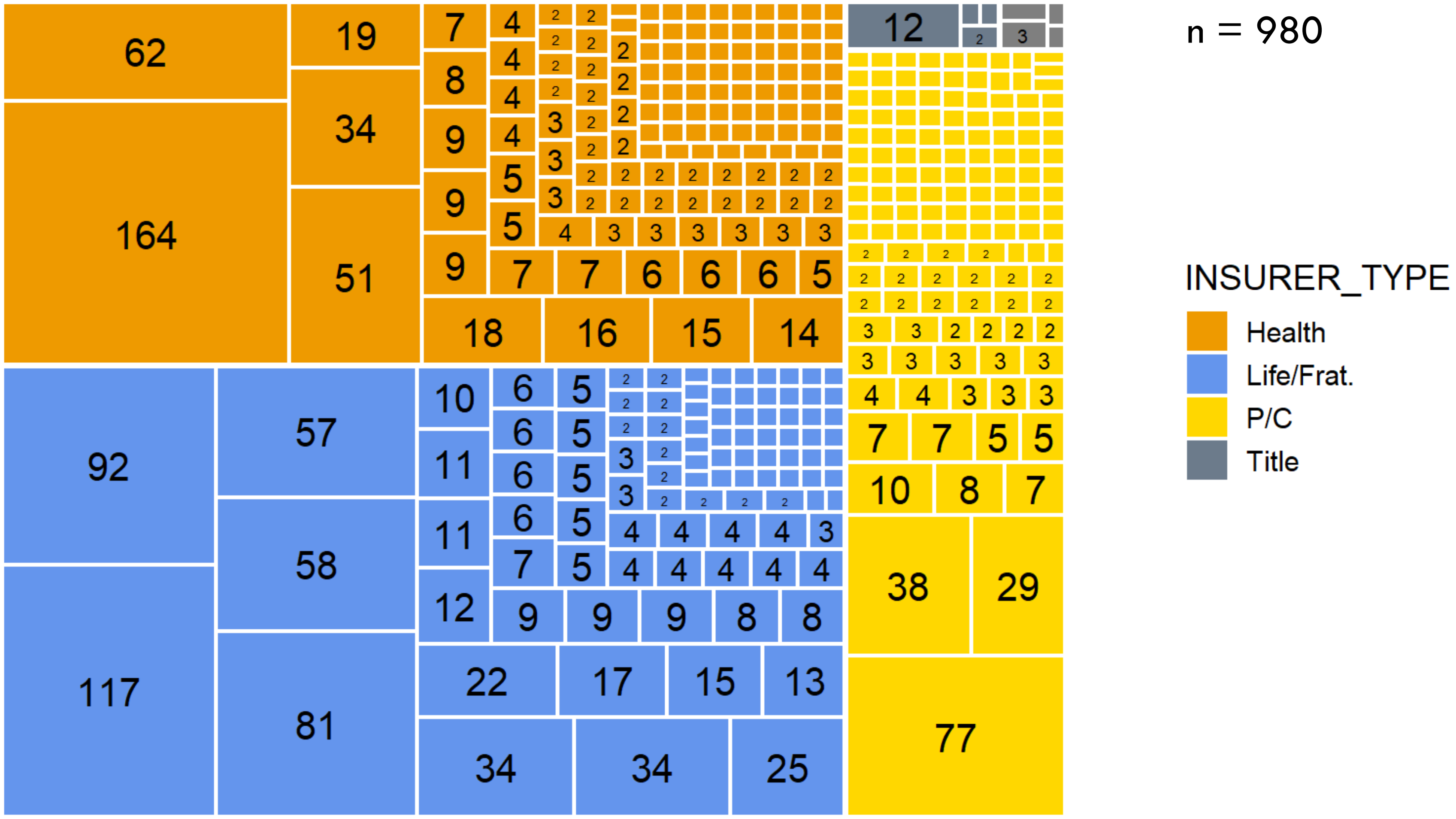
Malicious Breach Example:

A former employee took personal information from company records and sent it to their laptop to obtain OTC products from pharmacy. [54,000+ members potentially affected.]

