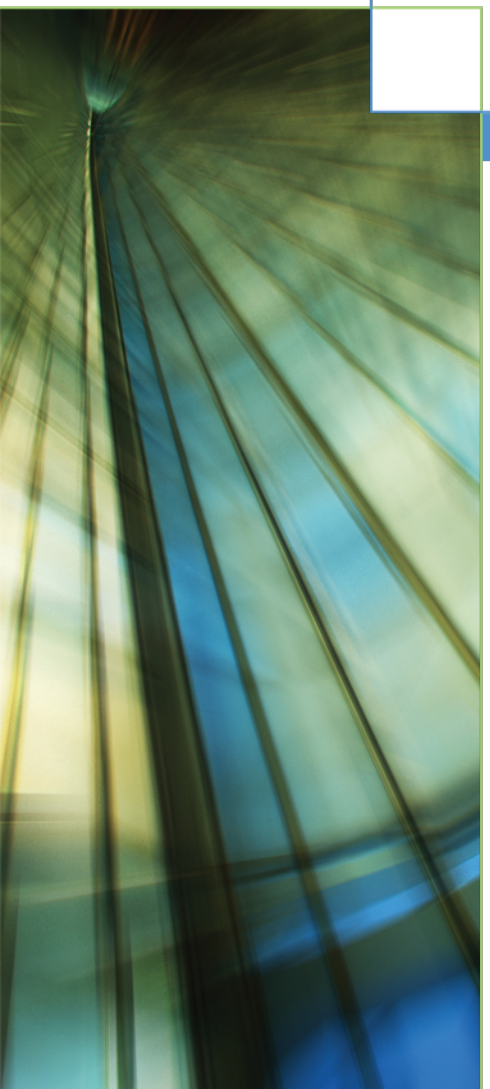


CYBERSECURITY
Recent Regulatory Developments and Compliance Pitfalls

Casualty Actuarial Society
Ratemaking and Product Management Seminar & Workshop
Orlando, Florida
March 14-16, 2016

Fred E. Karlinsky, Esq.
Shareholder & Co-Chair, Insurance Regulatory & Transactions Practice, Greenberg Traurig

GT GreenbergTraurig

Disclaimer

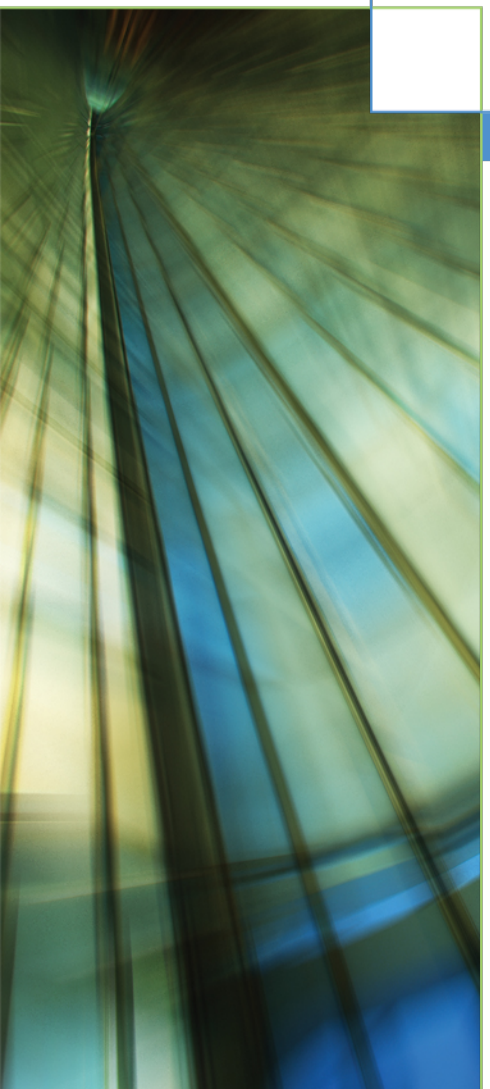
The materials in this presentation are intended to provide a general overview of the issues contained herein and are not intended nor should they be construed to provide specific legal or regulatory guidance or advice. If you have any questions or issues of a specific nature, you should consult with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

