Actuarial Quantification of Cyber Risk

Professor Shaun Wang, FCAS, CERA
Dr. Jing Rong Goh

Nanyang Business School
Part 1. Highlights of the Singapore Cyber Risk Management project (CyRiM)
Cyber Risk Management Project
(2016-2019)

Goals
1. Cyber Loss Database
2. Risk Analytics
3. Recommend Policy

Industry Partners
SCOR, Aon, MSIG, Lloyd’s, TransRe
Big Picture: Cyber Loss >> Cybersecurity Budget >> Cyber Insurance

• Annual global cyber-breach losses:
  ➢ ($450 billion, $3 trillion)

• Annual global cybersecurity budget
  ➢ $100 billion

• Annual global cyber insurance premium:
  ➢ ($1.7 billion, $3.5 billion)

• Annual global non-life insurance premium
  ➢ $2234 billion

• So, what is the value of cyber insurance?
3 components

• **Threat**: type/number $n$ of cyberattacks
• **Vulnerability**: probability $v$ of successful breach
• **Harm**: economic loss, $L$, of cyber breach
• **Annual loss expectancy** $= n \cdot v \cdot L$
Attack surface

- Common phrase among CISOs
  - Known-known
  - Known-unknown
  - Unknown-unknown
Insight: Threats-Vulnerability are inter-linked to the Asset Value!

Fast-growing Dark Web
Malware & Ransomware (arms race)
Effectiveness of Security Investment in addressing “vulnerability”
Gordon-Loeb Model and Variations

1) Exponential Power [Gordon-Loeb Model]
\[ v(z) = v(z_{\downarrow 0}) \uparrow (z/z_{\downarrow 0}) \uparrow \alpha \]

2) Proportional Hazard
\[ H(z) = H(z_{\downarrow 0}) \uparrow (z/z_{\downarrow 0}) \uparrow \alpha \]
\[ v(z) = 1 - [1 - v(z_{\downarrow 0})] \uparrow (z/z_{\downarrow 0}) \uparrow -\alpha \]

3) Wang Transform
\[ \uparrow -1 \ (v(z)) = \uparrow -1 \ (v(z_{\downarrow 0})) - \alpha \ln(z/z_{\downarrow 0}) \]

\( z_{\downarrow 0} = f(\text{Revenue}) \)
\( z/z_{\downarrow 0} \)
Optimal Security Spending

• A firm’s asset value $R$, spending $z^* \uparrow$ minimizes
  
  \[
  \text{Total Cost: } \{z + v(z) \cdot R\}
  \]

• For Exponential Power and Proportional Hazard curves, the optimal spending
  
  $$z^* \leq \frac{\alpha}{e} \cdot R \quad \text{[Gordon-Loeb (2002)]}$$

• For Wang Transform, the optimal spending
  
  $$z^* \leq \frac{\alpha}{\sqrt{2\pi}} \cdot R$$

• Key: security spending proportional to asset value
Mapping of Cyber-Harm and Its Propagation through Supply-Chain

• “A taxonomy of cyber-harms: Defining the impacts and cyber-attacks and understanding how they propagate” (ref. Agrafiotis et al, 2018)

• The authors advocate for “an asset-oriented assessment model”
  1) Identify core assets and potential harm to assets
  2) Measure indirect harm (propagation) for all stakeholders
  3) Assess emergent threats, and choose security measures to treat harm
Illustrative Comparison of Cost Structure

Auto Insurance vs Cyber Insurance
## Traditional vs. Cyber Insurance

<table>
<thead>
<tr>
<th>Traditional Insurance</th>
<th>Cyber Insurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk is Static</td>
<td>Cyber Risk is Dynamic</td>
</tr>
<tr>
<td>Contact once per year</td>
<td>Need close contacts pre-event &amp; post-event</td>
</tr>
<tr>
<td>Client does not want to hear from insurers</td>
<td>Client expects hands-on help!</td>
</tr>
<tr>
<td>Law of large numbers in risk diversification</td>
<td>Economics of scale in providing services</td>
</tr>
</tbody>
</table>
Cyber Insurance Product Innovation

• Use a portion (50%) of premium to help clients:
  1) Increase knowledge and awareness
  2) Quantify cyber risks
  3) Implement risk reduction

• Even if spending 50% premium on helping clients with risk reduction, the gross premium can still be cheaper!!