Source: Zywave data set, Jan. 26, 2023

FREQUENCY BY COMPANY: 2012 - 2022

MALICIOUS BREACH

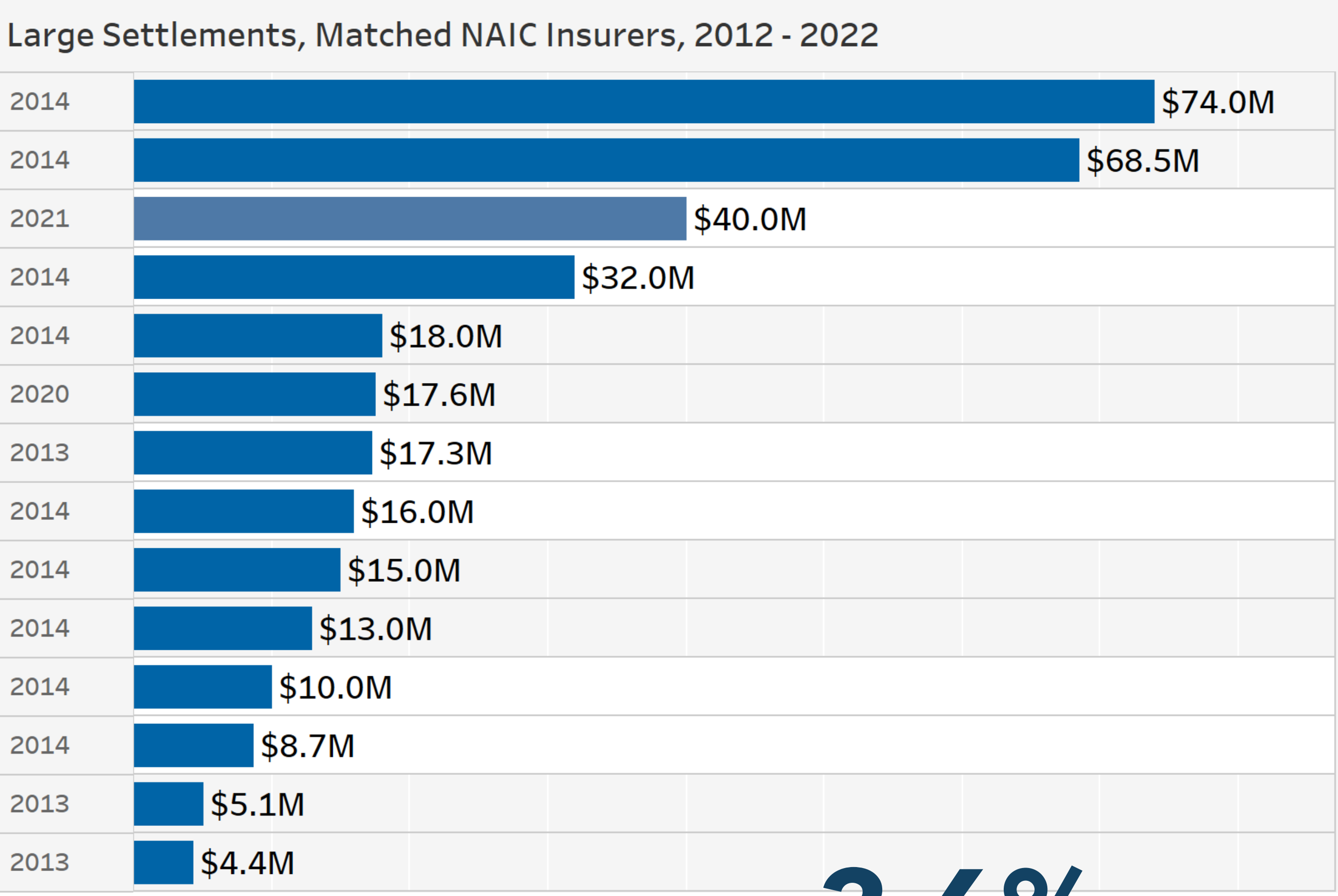


Source: Zywave data set, Jan 26, 2023

SEVERITY: 2012 - 2022

MALICOUS BREACH

n = 980



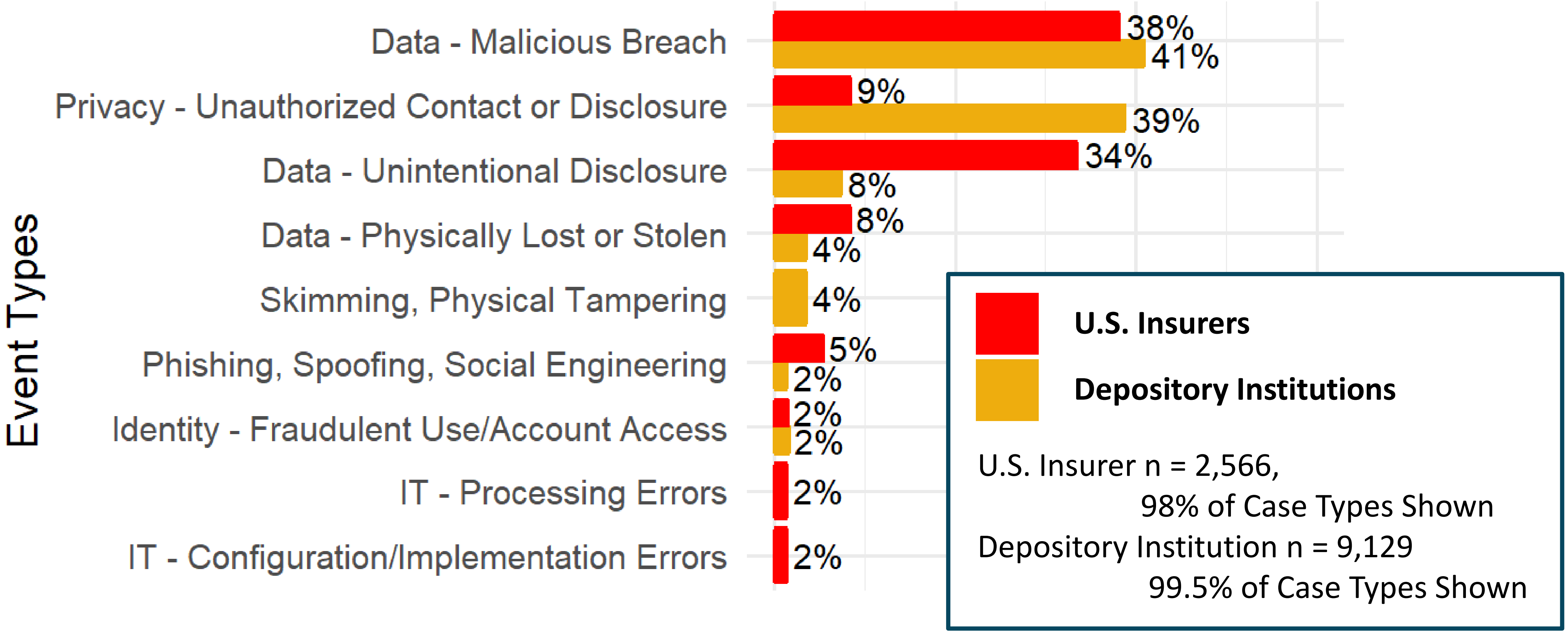
% of Class Action Lawsuits: **3.6%**

Event Percentile	Persons Affected
0%	1
10%	1
25%	2
50%	42
75%	1,324
90%	26,179
100%	11,000,000

Source: Zywave data set, Jan 26, 2023

EVENT TYPES: 2012 - 2022

NAIC INSURERS COMPARED TO FINANCIAL INSTITUTIONS

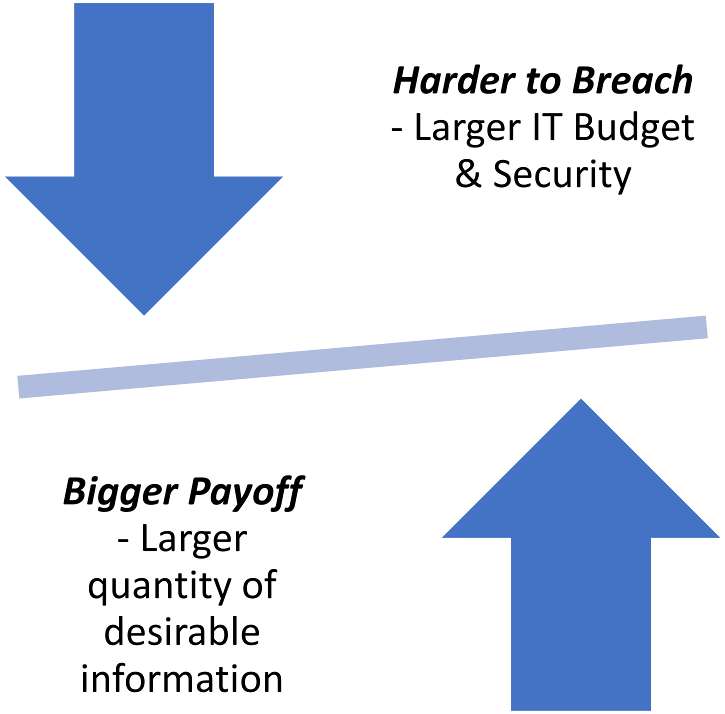


U.S. Insurer n = 2,566,
98% of Case Types Shown
Depository Institution n = 9,129
99.5% of Case Types Shown

Source: Zywave data set, Jan. 26, 2023

TYPE OF INSURER TO EXPERIENCE MALICIOUS CYBER LOSS EVENT

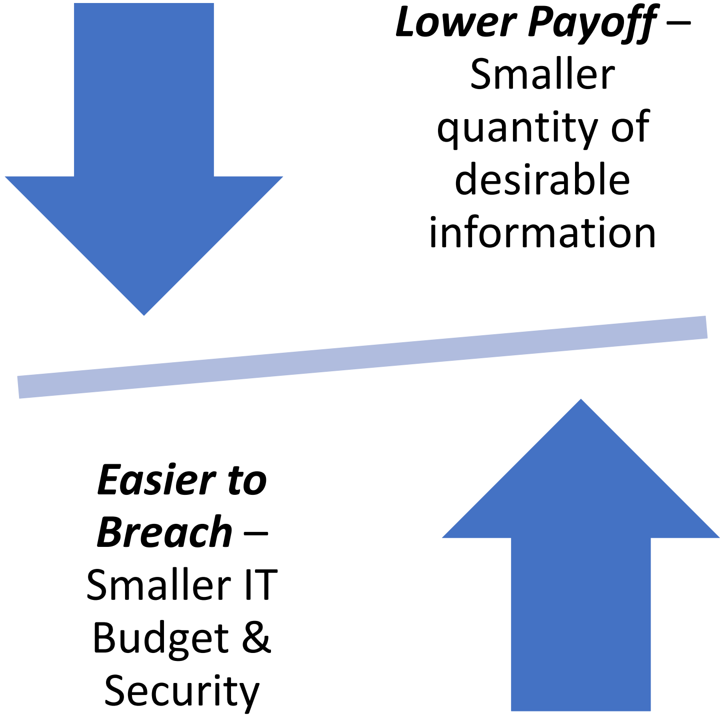
Relatively Larger Insurer



Harder to Breach - Larger IT Budget & Security

Bigger Payoff - Larger quantity of desirable information

Relatively Smaller Insurer



Lower Payoff – Smaller quantity of desirable information

Easier to Breach – Smaller IT Budget & Security

STATISTICAL ANALYSIS – DETERMINANTS OF MALICIOUS CYBER EVENTS

Research question

What types of insurers are more likely to experience a cyber loss event?

