Emerging Issues in Insurance

Association of Insurance Compliance Professionals
Northwest Chapter E-Day
Seattle, Washington
June 2, 2016

Rich J. Fidei, Esq.
Shareholder
Insurance Regulatory & Transactions Practice
Greenberg Traurig
Disclaimer

The materials in this presentation are intended to provide a general overview of the issues contained herein and are not intended nor should they be construed to provide specific legal or regulatory guidance or advice. If you have any questions or issues of a specific nature, you should consult with appropriate legal or regulatory counsel to review the specific circumstances involved.
General Overview

- CyberSecurity
- Big Data
- Price Optimization
- Corporate Governance
Emerging Cyber Issues for the Insurance Industry
Emerging Cyber Issues for the Insurance Industry

- Threats
  - Data Breaches
  - Theft of Intellectual Property
  - Business Interruption

- Cyber Liability Insurance
  - Coverage
  - Underwriting

- State/Federal Regulatory Development
Background

> Insurers and regulators consider cyber security threats to be one of their most significant risks

> Breaches are inevitable and the potential damage is tremendous

> Risks include:
  - Data loss
  - Compromise of personal information
  - Theft of intellectual property
  - Business interruption
## Loss Categories

**LOSS CATEGORIES DERIVING FROM CYBER ATTACKS AND NON-MALICIOUS IT FAILURES**

<table>
<thead>
<tr>
<th>Loss category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A  Intellectual property (IP) theft</td>
<td>Loss of value of an IP asset, expressed in terms of loss of revenue as a result of reduced market share.</td>
</tr>
<tr>
<td>B  Business interruption</td>
<td>Lost profits or extra expenses incurred due to the unavailability of IT systems or data as a result of cyber-attacks or other non-malicious IT failures.</td>
</tr>
<tr>
<td>C  Data and software loss</td>
<td>The cost to reconstitute data or software that has been deleted or corrupted.</td>
</tr>
<tr>
<td>D  Cyber extortion</td>
<td>The cost of expert handling for an extortion incident, combined with the amount of the ransom payment.</td>
</tr>
<tr>
<td>E  Cyber crime/cyber fraud</td>
<td>The direct financial loss suffered by an organization arising from the use of computers to commit fraud or theft of money, securities or other property.</td>
</tr>
<tr>
<td>F  Breach of privacy event</td>
<td>The cost to investigate and respond to a privacy breach event, including IT forensics and notifying affected data subjects. Third-party liability claims arising from the same incident. Fines from regulators and industry associations.</td>
</tr>
<tr>
<td>G  Network failure liabilities</td>
<td>Third-party liabilities arising from certain security events occurring within the organization’s IT network or passing through it in order to attack a third party.</td>
</tr>
<tr>
<td>H  Impact on reputation</td>
<td>Loss of revenues arising from an increase in customer churn or reduced transaction volumes, which can be directly attributed to the publication of a defined security breach event.</td>
</tr>
<tr>
<td>I  Physical asset damage</td>
<td>First-party loss due to the destruction of physical property resulting from cyber-attacks.</td>
</tr>
<tr>
<td>J  Death and bodily injury</td>
<td>Third-party liability for death and bodily injuries resulting from cyber-attacks.</td>
</tr>
<tr>
<td>K  Incident investigation and response costs</td>
<td>Direct costs incurred to investigate and “close” the incident and minimize post-incident losses. Applies to all the other categories/events.</td>
</tr>
</tbody>
</table>

Source: Marsh
Anthem Breach

- Announced in February, 2015
- Hackers breached Anthem’s IT systems
- Compromised information included insureds’ names, birthdays, social security numbers, addresses, emails, and employment information
- Led to swift regulatory and NAIC reaction
Insurance & Cybersecurity

> Insurance companies store large amounts of sensitive information/data on consumers, their employees and insureds
  - Length of storage of information is greater for life insurers

> Breaches that occur can/will compromise huge data sets and lead to significant exposure

> Regulators are requiring more diligence of insurers to protect consumer data from cyber threats
Cyber Coverage

> Most commercial general liability ("CGL") policies do not cover cyber risks
  - Many company executives do not know or are unsure whether their company is adequately insured for cyber risks

> To adequately cover cyber risk, companies must purchase special cyber liability policies
Cyber Coverage – Recent Cases

> The extent to which CGL policies cover cyber risks is unsettled

– *Travelers v. Portal Healthcare Solutions*: the availability online of information is “publication” of the information under a CGL policy

– *Zurich American Insurance Co. v. Sony*: hackers’ theft of confidential customer data is “publication” of the information

  ▪ Settled prior to appeals court’s decision

– *Recall Total Information Management v. Federal Insurance Co.*: physical loss of tapes containing personal employee information is not “publication”

> Insurers are beginning to exclude these risks
Underwriting Difficulties

> Cyber risks remain difficult to underwrite
  > Limited actuarial data
  > High potential costs
  > Policies must be closely tailored to each insured

> Result is higher rates
Trends

> Demand for cyber liability insurance has increased
  > Estimated total annual cyber insurance premiums:*
    > 2012: $1.0 billion
    > 2013: $1.3 billion
    > 2014: $2.0 billion
    > 2015: $2.75 billion

> Premium rates have increased
  > High profile attacks have driven recent increases

> Much of the growth in demand is from small and mid-sized businesses
  > However, large retailers have seen a decrease in capacity

Source: The Betterley Report
Recent Federal & State Legislation

> 2014: Five federal cyber security bills became law
> 2015: Federal legislation
    ▪ Authorizes private sector entities to share cyber threat information with each other and the federal government; provides a safe harbor for good faith sharing; and authorizes defensive measures
  - Data Security Act of 2015
    ▪ Would provide federal data security standards
    ▪ Opposed by the NAIC
> 47 states have enacted cybersecurity legislation
NAIC Cybersecurity Task Force

Task Force’s Larger Plan

- Model Laws
  - Health Information Privacy Model Act (Model 55)
  - Privacy of Consumer Financial and Health Information Regulation (Model 672)
  - Standards for Safeguarding Customer Information Model Regulation (Model 673)
  - Insurance Fraud Prevention Model Act (Model 680)
  - Insurance Data Security Model Law

- NAIC Roadmap for Cybersecurity Consumer Protections (formerly the Cybersecurity Bill of Rights)
NAIC Cybersecurity Roadmap

> The NAIC Roadmap for Cybersecurity Consumer Protections was adopted by the Executive Committee on December 17, 2015
  - Outlines what consumers have a right to expect of insurance carriers and agents with regard to data collection and protection

> Issue: How the Roadmap protections dovetail with existing state consumer protection laws
Consumers have the right to:

1. Know the information collected and stored by their insurer or its third party contractors
2. Expect companies to have privacy policies explaining their data collection practices
3. Expect companies to take reasonable steps to prevent unauthorized access to personal information
4. Receive notice from a company in the event of a breach
5. Receive one year of identity theft protection paid by the company in the event of a breach
6. If the consumer’s identity is stolen, take action to protect credit scores and prevent debt collection on fraudulent charges
Insurance Data Security Model Law


> The model law would establish requirements for insurance entities to prepare for and manage breaches

  − If widely adopted, it would introduce more uniformity to the states’ cybersecurity laws
Insurance Data Security Model Law

> Data breach: “the unauthorized acquisition of personal information”

> Personal information: includes financial information, health information, and other private information of a consumer or entity

> Licensees must maintain an “Information Security Program”

   - The scale and scope of Information Security Programs should be appropriate in relation to insurers’ size and complexity, the nature of their activities, and the sensitivity of the information they maintain
Insurance Data Security Model Law

> Licensees supervise third party contractors to ensure that they take appropriate measures to protect customer data

  - Contracts with third parties must require the vendor to maintain an Information Security Program

> In the event of a data breach, licensees must provide notice to regulators, law enforcement, consumers, and consumer credit agencies

> The model law explicitly allows regulators to conduct examinations of insurers’ IT security systems
Insurance Data Security Model Law

> Concerns:

- Difficulties for small insurance agencies to comply with all requirements
- Difficulty in supervising outside contractors
- Unnecessary preemption of other state laws
- Is an insurance industry specific data security law necessary? Duplicative standards?
- Third-party liability and extent of regulatory authority.
- Concerns with the process of development
Key Take-Aways

> Statutory and regulatory requirements are still in the early stages of development
  - Regulators are still learning how best to deal with cyber threats

> Regulators will devote additional attention to cyber threat preparedness, including through examinations
  - Preparing in advance is key – internal and external controls
  - Cyber breach plans

> Threats continue to evolve
Emerging Issues in Big Data
Overview

> What is Big Data?
  - Broad definition

> Insurance Industry Use
  - Set rates
  - Predict Risks - Underwriting
  - Marketing
  - Claims Management

> How do you regulate?
  - NAIC Working Group
Big Data and the Insurance Industry

> Rates and Underwriting
  - Automotive
  - Property & Casualty
  - Flood

> Marketing

> Fraud Detection & Prevention
Big Data and Insurance Regulation

> Use of Big Data by Regulators
  – Collecting Data to Assist in Regulating the Industry
  – Price Transparency

> Setting Legal Standards on Industry Use
  – Privacy/Confidentiality Concerns
  – For what purpose is data used?
  – Issue of Disclosure
NAIC Big Data Working Group

> Comprehensive Approach to Big Data:
  - Defining “Big Data”
  - Learning how it is used by Insurance Companies and Regulators

> Consumer Privacy Protections
  - How much information is too much information?