GT GreenbergTraurig

Overview

- Current Cybersecurity Landscape
- Key Cybersecurity Laws and Regulations
- Cyber Issues for the Insurance Industry
- Best Practices for Insurers

GT GreenbergTraurig



Current Cybersecurity Landscape

GT GreenbergTraurig

In the News

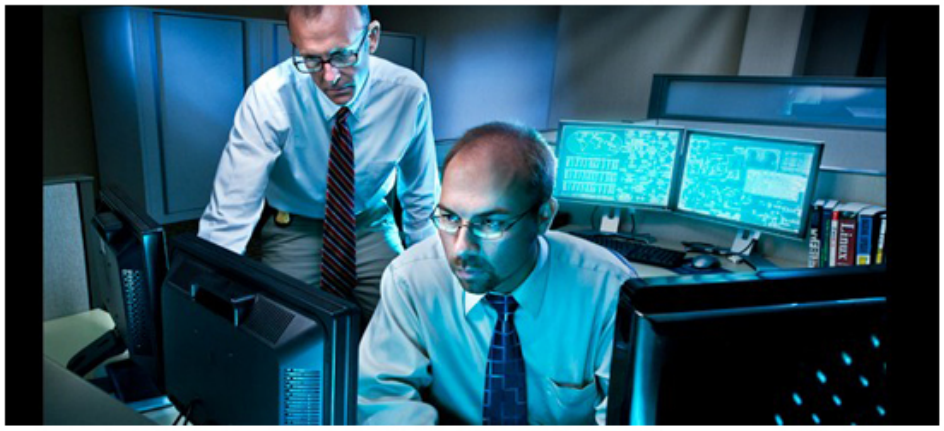
- November 24, 2014: Sony Corporation hacked
  - Release of confidential data: personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of (previously) unreleased Sony films, and other information
- December, 2013 breach of Target Corporation
  - Target settled a lawsuit with banks and credit unions in December, 2015 for $39 million

More Attacks

- Retailer
- Online Retailer
- National Home Improvement Retailer
- Financial Bank

The Recent Past

- Cyber crime in the past mostly involved unsophisticated attacks to deface websites of corporations and governments
- Motivated by the desire for notoriety and bragging rights
- Nation states and organized crime were minimally involved



The Current Picture

- Nation states are increasingly aggressive in attacking corporate and government systems
  - Nation states are highly sophisticated
- Emerging terrorist cyber threat

The New York Times — Business Day — Technology

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

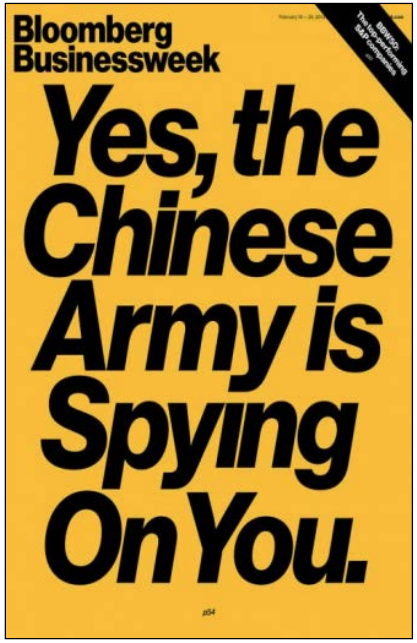
Chinese Army Unit Is Seen as Tied to Hacking Against U.S.

This 12-story building on the outskirts of Shanghai is the headquarters of Unit 61398 of the People's Liberation Army. China's defense ministry has denied that it is responsible for initiating digital attacks.