- Firm visibility
  - Age, Size (Total assets), Advertisement expense, Number of states
- Performance
  - Return on Assets (ROA) = Net income / Total assets
- Financial health
  - Leverage = Capital surplus / Total assets
- IT budget
- Intangible assets (Personal information)
  - Net premiums written

STATISTICAL ANALYSIS – DETERMINANTS OF MALICIOUS CYBER EVENTS

Sample

Includes all insurers that reported total assets greater than 0 in the annual statement from years 2012-2022

- 49,694 observations
- 7,219 insurers

Methodology

$$\text{Malicious cyber event}_t = \text{f(firm characteristics}_{t-1})$$

Malicious cyber event equals 1 if an insurer experienced a malicious cyber event in year *t*, and equals 0 otherwise

STATISTICAL ANALYSIS – DETERMINANTS OF MALICIOUS CYBER EVENTS

Key findings

Insurers are more likely to experience a cyber event when:

- Greater firm visibility (Size, Age, Advertisement expense, Number of states)
- Lower ROA
- Health insurer (3% > P&C, Life)
- Previous malicious cyber event (0.7%)
- Mutual insurers edge out non-mutual (0.3%)
- Grows over sample time frame

ORLANDO

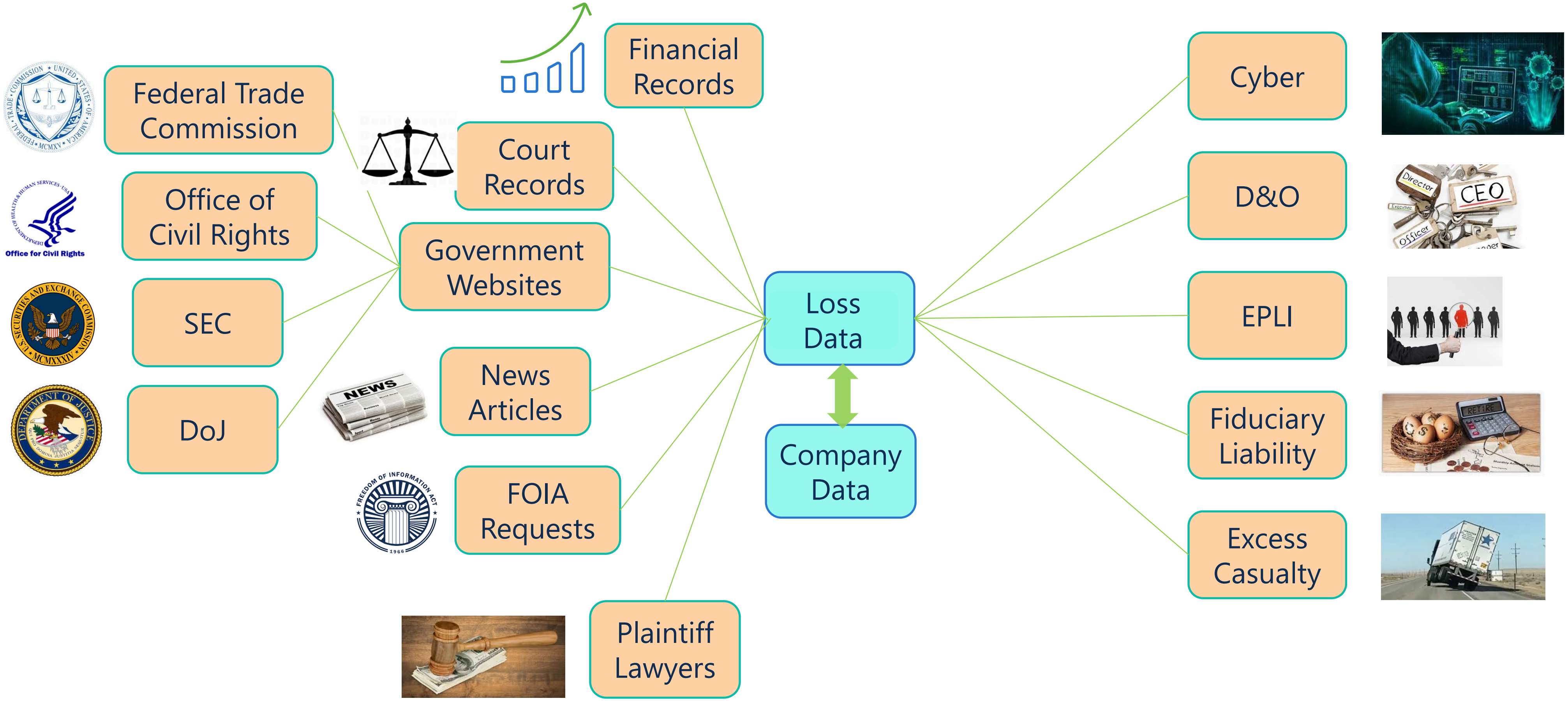
Zywave Loss Data Insights

Jim Blinn

Zywave

12/1/2023

Losses: Linking Disparate Sources



Federal Trade Commission

Office of Civil Rights

SEC

DoJ

Financial Records

Court Records

Government Websites

News Articles

FOIA Requests

Plaintiff Lawyers

Loss Data

Company Data

Cyber

D&O

EPLI

Fiduciary Liability

Excess Casualty

Comparison of Loss Types

Loss Type	Insurer	Non-Insurer FI	All Others	Total
Data - Malicious Breach	35.90%	38.46%	42.87%	41.88%
Privacy - Unauthorized Contact or Disclosure	13.63%	38.60%	22.67%	25.26%
Data - Unintentional Disclosure	28.87%	8.21%	14.27%	13.61%
Data - Physically Lost or Stolen	11.91%	4.64%	6.24%	6.11%
Network/Website Disruption	0.84%	2.04%	6.23%	5.32%
Phishing, Spoofing, Social Engineering	4.09%	2.78%	3.23%	3.18%
Privacy - Unauthorized Data Collection	0.49%	0.37%	1.22%	1.05%
IT - Configuration/Implementation Errors	1.15%	0.58%	0.92%	0.87%
Skimming, Physical Tampering	0.00%	2.26%	0.77%	1.01%
IT - Processing Errors	1.21%	0.68%	0.59%	0.62%
Identity - Fraudulent Use/Account Access	1.31%	1.04%	0.58%	0.68%
Undetermined/Other	0.59%	0.35%	0.30%	0.31%
Industrial Controls & Operations	0.02%	0.00%	0.11%	0.09%

Comparison of Actor Types

Actor Type	Insurer	Non-Insurer FI	All Others	Total
External - Other	40.96%	38.88%	41.03%	40.64%
Internal - Organization	33.49%	44.87%	33.50%	35.54%
External - Criminal Organization	5.25%	6.36%	10.80%	9.84%
Internal - Employee	11.57%	5.44%	8.22%	7.82%
External - Hacktivist	0.27%	0.86%	2.51%	2.15%
Internal - Trusted Third Party (TTP)	3.05%	1.07%	0.89%	0.98%
External - Vendor	3.09%	0.80%	0.66%	0.76%
External - Nation State	0.12%	0.22%	0.77%	0.65%
External - Former Employee	1.09%	0.60%	0.60%	0.62%
Internal - Other	0.54%	0.39%	0.47%	0.45%
External - Criminal Individual	0.21%	0.33%	0.21%	0.23%
External - Terrorist	0.04%	0.05%	0.12%	0.11%
Other	0.33%	0.14%	0.21%	0.20%

Comparison of Loss Types

Cyber Incident	Insurer	Non-Insurer FI	All Others	Total
MOVEit Cl0p Ransomware Attack, 2023	56	144	823	1023
Blackbaud Inc. Ransomware Attack, 2020		5	887	892
Heartland Payment Systems, Hacking, 2008	3	657	10	670
Ukraine-Russia Crisis Cyber Warfare, 2022		21	138	159
Insurance Technologies Data Breach, 2021	1	147	2	150
WannaCry Ransomware Attack, 2017		7	134	141
Sabre, Payment Card Data Breach, 2016	5	14	110	129
Connexin Software, Inc Data Breach, 2022			120	120
Luxottica Data Hacking Incident, 2020			106	106
Kronos Private Cloud Ransomware, 2021	4		92	96
Horizon Actuarial Services, Hacking 2021		42	52	94
AmeriCommerce, Data Hacking 2021			87	87
Accellion Unauthorized Access, 2020	3	8	58	69

ORLANDO

NATIONAL ASSOCIATION OF
INSURANCE COMMISSIONERS

CyberCube

Cyber risk modeling - an insurance industry view

December 2023

www.cybcube.com

About CyberCube

Mission

Deliver the world’s leading analytics and services to quantify cyber risk

History

- Founded in 2018
- Focused solely on cyber risk quantification and analytics
- Largest
  - single investment in cyber risk data and analytics
  - dedicated multi-functional team (>115)

Market Position

- > 100 (re)insurance clients
  - 20/30 top cyber carriers
  - 9/20 top global reinsurers
- > 95% client retention rate
- > 66% of global cyber insurance premiums

