Cyber Risk and Assessment
An Insurance Industry and Market Perspective

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)
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


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/)
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.


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;

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.
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

Total Number of Events: 150,341
Source: Zywave Data Set, 01/26/2023
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

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

TIME PERIOD: 2012 - 2022

All U.S.
124,589
events

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

12
INSURANCE EVENTS OVER TIME (2012-2022)

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

Roughly, insurance companies are 4x more likely than a depository institution to experience a cyber event.
EVENT FREQUENCY BY STATEMENT TYPE

Matched NAIC Insurers
n Events=2,566

Source: Zywave data set, Jan 26, 2023
INSURER SECTOR INFLUENCE

Proportion of Companies with Cyber Event to Financial Filings Received

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

TIME PERIOD:
2012 – 2022

All Cyber Events n = 2566
Companies w/ Cyber Event n = 526
Total Distinct Companies with Filings Requested 2012 - 2022 n = 5876
THIRD-PARTY FINANCIAL IMPACT

(# of Events Shown in Brackets Under Loss Amounts)

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

Source: Zywave data set, Jan 26, 2023
INSURER TOP 4 EVENT TYPES OVER TIME

Top 4 Case Types, Matched NAIC Insurers, 2012 - 2022

Source: Zywave data set, Jan 26, 2023
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.
# FREQUENCY BY COMPANY: 2012 - 2022
## UNINTENTIONAL DISCLOSURE

<table>
<thead>
<tr>
<th>Company</th>
<th>Health</th>
<th>Life/Frat.</th>
<th>P/C</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>42</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>34</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

Source: Zywave data set, Jan 26, 2023
# SEVERITY: 2012 - 2022

## UNINTENTIONAL DISCLOSURE

**% of Class Action Lawsuits:** 0.35%

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

## Large Settlements, Matched NAIC Insurers, 2012 - 2022

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
<th>Persons Affected</th>
<th>Percentile</th>
<th>Estimated Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>2022</td>
<td></td>
<td></td>
<td></td>
<td>$38.0M</td>
</tr>
<tr>
<td>2017</td>
<td></td>
<td></td>
<td>10%</td>
<td>$4.3M</td>
</tr>
<tr>
<td>2017</td>
<td></td>
<td></td>
<td>25%</td>
<td>$1.2M</td>
</tr>
<tr>
<td>2017</td>
<td></td>
<td></td>
<td>50%</td>
<td>$0.9M</td>
</tr>
<tr>
<td>2013</td>
<td></td>
<td></td>
<td>75%</td>
<td>$0.9M</td>
</tr>
<tr>
<td>2017</td>
<td></td>
<td></td>
<td>100%</td>
<td>$0.6M</td>
</tr>
<tr>
<td>2016</td>
<td></td>
<td></td>
<td></td>
<td>$0.6M</td>
</tr>
<tr>
<td>2016</td>
<td></td>
<td></td>
<td></td>
<td>$0.1M</td>
</tr>
<tr>
<td>2012</td>
<td></td>
<td></td>
<td></td>
<td>$0.0M</td>
</tr>
</tbody>
</table>

**n = 862**
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.]
FREQUENCY BY COMPANY: 2012 - 2022
MALICIOUS BREACH

Source: Zywave data set, Jan 26, 2023
SEVERITY: 2012 - 2022
MALICIOUS BREACH

Large Settlements, Matched NAIC Insurers, 2012 - 2022

<table>
<thead>
<tr>
<th>Event</th>
<th>Persons Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>1</td>
</tr>
<tr>
<td>10%</td>
<td>1</td>
</tr>
<tr>
<td>25%</td>
<td>2</td>
</tr>
<tr>
<td>50%</td>
<td>42</td>
</tr>
<tr>
<td>75%</td>
<td>1,324</td>
</tr>
<tr>
<td>90%</td>
<td>26,179</td>
</tr>
<tr>
<td>100%</td>
<td>11,000,000</td>
</tr>
</tbody>
</table>

% of Class Action Lawsuits: 3.6%

Source: Zywave data set, Jan 26, 2023
EVENT TYPES: 2012 - 2022
NAIC INSURERS COMPARED TO FINANCIAL INSTITUTIONS

Data - Malicious Breach
- U.S. Insurers: 38%, Depository Institutions: 41%
- U.S. Insurer n = 2,566, 98% of Case Types Shown
- Depository Institution n = 9,129, 99.5% of Case Types Shown

Privacy - Unauthorized Contact or Disclosure
- U.S. Insurers: 9%, Depository Institutions: 39%

Data - Unintentional Disclosure
- U.S. Insurers: 8%, Depository Institutions: 34%

Data - Physically Lost or Stolen
- U.S. Insurers: 8%, Depository Institutions: 4%

Skimming, Physical Tampering
- U.S. Insurers: 4%, Depository Institutions: 4%

Phishing, Spoofing, Social Engineering
- U.S. Insurers: 5%, Depository Institutions: 2%

Identity - Fraudulent Use/Account Access
- U.S. Insurers: 2%, Depository Institutions: 2%

IT - Processing Errors
- U.S. Insurers: 2%, Depository Institutions: 2%

IT - Configuration/Implementation Errors
- U.S. Insurers: 2%, Depository Institutions: 2%

Source: Zywave data set, Jan. 26, 2023
Harder to Breach
- Larger IT Budget & Security

Bigger Payoff
- Larger quantity of desirable information

Relatively Larger Insurer

Lower Payoff –
Smaller quantity of desirable information

Easier to Breach –
Smaller IT Budget & Security

Relatively Smaller Insurer
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
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

Malicious cyber event_t = 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
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
Zywave Loss Data Insights

Jim Blinn
Zywave
Losses: Linking Disparate Sources

- Federal Trade Commission
- Office of Civil Rights
- SEC
- DoJ
- Court Records
- Government Websites
- News Articles
- FOIA Requests
- Financial Records
- Plaintiff Lawyers
- Loss Data
- Company Data
- Cyber
- D&O
- EPLI
- Fiduciary Liability
- Excess Casualty
## Comparison of Loss Types

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

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

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

Company Count

<table>
<thead>
<tr>
<th>Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>1.2%</td>
</tr>
<tr>
<td>Life</td>
<td>14.5%</td>
</tr>
<tr>
<td>Health</td>
<td>20.9%</td>
</tr>
</tbody>
</table>

# of Carriers by Type

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

Premiums N/A
- <=0 Premiums: 6.5%
- <=0 Premiums: 9.8%
Insurance Industry loss modeling analysis: 2022 Direct Written Premium by Type

P&Cs: $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

* lowest CyberCube security scores

---

**P&C**
- Superior Specialty Ins Co
- Far
- Nev
- Unil
- Cali
- Wis
- Mid
- Pen
- Jet
- Consumer Specialties Ins

**Life**
- American Mut Life Assn
- Alli
- KJZ
- Amers Life
- Ass
- Fou
- Nat
- We:
- Por
- Dakota Capital Life Ins Co

**Health**
- Magna Ins Co
- Unit
- Pro
- Digi
- Opt
- Ryc
- Sol
- Mor
- Eor
- Central Mass Hlth LLC

**Title**
- American Eagle Title Ins Co
- Nat
- Sou
- Cali
- Ape
- Title
- AHf
- ARI
- Dak
- Conestoga Title Ins Co

---

- CyberCube
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
- Overlaid company size, Large and Medium companies have above average scores. Small are average and Micro are below average

<table>
<thead>
<tr>
<th>Industry-size</th>
<th>P&amp;C</th>
<th>Life</th>
<th>Health</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Least)</td>
<td>87</td>
<td>87</td>
<td>86</td>
<td>84</td>
</tr>
<tr>
<td>Averages</td>
<td>46</td>
<td>47</td>
<td>48</td>
<td>42</td>
</tr>
<tr>
<td>(Most)</td>
<td>4</td>
<td>2</td>
<td>6</td>
<td>2</td>
</tr>
</tbody>
</table>

### (Least) Security Scores
- Life: 46
- P&C: 47
- Health: 48
- Title: 42

### (Most) Security Scores
- Life: 87
- P&C: 87
- Health: 86
- Title: 84
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

<table>
<thead>
<tr>
<th>Group</th>
<th>Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Service Provider (Omni)</td>
<td>AWS, Azure, Salesforce</td>
</tr>
<tr>
<td>Content Delivery Network Provider</td>
<td>Cloudflare, Akamai, Amazon CloudFront</td>
</tr>
<tr>
<td>Certificate Authority</td>
<td>DigiCert, Let’s Encrypt, GoDaddy</td>
</tr>
<tr>
<td>Cloud-based Enterprise File Sharing Provider</td>
<td>MS OneDrive/Azure, Google Drive, Apple iCloud</td>
</tr>
<tr>
<td>Email Services Provider</td>
<td>MS Exchange, Gmail for Business, Zoho Mail</td>
</tr>
<tr>
<td>DNS Provider</td>
<td>Route53, Cloudflare, GoDaddy</td>
</tr>
<tr>
<td>Operating System - Server</td>
<td>Ubuntu, Unix, Linux</td>
</tr>
<tr>
<td>Content Management System Provider</td>
<td>WordPress, Adobe Experience Manager, HubSpot CMS</td>
</tr>
<tr>
<td>E-Commerce Platform</td>
<td>Shopify, Magento, Amazon</td>
</tr>
</tbody>
</table>
3. What type of event(s) can cause the largest losses to the Insurance Industry?