By DAVID E. SANGER, DAVID BARBOZA and NICOLE PERLROTH
Published: February 18, 2013 | 576 Comments

On the outskirts of Shanghai, in a run-down neighborhood dominated by a 12-story white office tower, sits a People's Liberation Army base for China's growing corps of cyberwarriors.

FACEBOOK
TWITTER



The Current Picture

- The U.S. National Security Agency (NSA) is responsible for conducting cyber intelligence
  - NSA conducts mass surveillance of electronic communications both within and without the United States

GT GreenbergTraurig

The Current Picture

- The consensus among governments and the business community is that cyber attacks against organizations will continue to increase for the foreseeable future
- The global cost of cyber crime is estimated to be in the hundreds of millions to billions of dollars
- The costs are either direct or indirect due to costs incurred preparing for breaches, containing breaches, and remediating damage caused by a breach

GT GreenbergTraurig

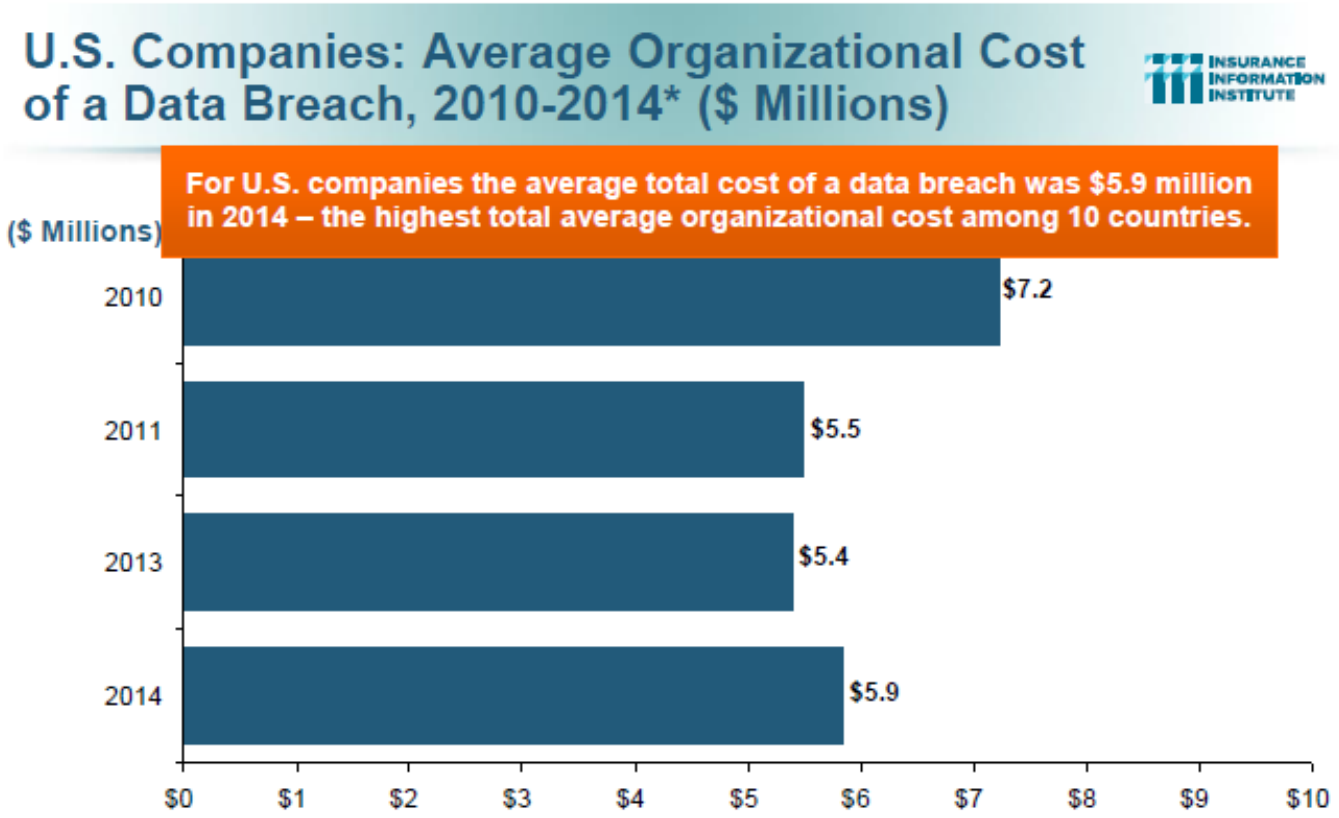
How Organizations are Compromised

- Threats from Outsiders
  - State sponsored entities
  - Terror groups
  - Hacktivists
  - Organized crime
  - Corporate rivals
  - Disgruntled former employees
- Threats from Insiders
  - Employees
  - Trusted third parties with access to data and systems

How Organizations are Compromised

- Spear Phishing