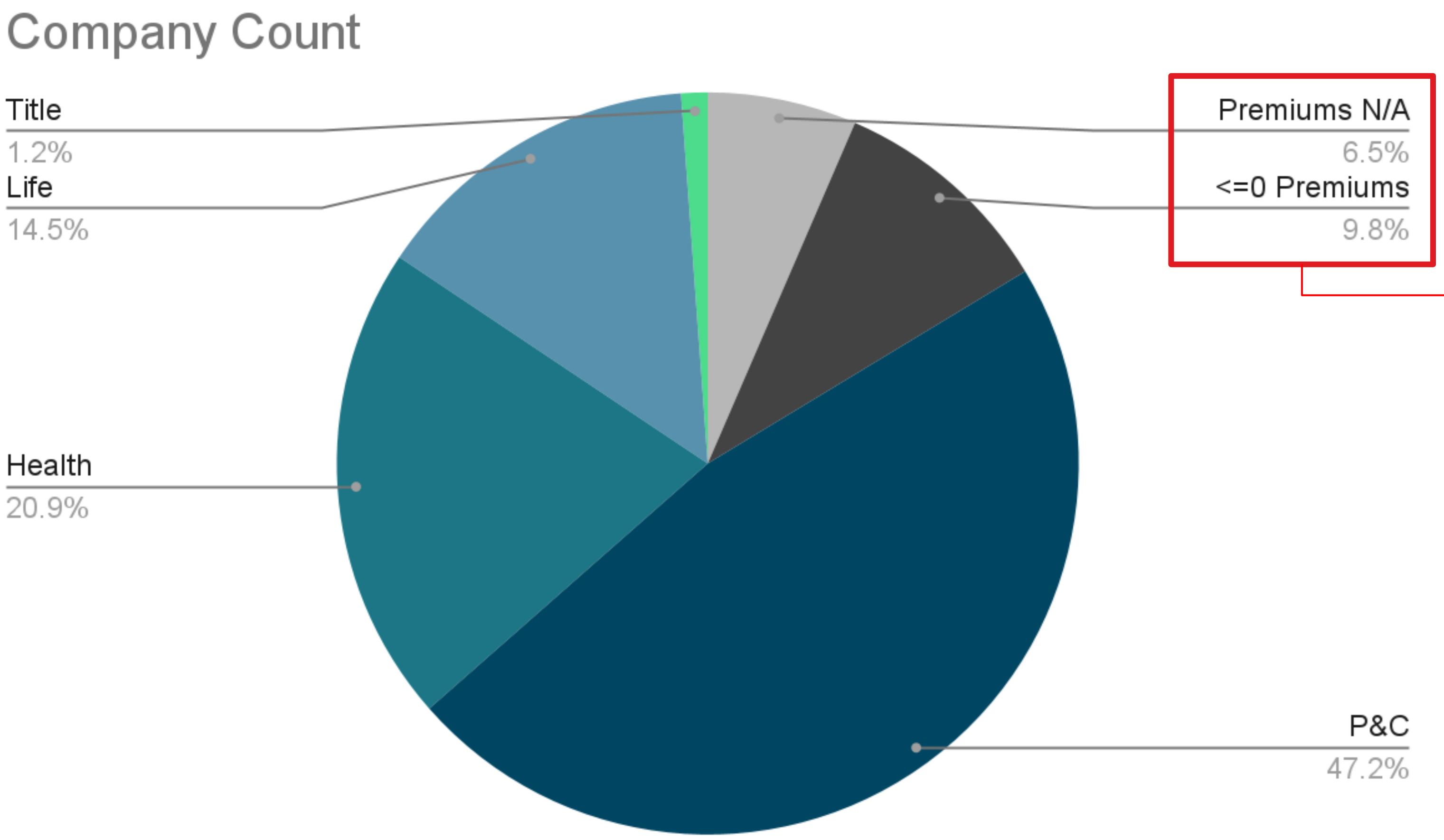
Regulatory Engagement

- Maintain active dialogues with regulators in key markets, and regularly engage on projects to develop cyber risk governance frameworks and risk management structures
- Partner with rating agencies to develop approaches to underwriting and rating cyber risk

CyberCube Solutions leveraged

- Portfolio Manager
  - SPoF scenario-class based cyber cat model
  - Quantify attritional and tail risk
- Account Manager
  - Predictive security score and risk factors

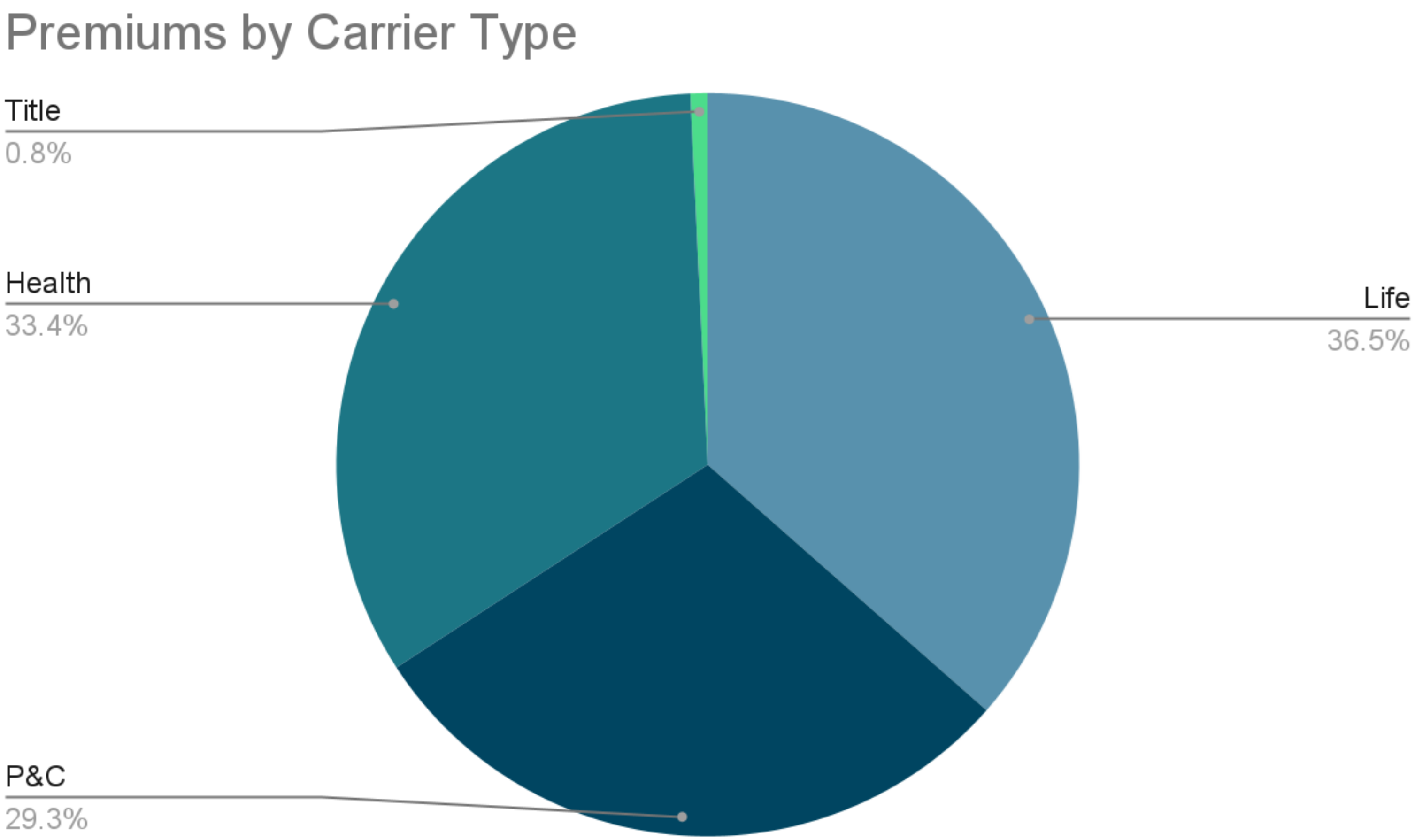
Insurance Industry loss modeling analysis: Carrier Count by Type



# of Carriers by Type

●	*Total*	*4155*
●	Excluded	679
●	*Subtotal*	*3476*
●	P&C	1960
●	Health	867
●	Life	601
●	Title	48

Insurance Industry loss modeling analysis: 2022 Direct Written Premium by Type



Premiums by Carrier Type*

- P&C
  $1,055B
- Life
  $967B
- Health
  $848B
- Title
  $21B

*excluding N/A, Zero, Negatives

What questions did we tackle?