> Embracing the New World of Statistical Analysis
  - Opportunities and Risks
Key Take-Aways

> Big Data is here to stay:
  - Insurance Industry has welcomed it
  - Regulators want to understand it
    - How do they use it?
    - How do they regulate it?

> Approach to Regulation
  - Consumer Privacy Concerns
  - Benefit vs. Risk

> NAIC Model Law or other guidance
Emerging Issues in Price Optimization
Definition

> “The process of using sophisticated tools and models to quantify other business considerations such as marketing goals, profitability or policyholder retention is referred to as ‘price optimization’.”

> NAIC Price Optimization White Paper adopted by the Property and Casualty Insurance (C) Committee on November 21, 2015
Concerns

> Concerns that low-income consumers will ultimately pay higher insurance rates

> Many states have issued bulletins prohibiting price optimization

  - Florida Bulletin OIR-15-04M: “The use of price optimization results in rates that are unfairly discriminatory in violation of Sections 627.062 and 627.0651, Florida Statutes”
State Treatment

> The definition of price optimization differs from state to state:

- **Ohio:** Price optimization is “an insurer’s practice of varying premiums based upon factors that are unrelated to risk of loss in order to charge each insured the highest price that the market will bear”

- **California:** “Price Optimization is defined as any method of taking into account an individual’s or class’s willingness to pay a higher premium relative to other individuals or classes”

- **Washington:** “The practice of price optimization involves and insurer’s use of sophisticated statistical analysis, often using non-insurance data, to predict a policyholder’s likelihood of renewing a policy”
Litigation

> There have been few cases dealing with insurers’ use of price optimization, but there is a potential for expensive class action lawsuits
  > The class actions that have been filed have been dismissed

> The plaintiffs in the cases made claims of unjust enrichment, ill-gotten gains, and violations of unfair insurance trade practices laws
  > The defendant companies responded by raising the filed rate doctrine defense

> The viability of these claims and defenses remain unknown until a case is brought to trial
Key Take-Aways

> Many insurance departments will likely ban price optimization where it is used to determine rates based on a customer’s willingness to pay
  - There may remain some gray area where it is used to base rates on other non-cost factors

> The potential for class action lawsuits remains unknown

> Can companies ever use assessment of willingness to pay?
Emerging issues in Corporate Governance
Overview

> Corporate Governance Annual Disclosure (CGAD)
  - Determining which entity reports
  - What should be included in CGAD
  - Lead State Filing
  - Need to establish and document organization and procedures
Corporate Governance Annual Disclosure (CGAD)

> Review and Oversight
  - Insurance Commissioners take a closer look at an insurer or insurance group’s corporate governance

> Annual Disclosure Filing
  - Who reports?
    - Controlling Party
    - Holding Company
    - Legal Entity/Insurance Company
CGAD Content

> CGAD must be detailed and address:
  
  - Insurer’s corporate governance framework and structure
  - Policies and practices of its board of directors and committees
  - Policies and practices directing senior management
  - Internal oversight procedures
Overall Governance Issues

> Broad Risk Management
> Group-level Evaluations
> Internal Controls
> Director and Management Duties
> Confidentiality
> Sanctions
> Prevent Criminal Exposure
Key Take-Aways

> State Regulators
  - More oversight of corporate structure and risk
  - Identification and mitigation

> Insurance and Insurance Groups
  - Structure and controls

> New Regulation
  - Fairly new legislation being adopted
  - Look out for the promulgation of new rules and regulations related to CGAD and ORSA reporting
Any Questions?
Contact Information

Rich J. Fidei, Esq.
Shareholder
Insurance Regulatory & Transactions Practice

Greenberg Traurig, P.A.
401 East Las Olas Boulevard,
Suite 2000
Fort Lauderdale, FL  33301
Tel: 954-768-8286
fideir@gtlaw.com
www.gtlaw.com