  - Directed attack to induce an individual into opening an attachment
- Structured Query Language (SQL) attacks
  - Weak digital security protocols can be exploited by SQL injection attacks
- Organizational insiders
  - Rogue employees
- Loss/theft of sensitive information, including loss/theft of mobile electronic devices

Typical Cost of Cyber Breach



Cyber Insurance Demand

- Demand for cyber 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*

GT GreenbergTraurig

Cyber Risk Coverage

- Loss/Corruption of Data
- Business Interruption
- Liability
- D&O/Management Liability
- Cyber Extortion
- Crisis Management
- Criminal Rewards
- Data Breach
- Identity Theft

Underwriting Difficulties

- Developing field
  - Each year, cyber criminals become more sophisticated – and more dangerous
- Costs uncertain
  - Reputational harm is difficult to quantify
  - Vulnerabilities often go unidentified until it is too late
- Lack of information
  - Much information is classified due to national security concerns

GT GreenbergTraurig

Defining Insurable and Uninsurable Cyber Risks

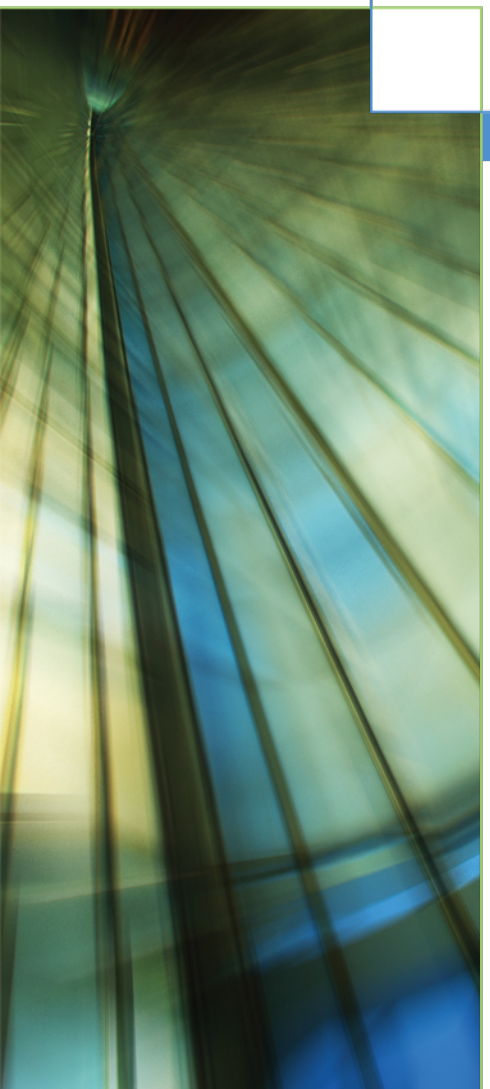
- Insurable Risks
  - Liability out of a data breach
  - Notifications
  - Network damage
  - Regulatory Issues
- Uninsurable Risks
  - Catastrophes
  - Operational mistakes
  - Reputational damage
  - Industrial espionage
  - Data as an asset