1. Which companies are most vulnerable from a security perspective?

2. Which of the insurer’s technology dependencies are the vector for loss?

3. What types of events are most likely to cause losses across the insurance industry?

4. What is the financial cost of cyber attacks on the US insurance industry?

5. Which companies present the largest risks?

Executive Summary

1. *Which companies are most vulnerable from a security perspective?*
   a. **Micro-sized insurers (<$10mn premium), on average, have the weakest cyber security postures and are most vulnerable to loss**
   b. **Large companies, on average, have the best cyber security among insurers**
   c. **The Insurance sector, on average, is below the Financial industry average on cyber security**
2. *Which of the insurer's technology dependencies are the vector for loss?*
   a. **Cyber attackers are most likely to access systems via shared technology dependencies such as certificate authorities, cloud service providers and content management systems**
3. *What types of events are most likely to cause losses across the insurance industry?*
   a. **Ransomware and Data Theft are the sources of largest loss to the insurance industry**
4. *What is the financial cost of cyber attacks on the US insurance industry?*
   a. **In any given year, the insurance industry will suffer $434mn in losses. At the 1-in-250 return period, the insurance industry could suffer losses of $8.3bn**
5. *Which companies present the largest risks?*
   a. **In a breakdown of individual companies that drive the industry loss, larger insurers contribute most to the loss quantum**

1a. Which companies are the most *vulnerable* from a security perspective?

- CyberCube’s security scores consider 45 security risk factors, including Open Ports, End-of-Life products, Unpatched software

- These top-10 vulnerable* companies are all Micro size (<$10mn GwP). Company names obscured below, because…

- ‘Vulnerable’ does not equal ‘Negligent’. Cybersecurity is fast moving and requires resource. The likelihood of being attacked is a function of cybersecurity, the company’s value as a target and the volume of data/assets to be stolen

P&C

- Superior Specialty Ins Co
- [redacted]
- Consumer Specialties Ins

Life

- American Mut Life Assn
- [redacted]
- Dakota Capital Life Ins Co

Health

- Magna Ins Co
- [redacted]
- Central Mass Hlth LLC

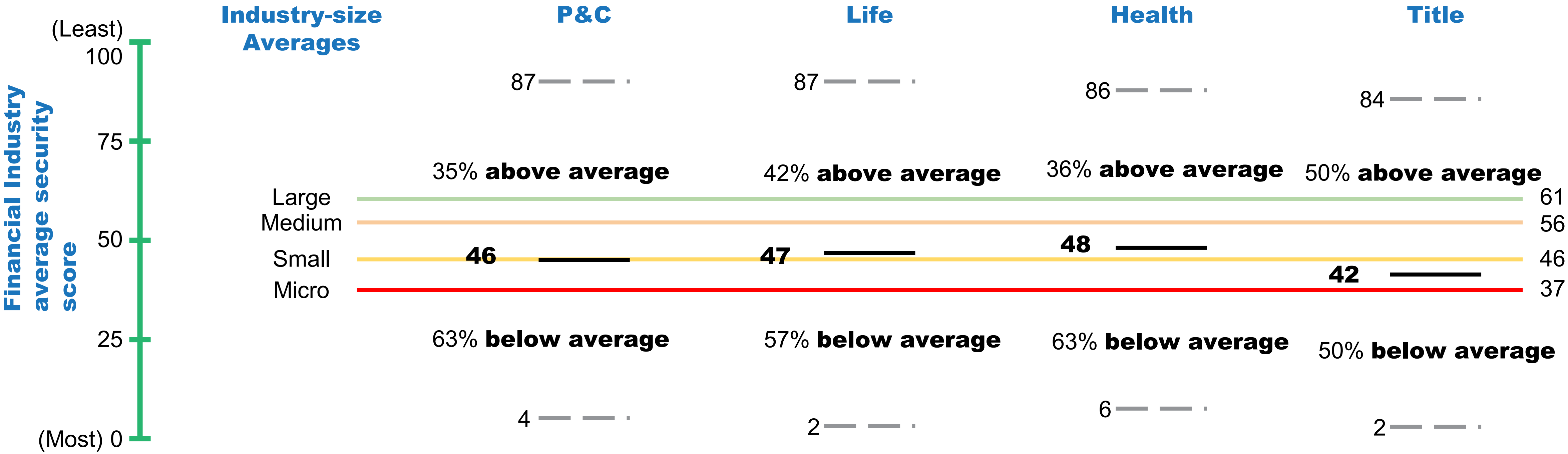
Title

- American Eagle Title Ins Co
- [redacted]
- Conestoga Title Ins Co

* lowest CyberCube security scores

1b. Which segment is the most *vulnerable* from a security perspective?

- CyberCube Security Score averages show *all* Financial industry companies
- For all insurers, the averages by segment range from 42-48, therefore slightly below average Financial companies
- For P&C and Health insurers, two-thirds are below average for all Financials
- Life and Title insurers sit around the Financial industry average
- Overlaying company size, Large and Medium companies have above average scores. Small are average and Micro are below average



2. Which of the insurer’s technology dependencies are main vectors for loss?

- CyberCube loss modeling is based on Single Points of Failure (SPoF) technology dependencies that act as vectors to cause loss

- We show here the top SPoF groups for the insurance industry

- Research highlights 4 main SPoF types as vulnerabilities for attack: Certificate Authority, File sharing providers, Email services providers and Content Management Systems

Insurer technology dependency groups

- **Cloud Service Provider** (Omni)
  - AWS, Azure, Salesforce
- **Content Delivery Network** Provider
  - Cloudflare, Akamai, Amazon CloudFront
- **Certificate Authority**
  - DigiCert, Let’s Encrypt, GoDaddy
- **Cloud-based Enterprise File Sharing Provider**
  - MS OneDrive/Azure, Google Drive, Apple iCloud
- **Email Services Provider**
  - MS Exchange, Gmail for Business, Zoho Mail
- **DNS Provider**
  - Route53, Cloudflare, GoDaddy
- **Operating System - Server**
  - Ubuntu, Unix, Linux
- **Content Management System Provider**
  - WordPress. Adobe Experience Manager, HubSpot CMS
- **E-Commerce Platform**
  - Shopify, Magento, Amazon

3. What type of event(s) can cause the largest losses to the Insurance Industry?

Five highest loss scenario classes

Loss type	SPoF exploited
Ransomware	File Sharing Provider
Data Theft	Fund Administrator
Destructive Malware	Cloud Services Provider
Ransomware	Endpoint Operating System
Data Theft	Enterprise Payroll Provider

Five lowest loss scenario classes

Loss type	SPoF exploited
Cash Theft	Financial Transaction Provider
Data Theft	E-Commerce Platform
Ransomware	Medical Device Manufacturer
Data Theft	Mobile Point of Sale Vendor
Extortion	Point of Sale Vendor

4. What is the financial cost of cyber attacks on the US insurance industry?

Individual Life & Health company contribution to loss is higher

Annual Probability	US Insurance Industry	P&C	Life	Health	Title
Average Annual Loss	**434**	120	168	142	4
2.0% or 1-in-50yr	4,267	1,167	1,738	1,387	35
1.0% or 1-in100yr	5,782	1,585	2,458	1,896	54
0.4% or 1-in-250yr	**8,284**	2,077	3,642	2,735	87
0.2% or 1-in-500yr	11,501	3,101	4,917	3,876	122

Losses shown in $millions.

