


DATA AND CYBERSECURITY

Legal and Regulatory Developments

Casualty Actuarial Society
2016 Annual Meeting
November 16, 2016
Orlando, Florida

Fred Karlinsky Shareholder & Co-Chair Insurance Regulatory and Transactions Practice	Lori Nugent Shareholder Cybersecurity, Privacy and Crisis Management
---	---

GREENBERG TRAURIG, LLP | ATTORNEYS AT LAW | WWW.GTLAW.COM
©2016 Greenberg Traurig, LLP. All rights reserved.



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.

©2016 Greenberg Traurig, LLP. All rights reserved. | gtlaw.com

 GreenbergTraurig

General Overview

- > Cyber Regulatory Landscape
- > Federal Cyber Regulations & Initiatives
- > NAIC/States Cyber Regulations
- > IAIS Study on Cyber Risk

©2016 Greenberg Traurig, LLP. All rights reserved. | gtlaw.com 3

 GreenbergTraurig



Cyber Regulatory Landscape

GREENBERG TRAUIG, LLP | ATTORNEYS AT LAW | WWW.GTLAW.COM
©2016 Greenberg Traurig, LLP. All rights reserved. 4

 GreenbergTraurig

Insurance & Cybersecurity

- > Insurance companies store large amounts of sensitive information/data on their employees and insureds
- > 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

©2016 Greenberg Traurig, LLP. All rights reserved. | gtlaw.com 5

 GreenbergTraurig



Federal Legislation & Initiatives

GREENBERG TRAUIG, LLP | ATTORNEYS AT LAW | WWW.GTLAW.COM
©2016 Greenberg Traurig, LLP. All rights reserved. 6

GT GreenbergTraurig

Recent Federal & State Legislation

- > 2015: Federal legislation
 - Cybersecurity Act of 2015 – passed in December 2015
 - 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

©2016 Greenberg Traurig, LLP. All rights reserved. | gtlaw.com

7

GT GreenbergTraurig

Health Insurance Portability & Accountability Act

- > Federal protections for patient health information
 - Applies to “Covered Entities” and “Business Associates” of Covered Entities
- > Regulations include:
 - Privacy Rule
 - Security Rule
 - Breach Notification Rule

©2016 Greenberg Traurig, LLP. All rights reserved. | gtlaw.com

8

GT GreenbergTraurig

HIPAA Security Rule

- > Minimum security standards for protecting electronic Protected Health Information (ePHI)
- > Safeguards & Requirements
 - Administrative safeguards
 - Physical safeguards
 - Organizational safeguards
 - Policies and procedures
- > Strong cybersecurity practices will help safeguard this information

©2016 Greenberg Traurig, LLP. All rights reserved. | gtlaw.com 9

GT GreenbergTraurig

SEC Issues Cybersecurity Guidance

- > Guidance Update for investment advisors and registered investment companies
 - Investment companies, broker-dealers and investment advisers must:
 - Review their cybersecurity preparedness
 - Update their policies and procedures
 - Examine their potential vulnerabilities and assess compliance with SEC regulations
- > SEC makes clear that the failure implement adequate cybersecurity protections could raise serious regulatory compliance issues


©2016 Greenberg Traurig, LLP. All rights reserved. | gtlaw.com 10

 GreenbergTraurig

SEC Safeguards Rule

- > Safeguards Rule requires registered brokers-dealers and investment advisers to adopt written policies and procedures to:
 - Insure the security and confidentiality of customer records and information;
 - Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
 - Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer


©2016 Greenberg Traurig, LLP. All rights reserved. | gtlaw.com 11

 GreenbergTraurig

SEC Safeguards Rule


- > June 8, 2016 SEC order:
 - An employee of a broker-dealer/investment advisory firm misappropriated data from approximately 730,000 customer accounts
 - The data subsequently surfaced online
 - Someone likely hacked the employee's personal server and stole the data from him
 - SEC found that the firm had violated the Safeguards Rule because its policies and procedures were not reasonably designed to meet the objectives of the Rule

©2016 Greenberg Traurig, LLP. All rights reserved. | gtlaw.com 12



NAIC/States Cyber Regulations

GREENBERG TRAURIG, LLP | ATTORNEYS AT LAW | WWW.GTLAW.COM
©2016 Greenberg Traurig, LLP. All rights reserved.




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)

©2016 Greenberg Traurig, LLP. All rights reserved. | gtlaw.com


14

 GreenbergTraurig

Insurance Data Security Model Law

- > The Cybersecurity Task Force released a draft Insurance Data Security Model Law in August 2016
- > 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


©2016 Greenberg Traurig, LLP. All rights reserved. | gtlaw.com 15

 GreenbergTraurig

Insurance Data Security Model Law

- > Data breach: “the unauthorized acquisition, release or use 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”
 - Must be commensurate with the size and complexity of the licensee, the nature and scope of the licensee’s activities and the sensitivity of the personal information in the licensee’s possession


©2016 Greenberg Traurig, LLP. All rights reserved. | gtlaw.com 16

 GreenbergTraurig

Insurance Data Security Model Law

- > Licensees supervise third party contractors to ensure that they take appropriate measures to protect customer data
 - Can only contract with third parties who are capable of maintaining appropriate safeguards
- > 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

©2016 Greenberg Traurig, LLP. All rights reserved. | gtlaw.com 17

 GreenbergTraurig

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?
 - Concerns with the process of development

©2016 Greenberg Traurig, LLP. All rights reserved. | gtlaw.com

New York Proposed Cybersecurity Regulation

- > Applies to Insurance Companies, Banks and other Financial Services
- > New standards for financial services companies to protect consumers from cyber threats
 - Annual Risk Assessment
 - Designation of Key Personnel to oversee cybersecurity measures within company
 - Internal policies and procedures that will ensure adequate ability to detect cyber risks and/or mitigate and prevent lasting harm from cyber breach

NYS Regulation vs. NAIC Model Law

- > Similarities
 - Cybersecurity Program requirements
 - Implementation of internal policies
 - Designation of Personnel responsible for Cybersecurity regulation compliance
 - Continuous self-assessment for cyber threat vulnerability
- > Differences
 - NAIC Model Law more provisions directed to ensuring protection of consumer information
 - New York Regulation applies to the banking industry



GT GreenbergTraurig

International Influence

GREENBERG TRAURIG, LLP | ATTORNEYS AT LAW | WWW.GTLAW.COM
©2016 Greenberg Traurig, LLP. All rights reserved.



GT GreenbergTraurig

IAIS Paper on Cyber Risk to Insurance Sector

- > Highlighted cybersecurity weaknesses involving insurance
 - Main cause of cyber breaches and how to shore up weak points in the sector
- > Advocated for cyber resilience
 - What are the best practices to protect against cyber threats
- > Reviewed supervisory/regulatory responses to cyber events to insurance worldwide
 - Evaluated whether the response was sufficient

©2016 Greenberg Traurig, LLP. All rights reserved. | gtlaw.com 22



Overview

- Cyber Climate Change
- Responding Well Matters
- Are You Prepared Financially?
- Who Needs a Seat at the Table?
- What are Your Proof Points?
- Breach Scenarios to Consider

Cyber Climate Change

[25]

Litigation Floodgates Opening

- **Post-Clapper Standing**
 - Threatened Injury Certainly Impending and Fairly Traceable to Defendant

- **California and the 7th Circuit Data Breach Class Actions**
 - **Sony:**
 - Wrongful Disclosure Causing
 - Threat of Future Harm is Enough—
 - No 3d Party Access Required

 - **Neiman Marcus:**
 - Data Theft Necessarily Implies
 - Imminent Threat of Harm Because
 - Misuse of Data is the Purpose of a Breach

[26]

GT

Litigation Floodgates Opening

- **Data Breach Class Action Claims**
 - Negligence
 - Breach of Contract
 - Fraud
 - Unfair Trade Practices/Consumer Protection Violations
 - Directors and Officers' Liability for Breach of Fiduciary Duty

- **Prepare for Defense on the Merits**

[27]

GT

Regulatory Hot Tin Roof

- **Federal Agencies After OPM Breach**

- **State Regulator Coordination**

- **International Regulators' Scrutiny**
 - Post-Snowden Mistrust
 - Different Values and Approaches

- **Regulators are Cash Positive**

[28]

GT

Which Regulator is Most Aggressive?

- SEC
 - Sweeps
- FTC
 - Consent Decrees with Audits for 20 Years
- HHS
 - Hospice of Northern Idaho
- Cyber Regulators Worldwide are Cash Positive

[29]

GT

California Leads the Pack

- By Statute, California Requires:
 - Use of:

Reasonable Security Procedures and Practices to Protect California Residents' PII and PHI
- On February 16, 2016, California's Attorney General Specified 20 Critical Controls that Constitute Minimum Security and Stated That:
 - Failure to Implement ALL of the Applicable Controls Constitutes

"Lack of Reasonable Security"

[30]

California Department of Justice 2016 Data Breach Report
February, 16, 2016

The CIS Critical Security Controls for Effective Cyber Defense

CSC 1	Inventory of Authorized and Unauthorized Devices
CSC 2	Inventory of Authorized and Unauthorized Software
CSC 3	Secure configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
CSC 4	Continuous Vulnerability Assessment and Remediation
CSC 5	Controlled Use of Administrative Privileges
CSC 6	Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7	Email and Web Browser Protection
CSC 8	Malware Defenses
CSC 9	Limitation and Control of Network Ports, Protocols, and Services
CSC 10	Data Recovery Capability
CSC 11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12	Boundary Defense
CSC 13	Data Protection
CSC 14	Controlled Access Based on the Need to Know
CSC 15	Wireless Access Control
CSC 16	Account monitoring and Control
CSC 17	Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18	Application Software Security
CSC 19	Incident Response and Management
CSC 20	Penetration Tests and Red Team Exercises

[31]

Responding Well Matters

[32]

Responding Well Matters

- **Response will be Evaluated by Regulators and Questioned by Plaintiffs' Attorneys**

- **Conduct Sets the Tone for Public Perception**

- **Prepare to Act Appropriately to Protect:**
 - Customers
 - Shareholders
 - Brand
 - Bottom Line

[33]

What do Regulators Expect?

- **Proof that Your Operation Isn't Careless, Including:**
 - A Solid, Workable Breach Response Plan

 - Evidence that You:
 - Know What Sensitive Data You Handle,
 - Keep Only What it is Necessary, and
 - Take Reasonable Steps to Protect It

[34]

What do Regulators Expect?

- **Timely Notification**
- **Accurate Count of the Number of Impacted Individuals Resident in Each Jurisdiction**
- **Clear, Fair Communication**
- **Services for Impacted Individuals**

[35]

Are You
Prepared
Financially?

[36]

Are You Prepared Financially?

■ Do You Know Your Maximum Probable Loss and Likely Frequent Losses?

- Maximum Probable Loss
 - \$158- \$214 Per Impacted Individual
 - More Robust Valuation Using Breach Calculators
- Frequency Valuation
 - Evaluate Prior Situations
 - Consider Impact of Mobile Technology
 - Don't Forget Insider Risks and Vendors

[37]

Are You Prepared Financially?

■ Are Your Cyber Reserves/Insurance Adequate?

- Evaluated Annually
- Based on MPL and Frequency Assessment
- Supported by Independent Evaluation (e.g. Broker)

■ Are Your Vendors' Reserves/Insurance Adequate if They Cause Your Loss?

■ Are You Satisfied with Contractual Joint Breach Response Requirements and Planning?

[38]

Who Needs a Seat at the Table?

[39]

Who Needs a Seat at the Table?

■ Responding Well Requires an Enterprise-Level Plan

- IT
- Legal
- Compliance
- Finance
- Risk Management
- Human Resources
- Public Relations
- Each Operating Unit

[40]

GT

Who Needs a Seat at the Table?

- **Strong Enterprise-wide Incident Response Plan Includes:**
 - Agreed Upon Authority and Roles
 - Agreed Upon Stakeholder Communication Plans
 - Prudently Engaged Management and Board
 - Core Initial Investigation
 - Full Incident Response Team Reflects Enterprise

[41]

GT

Who Needs a Seat at the Table?

- **Incident Response Team Members = Witnesses**
- **Identify Individuals and Alternates**
- **Choose Carefully and Confirm Readiness**
- **Train the Team**
 - Know Who does What, When and Why
 - Agreed Upon Process and Authority
 - Appropriate Documentation
 - Method(s) for Keeping Stakeholders Informed

[42]

What are Your Proof Points?

[43]

What are Your Proof Points?

- What Evidence Proves Your Reasonableness to Customers, Regulators, Plaintiffs' Attorneys, Shareholders and the Public?
 - Is Your Cybersecurity Governance Defensible?
 - Are You PCI Compliant?
 - Has Your Incident Response Plan been Tested This Year—and Not Just the IT Portion?
 - Do You Benchmark Favorably?

[44]

What are Your Proof Points?

- Defensible Positions
 - Maximize Legal Protection of Response
 - Document Prudently
 - Strong Proof Points are Identified in Advance:
 - Active Management and Board Engagement
 - Reasonable Steps Taken to Minimize and Protect Reportable Information Cradle to Grave
 - Appropriate Training and Testing
 - Independent Expert Validation of Good Practices
 - Key Documents and Witnesses are Ready

[45]

Breach Scenarios to Consider

[46]

GT

Breach Scenarios to Consider

- PCI Breach
- Employee Data Breach
- Vendor's Breach of Your Customer Data
- Ransomware
- Insider Compromise

[47]

GT

Questions?

[48]

GT

Thank You!

Presented by:
Lori S. Nugent
Greenberg Traurig, LLP
nugentl@gtlaw.com
214-665-3630

[49]

GT GreenbergTraurig

Contact Information

<p>Fred Karlinsky Shareholder & Co-Chair Insurance Regulatory & Transactions</p> <p>karlinskyf@gtlaw.com</p> <p>Greenberg Traurig, P.A. 401 East Las Olas Boulevard, Suite 2000 Fort Lauderdale, FL 33301 Tel: 954-768-8278 www.gtlaw.com</p>	<p>Lori Nugent Shareholder Cybersecurity, Privacy and Crisis Management</p> <p>nugentl@gtlaw.com</p> <p>Greenberg Traurig, LLP 2200 Ross Avenue Suite 5200 Dallas, TX 72501 Tel: 214-665-3630 www.gtlaw.com</p>
---	--

©2016 Greenberg Traurig, LLP. All rights reserved. | gtlaw.com 50