<table>
<thead>
<tr>
<th>Five highest loss scenario classes</th>
<th>Loss type</th>
<th>SPoF exploited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ransomware</td>
<td>File Sharing Provider</td>
<td></td>
</tr>
<tr>
<td>Data Theft</td>
<td>Fund Administrator</td>
<td></td>
</tr>
<tr>
<td>Destructive Malware</td>
<td>Cloud Services Provider</td>
<td></td>
</tr>
<tr>
<td>Ransomware</td>
<td>Endpoint Operating System</td>
<td></td>
</tr>
<tr>
<td>Data Theft</td>
<td>Enterprise Payroll Provider</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Five lowest loss scenario classes</th>
<th>Loss type</th>
<th>SPoF exploited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash Theft</td>
<td>Financial Transaction Provider</td>
<td></td>
</tr>
<tr>
<td>Data Theft</td>
<td>E-Commerce Platform</td>
<td></td>
</tr>
<tr>
<td>Ransomware</td>
<td>Medical Device Manufacturer</td>
<td></td>
</tr>
<tr>
<td>Data Theft</td>
<td>Mobile Point of Sale Vendor</td>
<td></td>
</tr>
<tr>
<td>Extortion</td>
<td>Point of Sale Vendor</td>
<td></td>
</tr>
</tbody>
</table>

www.cybcube.com
### 4. What is the financial cost of cyber attacks on the US insurance industry?

<table>
<thead>
<tr>
<th>Annual Probability</th>
<th>US Insurance Industry</th>
<th>P&amp;C</th>
<th>Life</th>
<th>Health</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0% or 1-in-50yr</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>4,267</td>
<td>1,167</td>
<td>1,738</td>
<td>1,387</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>1.0% or 1-in100yr</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>54</td>
</tr>
<tr>
<td>5,782</td>
<td>1,585</td>
<td>2,458</td>
<td>1,896</td>
<td>54</td>
<td></td>
</tr>
<tr>
<td>0.4% or 1-in-250yr</td>
<td>8,284</td>
<td>2,077</td>
<td>3,642</td>
<td>87</td>
<td></td>
</tr>
<tr>
<td>0.2% or 1-in-500yr</td>
<td>11,501</td>
<td>3,101</td>
<td>4,917</td>
<td>122</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Losses shown in $millions.

Individual Life & Health company contribution to loss is higher.
5. Which companies drive the most losses – on average vs in a cyber catastrophe?

### P&C

#### Average Annual Loss
- State Farm Mut Auto Ins Co
- United Specialty Ins Co
- State Farm Fire & Cas Co
- Nations Ins Co
- Federal Ins Co

#### 1-in-250yr cat
- State Farm Mut Auto Ins Co
- United Specialty Ins Co
- State Farm Fire & Cas Co
- Nations Ins Co
- United Serv Automobile Assn

### Life

#### Average Annual Loss
- Health Net Life Ins Co
- American Nat Life Ins Co of NY
- Globe Life Ins Co of NY
- Wysh Life & Hlth Ins Co
- Reliance Standard Life Ins Co

#### 1-in-250yr cat
- Health Net Life Ins Co
- American Nat Life Ins Co of NY
- Wysh Life & Hlth Ins Co
- Reliance Standard Life Ins Co
- Globe Life Ins Co of NY

### Health

#### Average Annual Loss
- Pacificare Life & Hlth Ins Co
- Clover Ins Co
- Golden Security Ins Co
- Anthem Ins Co Inc
- Cigna Dental Hlth of NC Inc

#### 1-in-250yr cat
- Pacificare Life & Hlth Ins Co
- Clover Ins Co
- Golden Security Ins Co
- Anthem Ins Co Inc
- Cigna Dental Hlth of NC Inc

### Title

#### Average Annual Loss
- Conestoga Title Ins Co
- Attorneys Title Guaranty Fund Inc
- National Title Ins Of NY Inc
- Alliant Natl Title Ins Co Inc
- Real Advantage Title Ins Co

#### 1-in-250yr cat
- Conestoga Title Ins Co
- Alliant Natl Title Ins Co Inc
- Attorneys Title Guaranty Fund Inc
- National Title Ins Of NY Inc
- Real Advantage Title 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

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
Cyber Catastrophe Modeling: Q&A
Rebecca Bole, Shaveta Gupta
**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**

- Single Point of Failure Technology
  - Amazon Web Services

- Dependent Companies
  - Abercrombie & Fitch Co.
  - Pacific Gas and Electric Company
  - ... USAA Real Estate Company

---

**Company to SPOFs Relationships**

- Company
  - Walmart

- Technology Dependencies
  - Amazon Web Services
  - Shopify
  - ... WooCommerce
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

<table>
<thead>
<tr>
<th>1. Exposure</th>
<th>Property</th>
<th>Cyber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creates aggregation potential</td>
<td>![California map]</td>
<td>![Amazon Web Services]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2. Peril</th>
<th>Property</th>
<th>Cyber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency &amp; severity of events</td>
<td>![House and hurricane]</td>
<td>![Lock and chain]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3. Vulnerability</th>
<th>Property</th>
<th>Cyber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Susceptibility to peril</td>
<td>![Vulnerability chart]</td>
<td>![CVE-2021-44228]</td>
</tr>
</tbody>
</table>
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