5. Which companies drive the most losses – on average vs in a cyber catastrophe?

P&C

Average Annual Loss

- Stat [redacted] Auto Ins Co
- Unit [redacted] Ins Co
- Stat [redacted] & Cas Co
- Nati [redacted]
- Fed [redacted]

1-in-250yr cat

- State F [redacted] o Ins Co
- United [redacted] Co
- State F [redacted] Cas Co
- Nations [redacted]
- United [redacted] bile Assn

Life

Average Annual Loss

- Healtl [redacted] Co
- Ameri [redacted] Ins Co of NY
- Globe [redacted] of NY
- Wysh [redacted] ns Co
- Relian [redacted] Life Ins Co

1-in-250yr cat

- Health [redacted] Co
- Americ [redacted] ns Co of NY
- Wysh L [redacted] s Co
- Relianc [redacted] Life Ins Co
- Globe L [redacted] NY

Health

Average Annual Loss

- Pacif [redacted] Hlth Ins Co
- Clove [redacted]
- Gold [redacted] ns Co
- Anthe [redacted] c
- Cigna [redacted] of NC Inc

1-in-250yr cat

- Pacif [redacted] Hlth Ins Co
- Clove [redacted]
- Gold [redacted] ns Co
- Anthe [redacted] c
- Cigna [redacted] of NC Inc

Title

Average Annual Loss

- Cone [redacted] ns Co
- Attorr [redacted] aranty Fund Inc
- Natio [redacted] Of NY Inc
- Allian [redacted] s Co Inc
- Real [redacted] itle Ins Co

1-in-250yr cat

- Cone [redacted] ns Co
- Allian [redacted] s Co Inc
- Attorr [redacted] aranty Fund Inc
- Natio [redacted] Of NY Inc
- Real [redacted] itle Ins Co

Executive Summary

1. *Which companies are most vulnerable from a security perspective?*
   a. **Micro-sized insurers (<$10mn premium), on average, have the weakest cyber security postures and are most vulnerable to loss**
   b. **Large companies, on average, have the best cyber security among insurers**
   c. **The Insurance sector, on average, is below the Financial industry average on cyber security**
2. *Which of the insurer's technology dependencies are the vector for loss?*
   a. **Cyber attackers are most likely to access systems via shared technology dependencies such as certificate authorities, cloud service providers and content management systems**
3. *What types of events are most likely to cause losses across the insurance industry?*
   a. **Ransomware and Data Theft are the sources of largest loss to the insurance industry**
4. *What is the financial cost of cyber attacks on the US insurance industry?*
   a. **In any given year, the insurance industry will suffer $434mn in losses. At the 1-in-250 return period, the insurance industry could suffer losses of $8.3bn**
5. *Which companies present the largest risks?*
   a. **In a breakdown of individual companies that drive the industry loss, larger insurers contribute most to the loss quantum**

Questions?
Email rebeccab@cybcube.com

CyberCube

This document is for general information purpose only and is not and shall not under any circumstance be construed as legal advice. It is not intended to address all or any specific area of the topic in this document. Unless otherwise expressly set out to the contrary, the views and opinions expressed in this document are those of CyberCube's and are correct as at the date of publication. Whilst all reasonable care has been taken in the preparation of this document including in ensuring the accuracy of the content of this document, no liability is accepted by CyberCube and its affiliates for any loss or damage suffered as a result of reliance on any statement or opinion, or for any error or omission, or deficiency contained in the document. CyberCube and its affiliates shall not be liable for any action or decisions made on the basis of the content of this document and accordingly, you are advised to seek professional and legal advice before you do so. This document and the information contained herein are CyberCube's proprietary information and may not be reproduced without CyberCube's prior written consent. Nothing herein shall be construed as conferring on you by implication or otherwise any license or right to use CyberCube's intellectual property. All CyberCube's rights are reserved.

CyberCube Analytics, Inc., 58 Maiden Lane, 3rd Floor, San Francisco, 94108

CyberCube

Cyber Catastrophe Modeling: Q&A

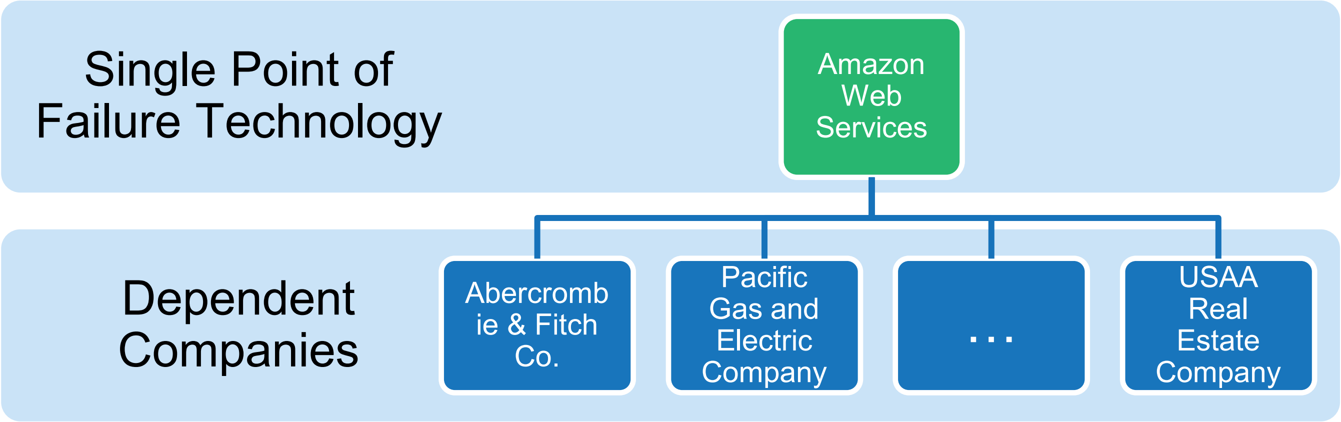
Rebecca Bole, Shaveta Gupta

Digital Supply Chain - Single Point of Failure (SPOF) Overview

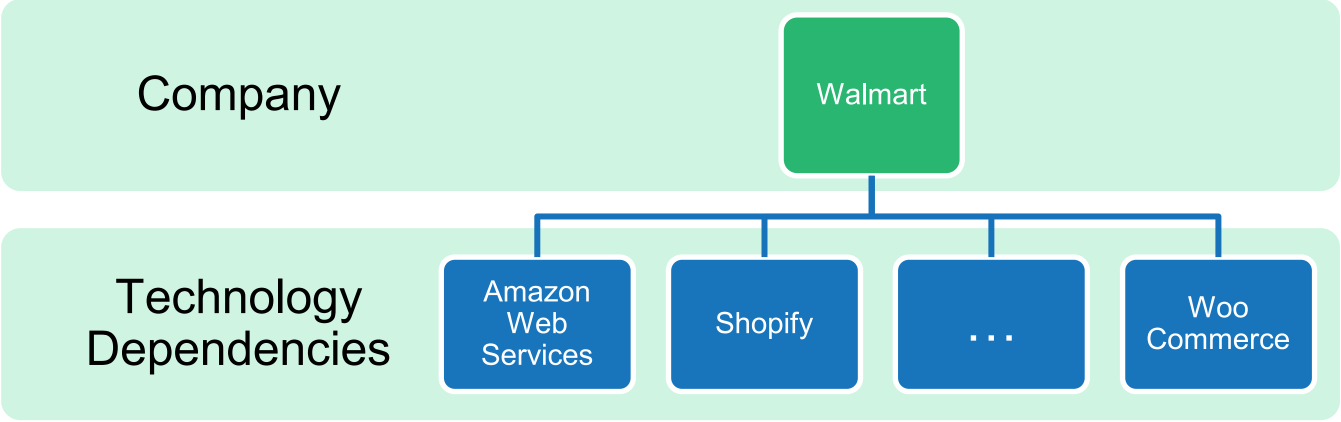
Single Point of Failure (SPoF)

- Signifies the company, service, etc. within each scenario class that caused the system failure.
- SPoF Intelligence provides information to better understand your insurance portfolio and connections by understanding which single points of failure an insured relies on
- Understand which accounts are dependent upon a Single Point of Failure