GT GreenbergTraurig

Cyber Security & the Human Element

- Cyber incidents are caused by people
  - Accidentally or intentionally
- People implement cyber security
  - Boards
  - Employees
- Bad actors/hackers
- Constant Evolution

GT GreenbergTraurig



Key Cybersecurity Laws & Regulations

GT GreenbergTraurig

Recent Federal & State Legislation

- 2014: Five federal cyber security bills became law
- 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
- 47 states have enacted cybersecurity legislation
  - 32 states in 2015 introduced or are considering security breach notification bills or resolutions

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

GT GreenbergTraurig

HIPAA Security Rule

- Minimum security standards for protecting ePHI
- Safeguards & Requirements
  - Administrative safeguards
  - Physical safeguards
  - Organizational safeguards
  - Policies and procedures
- Stong cybersecurity practices will help safeguard this information

GT GreenbergTraurig

Federal Trade Commission

- FTC Act
  - Prohibits "deceptive" and "unfair" acts or practices
  - Generally prohibits false advertisements
- Failure to use proper data security protocols can violate the FTC Act
- Unfortunately, FTC does not have published regulations detailing the data security protocols
- Companies must examine over three-dozen FTC settlements and other guidance to attempt to determine what the FTC expects

GT GreenbergTraurig

SEC Issues Cybersecurity Guidance

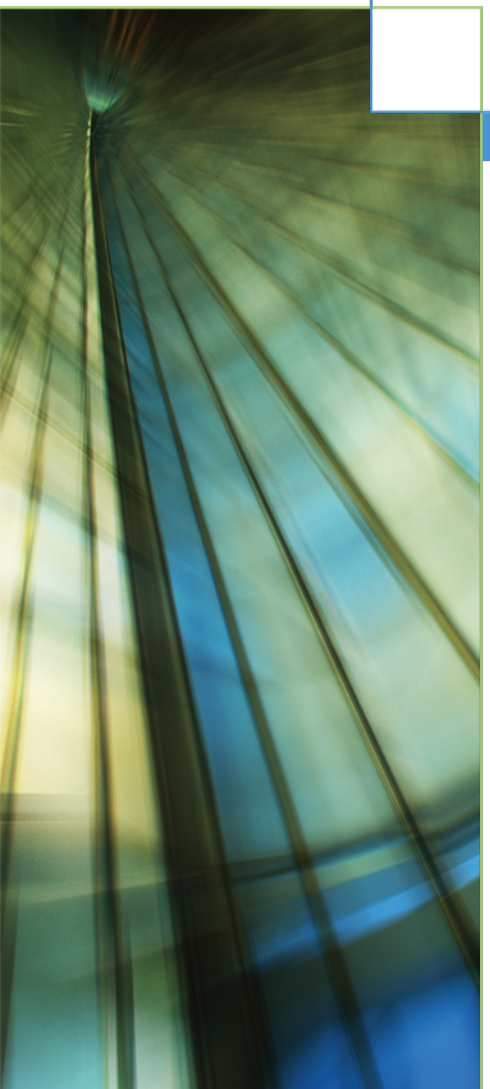
- Guidance Update for investment advisors and registered investment companies
  - Investment companies, broker-dealers and investment advisers must:
    - Review their cybersecurity preparedness
    - Update their policies and procedures
    - Examine their potential vulnerabilities and assess compliance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

GT GreenbergTraurig

SEC Issues Cybersecurity Guidance

- Examination of 57 broker-dealers and 49 registered investment advisors
- Vast majority of broker-dealers and firms:
  - Implemented written information security plans
  - Regularly reviewed such plans
  - Inventoried and catalogued their information security resources
  - Made use of encryption and had suffered a cybersecurity incident
- However, only approximately half participated in information sharing programs
- SEC noted varying results on designation of a chief information security officer and oversight and policies governing the use of vendors

GT GreenbergTraurig



Cyber Issues for the Insurance Industry

GT GreenbergTraurig

Large Insurer Breaches

- February 2015: Anthem, Inc. breach
  - Cybersecurity attack
  - Compromised information included insureds' names, birthdays, social security numbers, addresses, emails, and employment information

Insurance & Cybersecurity

- Insurance companies store large amounts of sensitive information/data on their employees and insureds
  - Length of storage of information is greater for life insurers
- Breaches that occur can/will expose huge data sets and lead to significant exposure
- Regulators are requiring more diligence of insurers to protect client data from cyber threats

INSURANCE JOURNAL

View this article online: http://www.insurancejournal.com/magazines/features/2013/06/17/295232.htm

Regulators Examining Insurers' Cyber Security Readiness

New York's top financial regulator has asked some of the largest U.S. insurance companies to disclose details on their preparedness for cyber attacks, following a similar request to major banks earlier this year.

The New York State Department of Financial Services said it sent letters on May 28 asking insurers whether they have faced any cyber attacks in the last three years, what safeguards they have put in place and how much money they have set aside for dealing with cyber issues.

"Insurance companies, in some cases sometimes more than banks, hold incredibly sensitive information of regular people," said Ben Lawsky, New York's superintendent of financial services, in an interview. "We're trying to get ahead of a problem and focus here on an area that I think has been underappreciated and maybe not focused on enough by regulators."

Medical Data is Highly Lucrative

- Pat Calhoun: Senior Vice President of Network Security at Intel Security
  - Medical information has a higher value on the black market than credit card information
  - Medical information does not allow for steps to take back the information or cancel the information like credit cards

GT GreenbergTraurig

Study of Insurance Company & Cyber Risk

- 74% of insurance executives expect cyber IT risks to increase.
  - 2015 Accenture Global Risk Management Study
- 59% of insurance executives experience significant cyber attacks daily or weekly
  - Business Resilience in the Face of Cyber Risk
- Executives expect to hire more people who are experts in managing cyber risks

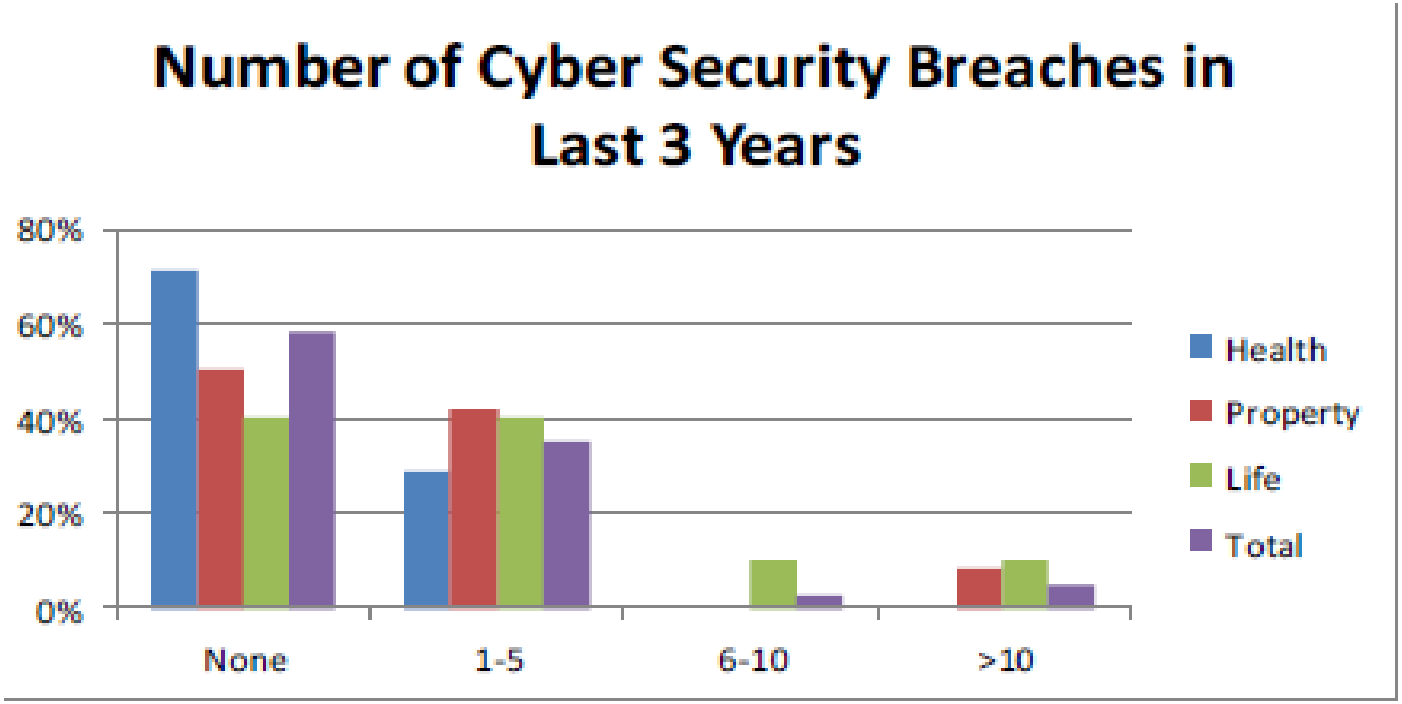
GT GreenbergTraurig

N.Y. DFS Report on Cyber Security in the Insurance Sector

- February 9, 2015
- Survey of 43 insurers about cybersecurity programs, costs, and future plans
- DFS measures in the future to strengthen cyber security:
  - targeted assessments of “cybersecurity preparedness”
  - proposing enhanced regulations requiring insurers to meet heightened standards for cybersecurity
  - exploring measures related to the representations and warranties insurers receive from third-party vendors that handle customer data

GT GreenbergTraurig

N.Y. DFS Survey on Cyber Insurance in the Insurance Sector



GT GreenbergTraurig

Enterprise Risk Management

- N.Y. DFS also reviewed ERM reports to understand how cybersecurity fits into the insurers' overall risk management strategy
- Found a wide array of factors that affect an insurer's cybersecurity program
  - Report assets
  - Transactional frequency
  - Variety of business lines
  - Sales and marketing technologies

GT GreenbergTraurig

N.Y. Letter on IT Examination Framework

- March 26, 2014: Letter to all insurers noting key revisions to the existing IT examination framework
- IT/cybersecurity examinations will now include:
  - Corporate governance
  - Management of cyber issues
  - Resources
  - Risks posed by infrastructure
  - Protections against intrusions
  - Testing and monitoring
  - Management of 3rd party service providers
  - Cybersecurity insurance coverage

N.Y. Letter on IT Examination Framework

- Department would conduct comprehensive risk assessment and require a report on an insurer's cybersecurity practices and procedures
- Report must include responses to 16 wide ranging questions
  - The deadline for submission of the responses was April 27, 2015
- Once the report is submitted and the risk assessment is conducted, the Department would schedule IT/cybersecurity examination

GT GreenbergTraurig

NAIC Cybersecurity Task Force

- NAIC's Principles for Effective Cybersecurity Insurance Regulatory Guidance adopted April 16, 2015
- Principle 1
  - PII is protected from cybersecurity risks
- Principle 2
  - Confidential consumer information is property safeguarded
- Principle 3
  - Regulators must protect information
- Principle 4
  - Cybersecurity regulations must be flexible

NAIC Cybersecurity Task Force

- Principle 5
  - Cybersecurity Regulations must be risk based and consider insurer resources
- Principle 6
  - Regulators should provide appropriate regulatory oversight
- Principle 7
  - Planning for incident responses
- Principle 8
  - Third parties and service provider must have controls in place to protect PII

GT GreenbergTraurig

NAIC Cybersecurity Task Force

- Principle 9
  - Cybersecurity risks should be incorporated into an insurer's ERM
- Principle 10
  - IT internal audits should be reviewed by BODs and appropriate committees
- Principle 11
  - Information sharing and analysis organization
- Principle 12
  - Training and assessments for employees

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

GT GreenbergTraurig

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

GT GreenbergTraurig

NAIC Cybersecurity Roadmap

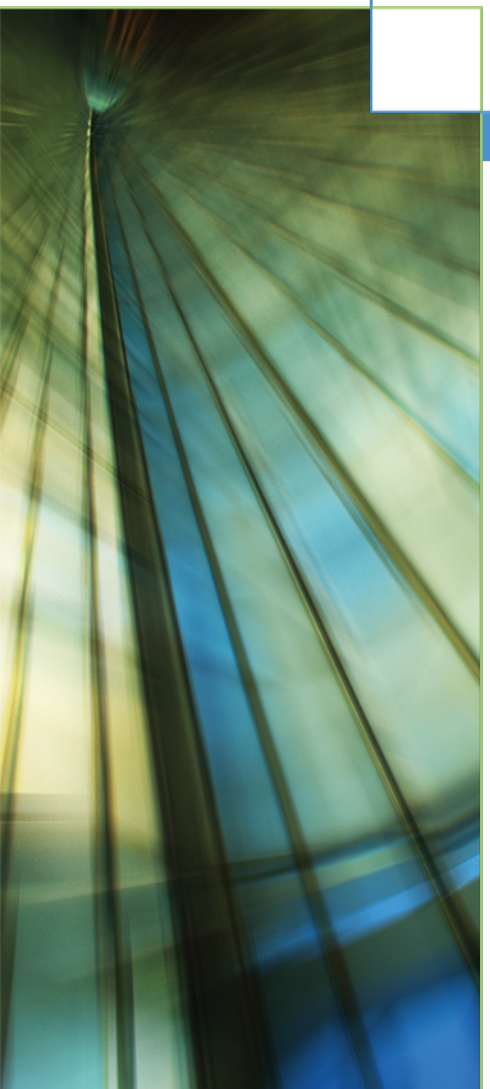
- Initially the Bill of Rights featured 12 points, but the Roadmap was later reduced to 6 points
  - The document was updated based on the 45 pages of comments received from Interested Parties
  - Revised or simplified the remaining points and definitions found in the document

GT GreenbergTraurig

Roadmap Summary

- 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

GT GreenbergTraurig



Best Practices for Insurers

GT GreenbergTraurig

Best Practices

- Prioritize cybersecurity
- Incident response teams
  - Outside counsel?
- Security policies and procedures
  - Document cybersecurity roles and responsibilities
  - Alignment with company goals and practices
  - Compliance with regulatory requirements
  - Testing procedures

GT GreenbergTraurig

Best Practices

- Where is critical information stored? How is it processed?
  - Computers
  - Personal devises
  - Home computers
  - Vendors' systems
  - The "Cloud"
  - Backup media
  - Portable media
  - Nontraditional platforms

GT GreenbergTraurig

Best Practices

- Assess your security posture
- Develop a detailed incident response plan
  - Simulations
  - Continually improve plan
- Review plan with management and BOD
- Apply risk management principles
- Information sharing process

Best Practices

- Document who has access to information assets
  - Review for appropriate access
  - Review document controls
- Vendors must have sufficient cybersecurity insurance coverage
- Cyber insurance coverage is adequate for company
- Regularly train employees and vendors
  - Procedures and responsibilities
  - Data protection measures

GT GreenbergTraurig

Questions

GT GreenbergTraurig

Contact Information

Fred E. Karlinsky, Esq.

Shareholder

Co-Chair, Insurance Regulatory & Transactions Practice

karlinskyf@gtlaw.com

Greenberg Traurig, P.A.

401 East Las Olas Boulevard, Suite 2000

Fort Lauderdale, FL 33301

Tel: 954-768-8278

www.gtlaw.com