• Or, market product as risk mitigation services, and then provide assurance (guarantee)
Part II. Cyber Risk Quantification

Database,
Data Analysis,
AI/ML
Applications
Overview

• Spectrum of Cyber Breaches
• Proprietary Database
• Some interesting insights
• Hidden layer: AI/ML Algorithm
Spectrum of Cyber Breaches

• Hacking (unauthorized access)
  a) Malware including ransomware
  b) Phishing
  c) Distributed Denial of Service attacks
  d) Man in the middle attacks
  e) SQL injection
  f) Zero-day exploits

• Data Breach (unauthorized transfer of data)
  a) Personal Data and Privacy Breach
  b) Leak of Business Data and Intellectual Property

• Cyber-enabled Financial Frauds (unauthorized transfer of money)
  a) Business Email Compromise
  b) Confidence/Romance Fraud
  c) Blackmail and cyber extortion

• Cyber Access to Industry Control (unauthorized control of operations)
Proprietary Database

• Primary data source is compiled by the Insurance Risk and Finance Research Center (IRFRC) for the Cyber Risk Management (CyRiM) Project.

• Collaboration with various industry partners, including:
  – Global insurance companies
  – Cyber-risk consulting companies
  – Fortune 500 telecommunications and media company
  – Among many others

• Supplemented our data with external sources
Proprietary Database

- Time: 2014 – 2019
- 3,189 observations of unique cyber breach events
- Each observation records more than 600 unique features, including the target, class, country, attack type, a list of cyber incident triggers, etc.
- Each observation also records a list of 11 unique outcome events (such as assets affected, breached records, operations disrupted, etc).
Some interesting insights

- Relative weights
- Loss types distribution
- Correlation of insurance claims with revenue
## Relative weights

<table>
<thead>
<tr>
<th></th>
<th>People &amp; Process (θ)</th>
<th>Technology &amp; Tools (1-θ)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ransomware</td>
<td>≤ 10%</td>
<td>≥ 90%</td>
</tr>
<tr>
<td>DDOS</td>
<td>20% - 30%</td>
<td>70% - 80%</td>
</tr>
<tr>
<td>APT via Phishing</td>
<td>40% - 60%</td>
<td>40% - 60%</td>
</tr>
<tr>
<td>Wire transfer fraud</td>
<td>70% - 80%</td>
<td>20% - 30%</td>
</tr>
<tr>
<td>Romance Scam</td>
<td>≥ 90%</td>
<td>≤ 10%</td>
</tr>
</tbody>
</table>
CyRiM Database of Cyber Insurance Claims (non-US)

- Main losses
  a) Fraudulent money transfer
  b) Business disruption costs

Summary of Cyber Insurance Claim Data
Cyber Insurance Claims are Correlated with Revenue

Regression
R-squared: 0.4234
Hidden layer: AI/ML Algorithm

- Recall: Our proprietary database consists of >3,000 observations and >600 features
- It’ll be easy for us to directly apply out-of-the-box AI algorithms, and achieve high in-sample accuracy. **BUT** overfitting will be an obvious problem.
- Need a way to circumvent this problem.
Hidden layer: AI/ML Algorithm
Hidden layer: AI/ML Algorithm

- Least Absolute Shrinkage and Selection Operator (LASSO)

$$
\min_{\beta} \quad \frac{1}{n} \sum_{i=1}^{n}(y_i - \mathbf{x}_i^T \mathbf{\beta})^2 + \lambda \sum_{j=1}^{p} |\beta_j|
$$

$$
\beta_L = \arg \min_{\beta} \quad \sum_{i=1}^{n}(y_i - \mathbf{x}_i^T \mathbf{\beta})^2 \quad \text{s.t.} \quad \sum_{j=1}^{p} |\beta_j| < \tau
$$

- Information criteria:
  - AIC, BIC, AICc, EBIC

- LASSO is only one of the hidden layer
Hidden layer: AI/ML Algorithm

- This hidden layer **automatically** selects the subset of features.
- **Some result:** Depending on the outcome event, the selected features run from **between 14 to 29 features**
- We also conduct undersampling as well to account for the class imbalance problem
Hidden layer: AI/ML Algorithm

- Some results:

<table>
<thead>
<tr>
<th>Information Criterion: AIC Summary</th>
<th>TruePN</th>
<th>SD</th>
<th>Mean</th>
<th>SD</th>
<th>TruePN</th>
<th>SD</th>
<th>Mean</th>
<th>SD</th>
<th>Mean</th>
<th>SD</th>
</tr>
</thead>
<tbody>
<tr>
<td>StillPartyTransfer</td>
<td>0.8590</td>
<td>0.0080</td>
<td>0.8150</td>
<td>0.0057</td>
<td>0.8272</td>
<td>0.0053</td>
<td>0.7895</td>
<td>0.0070</td>
<td>21.30</td>
<td>2.71</td>
</tr>
<tr>
<td>BreachInRecords</td>
<td>0.8830</td>
<td>0.0058</td>
<td>0.8384</td>
<td>0.0028</td>
<td>0.8806</td>
<td>0.0140</td>
<td>0.8853</td>
<td>0.0144</td>
<td>18.40</td>
<td>1.78</td>
</tr>
<tr>
<td>AssetsAffected</td>
<td>0.7784</td>
<td>0.0154</td>
<td>0.7759</td>
<td>0.0185</td>
<td>0.7699</td>
<td>0.0239</td>
<td>0.7659</td>
<td>0.0264</td>
<td>15.20</td>
<td>1.48</td>
</tr>
<tr>
<td>LocationAffected</td>
<td>0.7715</td>
<td>0.0064</td>
<td>0.7665</td>
<td>0.0067</td>
<td>0.7590</td>
<td>0.0235</td>
<td>0.7535</td>
<td>0.0203</td>
<td>10.50</td>
<td>0.72</td>
</tr>
<tr>
<td>PersonEmployeeAffected</td>
<td>0.7291</td>
<td>0.0154</td>
<td>0.7227</td>
<td>0.0144</td>
<td>0.6906</td>
<td>0.0258</td>
<td>0.8870</td>
<td>0.0505</td>
<td>17.40</td>
<td>1.84</td>
</tr>
<tr>
<td>InaccessibleModifiedSystem</td>
<td>0.7411</td>
<td>0.0050</td>
<td>0.7662</td>
<td>0.0042</td>
<td>0.7463</td>
<td>0.0275</td>
<td>0.7673</td>
<td>0.0203</td>
<td>16.70</td>
<td>3.65</td>
</tr>
<tr>
<td>OperationsDisrupted</td>
<td>0.7538</td>
<td>0.0073</td>
<td>0.7551</td>
<td>0.0108</td>
<td>0.7374</td>
<td>0.0159</td>
<td>0.7397</td>
<td>0.0158</td>
<td>27.90</td>
<td>0.89</td>
</tr>
<tr>
<td>AttributedBy3rdPartyEcosystem</td>
<td>0.6640</td>
<td>0.0164</td>
<td>0.6217</td>
<td>0.0664</td>
<td>0.6460</td>
<td>0.0244</td>
<td>0.3880</td>
<td>0.0709</td>
<td>17.10</td>
<td>2.73</td>
</tr>
<tr>
<td>IncidentResponseCost</td>
<td>0.8031</td>
<td>0.0050</td>
<td>0.7975</td>
<td>0.0049</td>
<td>0.8033</td>
<td>0.0160</td>
<td>0.7983</td>
<td>0.0165</td>
<td>14.50</td>
<td>12.59</td>
</tr>
<tr>
<td>RecoveryCost</td>
<td>0.8053</td>
<td>0.0090</td>
<td>0.8155</td>
<td>0.0097</td>
<td>0.8045</td>
<td>0.0228</td>
<td>0.8145</td>
<td>0.0207</td>
<td>28.00</td>
<td>2.90</td>
</tr>
<tr>
<td>CompromiseAssessment</td>
<td>0.7730</td>
<td>0.0163</td>
<td>0.7666</td>
<td>0.0154</td>
<td>0.7503</td>
<td>0.0217</td>
<td>0.7648</td>
<td>0.0267</td>
<td>14.70</td>
<td>4.76</td>
</tr>
<tr>
<td>Average</td>
<td>0.7782</td>
<td>0.0094</td>
<td>0.7738</td>
<td>0.0143</td>
<td>0.7651</td>
<td>0.0235</td>
<td>0.7663</td>
<td>0.0289</td>
<td>11.18</td>
<td>3.59</td>
</tr>
</tbody>
</table>
Hidden layer: AI/ML Algorithm

- Accuracy defined as:
  - Sensitivity
  - Specificity
  - F1-score

- Some results:
- Without the LASSO hidden layer, our results have a high fit to training sample, but accuracy to testing sample is poor
- Including this hidden layer, the within-sample and out-of-sample accuracy is high and consistent
Hidden layer: AI/ML Algorithm

• **Some results:**
  
  • Our algorithm is also able to **identify the key points of vulnerabilities** within a firm’s cyber security posture.
  
  • Our algorithm also describes the firms that are most susceptible to different types of attacks.
    – Industry type
    – Firm size
    – Country of operation
    – etc
References


https://ssrn.com/abstract=3064533


Contacts:

- Professor Shaun Wang, FCAS, CERA
  shaun.wang@ntu.edu.sg
  shaunwang777@me.com

- Dr. Jing Rong Goh
  jingrong.goh@ntu.edu.sg
  gohjingrong@Hotmail.com