SPOF to Company Relationships



Company to SPOFs Relationships



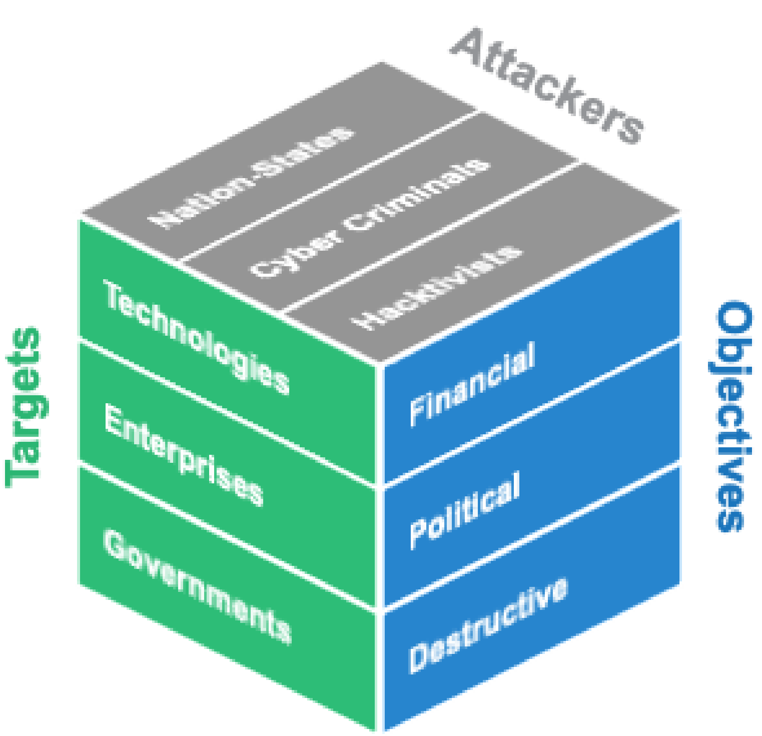
Scenario Generation: CUBE Framework

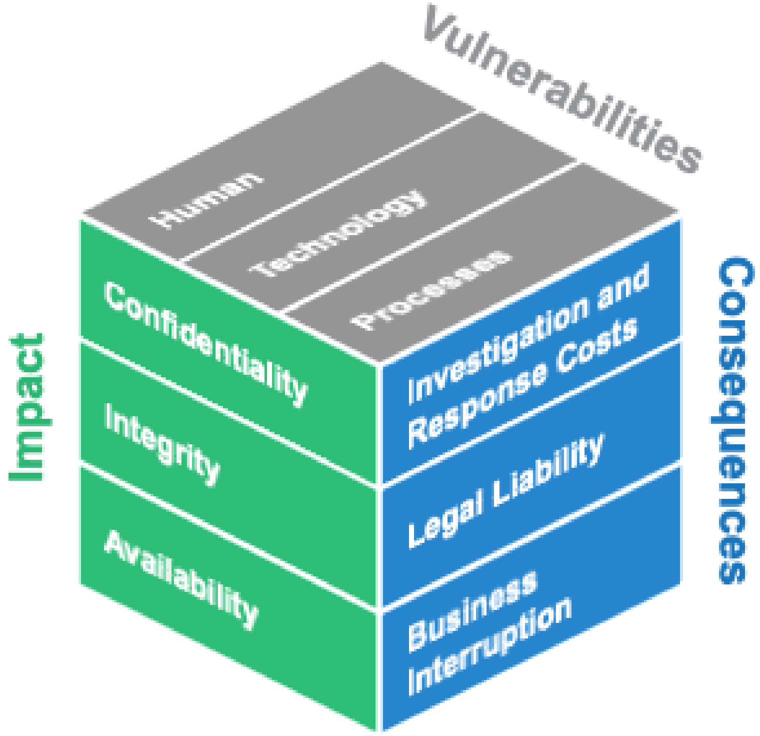
Our multi-disciplinary expert teams leverage our proprietary **CUBE Framework** to quantify the impacts of cyber attacks across the six dimensions of an attack:

- Attackers
- Targets
- Objectives
- Vulnerabilities
- Impact
- Consequences

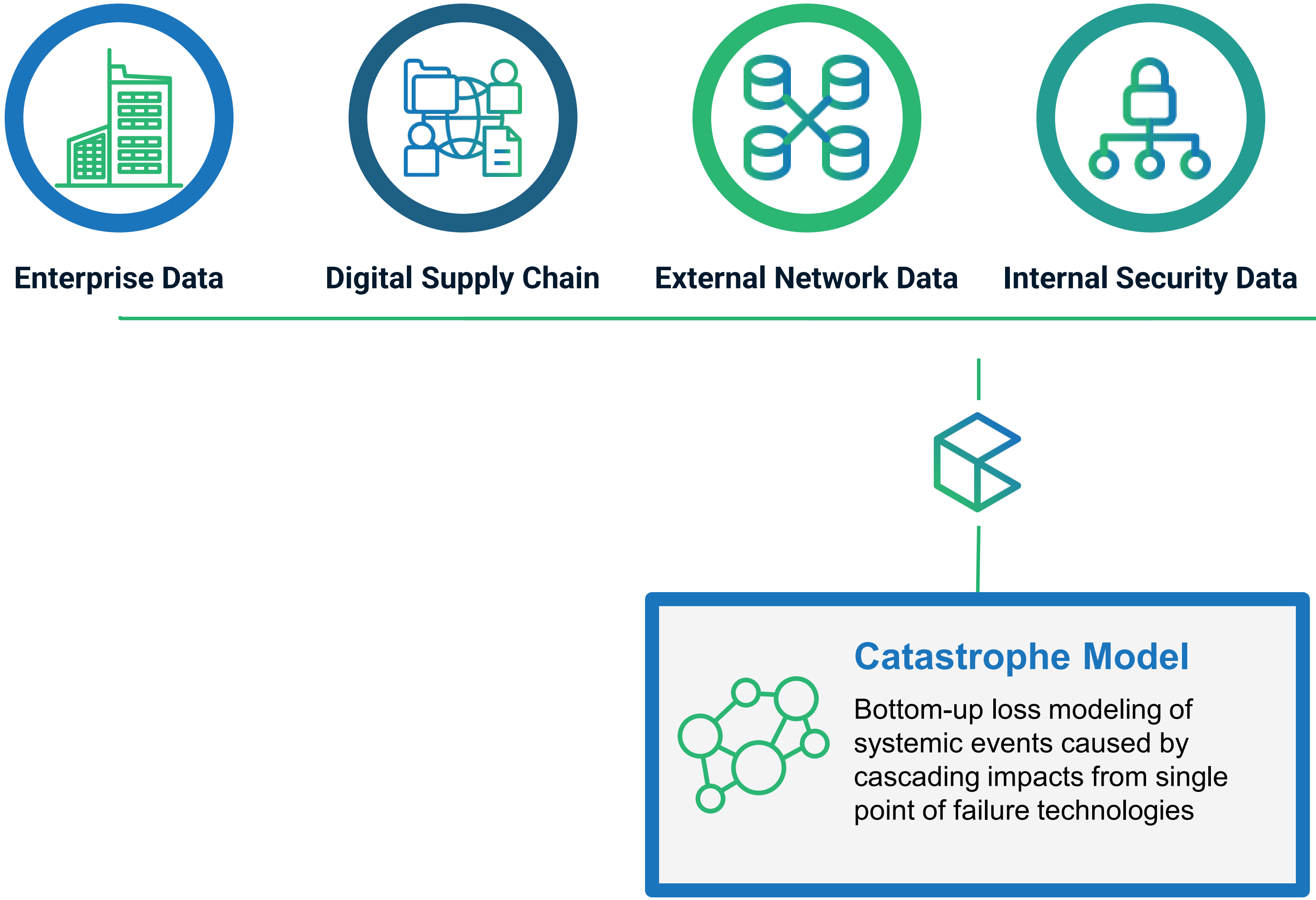
This framework:

- Breaks down the technical complexity of a cyber attack into meaningful and complete narratives easily understood by both experts and non-experts.
- Provides a consistent methodology to create representative scenarios with the greatest combined probability, impact, and reach which would cause catastrophic loss accumulation for (re)insurers.





CyberCube Exposure Data



Enterprise Data

Digital Supply Chain

External Network Data

Internal Security Data

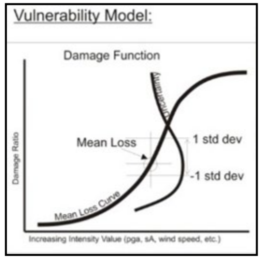
Expert Intelligence

Historical Data

Catastrophe Model

Bottom-up loss modeling of systemic events caused by cascading impacts from single point of failure technologies

As with Property, 3 factors must be present to create Cyber insurance risk

	Property	Cyber
1. Exposure Creates aggregation potential	 	amazon web services Microsoft
2. Peril Frequency & severity of events	 	
3. Vulnerability Susceptibility to peril	 	 CVE-2021-44228 Base Score: 10.0 CRITICAL

Cyber risk shares many qualities with other P&C lines

How cyber risk is like…

Property

- Short tail
- Catastrophe-exposed line
- Embrace of catastrophe modeling & exposure management
- Focus on risk tolerance at the extreme tail: 1-in-100, 1-in-250

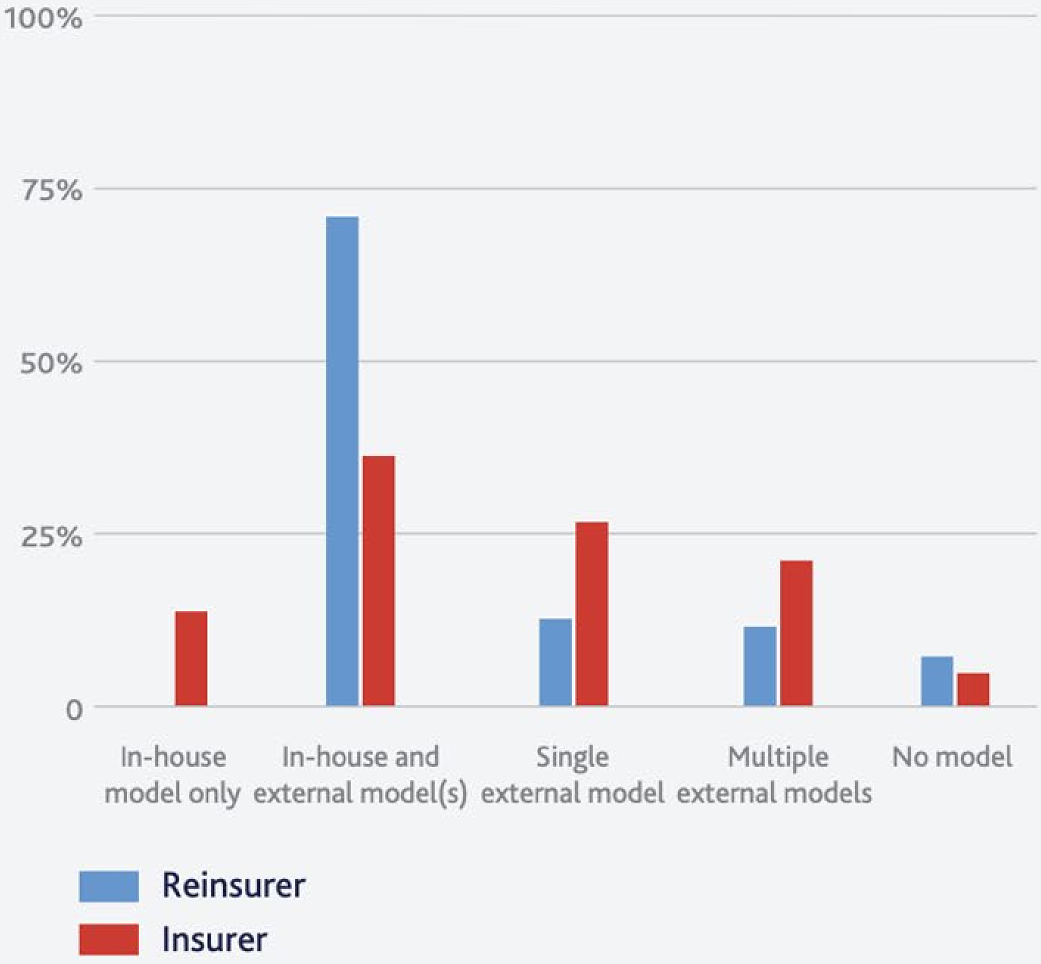
Casualty

- Social science, not natural science
- Managed within Specialty / Professional Liability / E&O
- Concern about systemic risk (theoretically cannot be diversified)
- Pricing volatility & underwriting cycle
- Mean vs median vs mode loss ratio

Terrorism

- Man-made peril
- Sensitive to political environment
- Dynamic & rapidly evolving threat

FIGURE 6: USE OF CYBER RISK MODELS BY RE/INSURERS (% OF FIRMS)

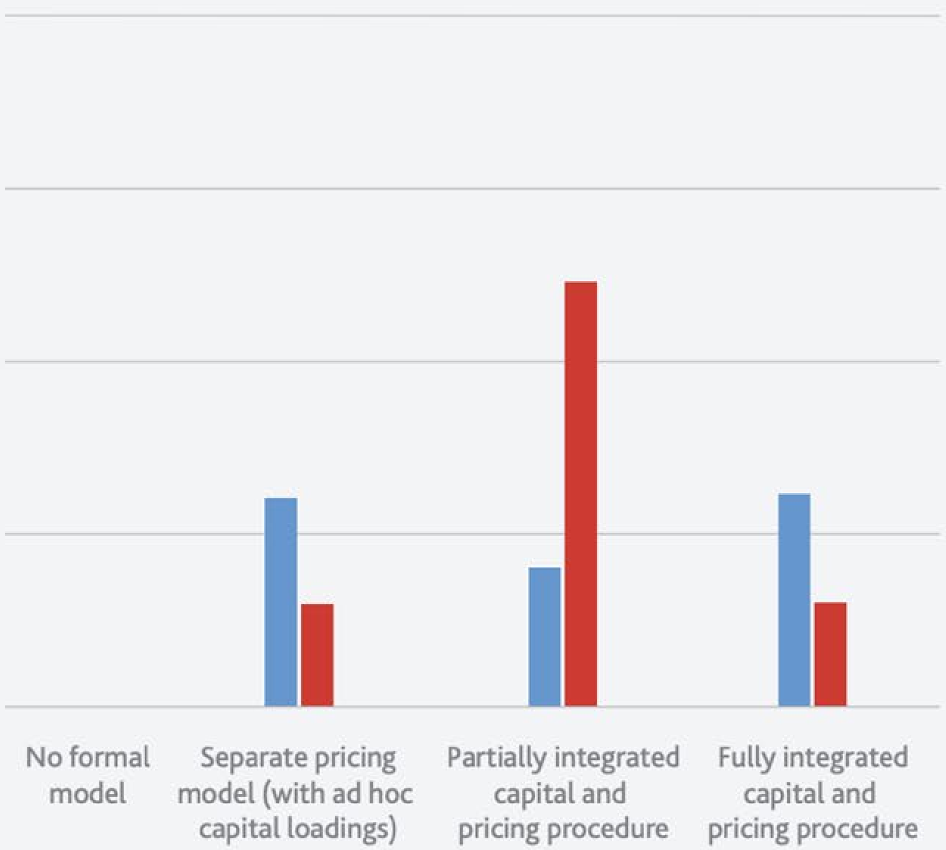


Based on 52 re/insurers who have in-house or licence external models, weighted by cyber insurance premiums

Source: The Geneva Association, based on data from Gallagher Re

FIGURE 7: ROLE OF CYBER MODELS IN UNDERWRITING (% OF RESPONDENT RE/INSURERS)

Is cyber accumulation assessment integrated within underwriting?



Based on a poll of 11 GA member cyber re/insurers, weighted by relative size of cyber insurance premiums

Source: The Geneva Association

Questions?
Email rebeccab@cybcube.com

CyberCube

This document is for general information purpose only and is not and shall not under any circumstance be construed as legal advice. It is not intended to address all or any specific area of the topic in this document. Unless otherwise expressly set out to the contrary, the views and opinions expressed in this document are those of CyberCube's and are correct as at the date of publication. Whilst all reasonable care has been taken in the preparation of this document including in ensuring the accuracy of the content of this document, no liability is accepted by CyberCube and its affiliates for any loss or damage suffered as a result of reliance on any statement or opinion, or for any error or omission, or deficiency contained in the document. CyberCube and its affiliates shall not be liable for any action or decisions made on the basis of the content of this document and accordingly, you are advised to seek professional and legal advice before you do so. This document and the information contained herein are CyberCube's proprietary information and may not be reproduced without CyberCube's prior written consent. Nothing herein shall be construed as conferring on you by implication or otherwise any license or right to use CyberCube's intellectual property. All CyberCube's rights are reserved.

CyberCube Analytics, Inc., 58 Maiden Lane, 3rd Floor, San Francisco, 94108

NAIC

NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS