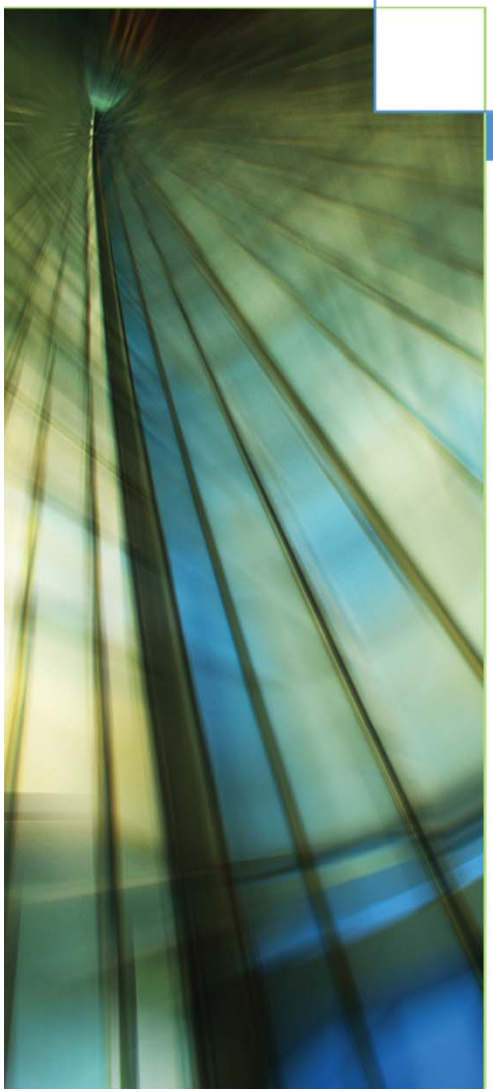


CYBER AND DATA SECURITY
Coverage and Compliance Considerations

Casualty Actuarial Society
2017 Annual Meeting
November 7, 2017
Anaheim, California

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

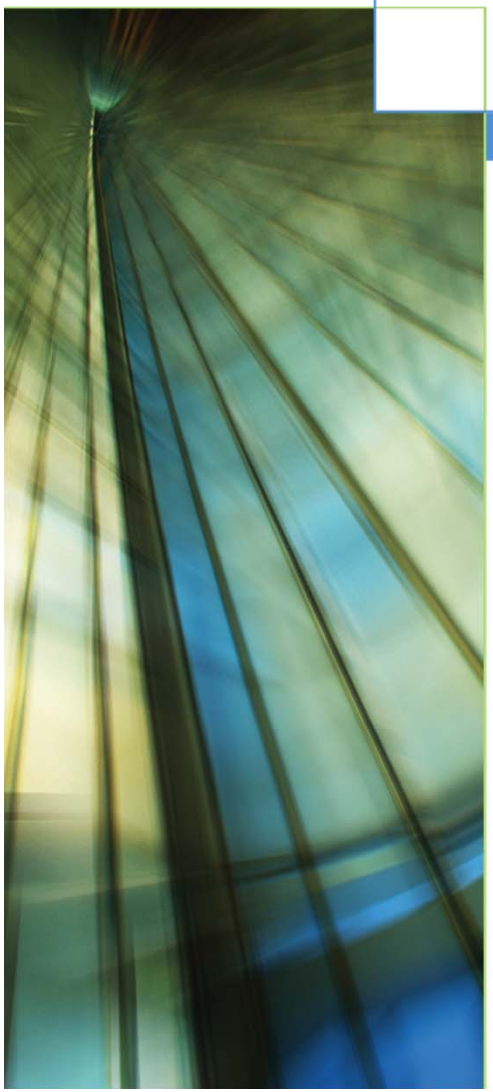
Speakers

- Fred Karlinsky
  - Shareholder & Co-Chair, Insurance Regulatory and Transactions Practice, Greenberg Traurig, P.A.
- Karl Pedersen
  - Managing Director, Cyber Product Leader, Marsh USA Inc.
- Lori Nugent
  - Shareholder, Greenberg Traurig, P.A.
- Wesley Griffiths
  - *Moderator*

GT GreenbergTraurig

Overview

- State and Federal Regulatory Developments
- Cyber Liability Market Trends
- Data Breach Preparedness and Response



State Regulatory Developments

GT GreenbergTraurig

Poll Question

- *How confident are you that your organization's cybersecurity policies and procedures will stand up to regulatory scrutiny?*
  1. Very confident
  2. Somewhat confident
  3. Not confident
  4. Not sure

GT GreenbergTraurig

New York Cybersecurity Requirements for Financial Services Companies

- "Cybersecurity Requirements for Financial Services Companies" promulgated on February 16, 2017
  - Applies to Insurance Companies, Banks and other Financial Services
  - New standards for financial services companies to protect consumers from cyber threats
- Took effect March 1, 2017

GT GreenbergTraurig

New York Regulation Summary

- 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

GT GreenbergTraurig

Annual Risk Assessment

- Insurers must conduct and document annual risk assessments to help develop a cybersecurity policy
- The Risk Assessment must be based on written policies and procedures, which must include:
  - Evaluation of identified risks
  - Assessment of systems and controls
  - How risks will be evaluated and either accepted or mitigated

GT GreenbergTraurig

Cybersecurity Policy

- Entities must maintain a written cybersecurity policy
  - Based on the Risk Assessment
  - Must be approved by the board of directors
- Must consider software protections, physical safeguards, and the entity's cybersecurity protocols for breach response and recovery

GT GreenbergTraurig

Additional Requirements

- Third Party Service Provider oversight
- Incident Response Plan
  - Notice to the Department
- Chief Information Security Officer ("CISO")
- Penetration Testing and Vulnerability Assessments
- Access Privileges
- Training for personnel

GT GreenbergTraurig

New York Requirements – Key Takeaways

- Entities may develop the plans that fit their own risk profiles
- Boards of Directors must be involved in cybersecurity planning
- Other regulators are monitoring the impact of New York's regulation

GT GreenbergTraurig

Insurance Data Security Model Law

- NAIC Cybersecurity Working Group development of the Insurance Data Security Model Law ("Model Law")
  - First draft released March, 2016
  - Second draft released August, 2016
  - Third draft released February, 2017
  - Fourth draft released April, 2017
  - Fifth draft released July, 2017
  - Sixth draft released August, 2017
- 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

GT GreenbergTraurig

Insurance Data Security Model Law

- Licensees must maintain a "comprehensive written Information Security Program"
  - Must be "commensurate with the size and complexity of the Licensee, the nature and scope of the Licensee's activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody or control"
  - Includes the administrative, technical, and physical safeguards used to protect Nonpublic Personal Information and the Licensee's Information System
- Licensees must regularly conduct Risk Assessments to ensure the adequacy of their Information Security Program

GT GreenbergTraurig

Insurance Data Security Model Law

- Oversight of Third-Party Service Providers
  - A Licensee shall exercise due diligence in selecting its Third-Party Service Provider; and
  - A Licensee shall require a Third-Party Service Provider to implement appropriate administrative, technical, and physical measures to protect and secure the Information Systems and Nonpublic Information that are accessible to, or held by, the Third-Party Service Provider

GT GreenbergTraurig

Insurance Data Security Model Law

- Incident Response Plan: “each Licensee shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event that compromises the confidentiality, integrity or availability of Nonpublic Information”
- Insurers must annually certify to their domiciliary commissioner that they are in compliance with the law

GT GreenbergTraurig

Insurance Data Security Model Law

- "Each Licensee shall notify the Commissioner as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred"
  - Must notify the domiciliary state regulator
  - Foreign state regulators must be notified if there are 250 or more affected residents and there is a "reasonable likelihood" of material harm to consumers or the Licensee's business operations
- As much information as possible must be provided
- Licensees must supplement initial notice as more information becomes available
- Consumers must be notified in accordance with the states' data breach notification laws

GT GreenbergTraurig

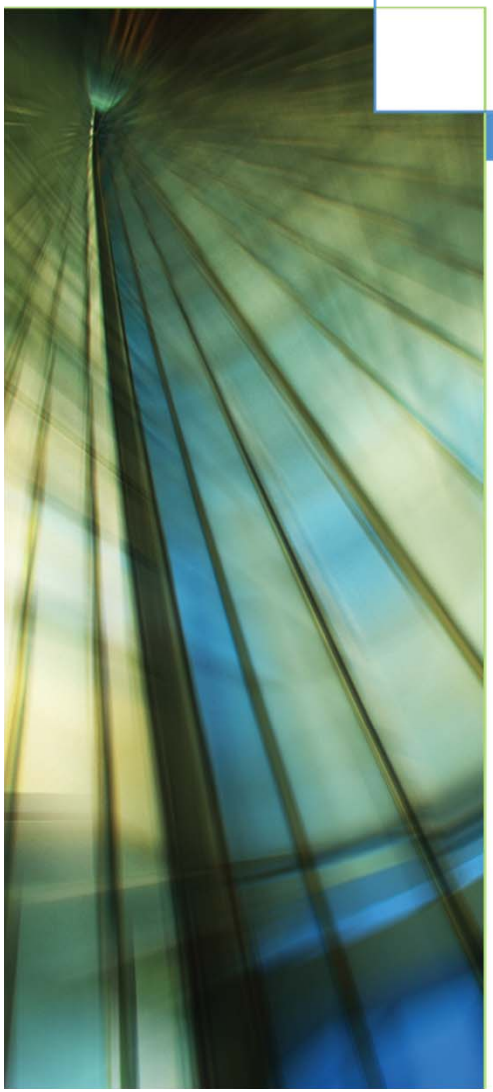
Insurance Data Security Model Law

- 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

GT GreenbergTraurig

Other NAIC Activity

- IT Examination Working Group:
  - Recently released proposed revisions to the Financial Examiners Handbook to include cyber-related guidance
    - Guidance similar to National Institute of Standards and Technology ("NIST") standards
  - Comments to changes due September 10, 2017
  - Continues to monitor development of the Insurance Data Security Model Act



Federal Legislation & Initiatives

GT GreenbergTraurig

Federal Activity

- 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
- Uniform cybersecurity reviews

MARSH

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

Understanding Cyber Risk and Insurance Solutions

Insights and Market Update

MARSH & McLENNAN COMPANIES

There are Many Types of Cyber-Vulnerable Assets

What are Cyber Risks?

If an entity:

- **uses technology in its operations, or**
- **handles/collects/stores confidential information**
  - Legal liability to others for computer security breaches
  - Legal liability to others for privacy breaches of confidential information
  - Regulatory actions, fines and scrutiny
  - Cyber extortion
  - Cyber terrorism
  - Loss or damage to data / information
  - Loss of revenue due to a computer attack
  - Extra expense to recover / respond to a computer attack
  - Loss or damage to reputation

Type of Information at Risk

Consumer Information

- Credit cards, debit cards, and other payment information
- Social Security Numbers, ITIN's, and other taxpayer records
- Customer transaction information, like order history, account numbers, etc.
- Protected Healthcare Information (PHI), including medical records, test results, appointment history
- Personally Identifiable Information (PII), like drivers license and passport details
- Financial information, like account balances, loan history, and credit reports
- Non-PII, like email addresses and passwords, phone lists, and home address that may not be independently sensitive, but may be more sensitive with one or more of the above

Employee Information

- Employers have at least some of the above information on all of their employees, spouses, dependents, former employees, retirees and job applicants

Business Partners

- Vendors and business partners may provide some of the above information, particularly for subcontractors and independent contractors
- All of the above types of information may also be received from commercial clients as a part of commercial transactions or services
- In addition, B2B exposures like design plans, manufacturing plans, projections, forecasts, M&A activity, and trade secrets

Data Privacy and Network Security
A Multi-Threat Environment

Technology
- Viruses, SQL Injections, DDoS attacks, etc.
  - Structural vulnerability
- Social Media/Networking
  - Phishing

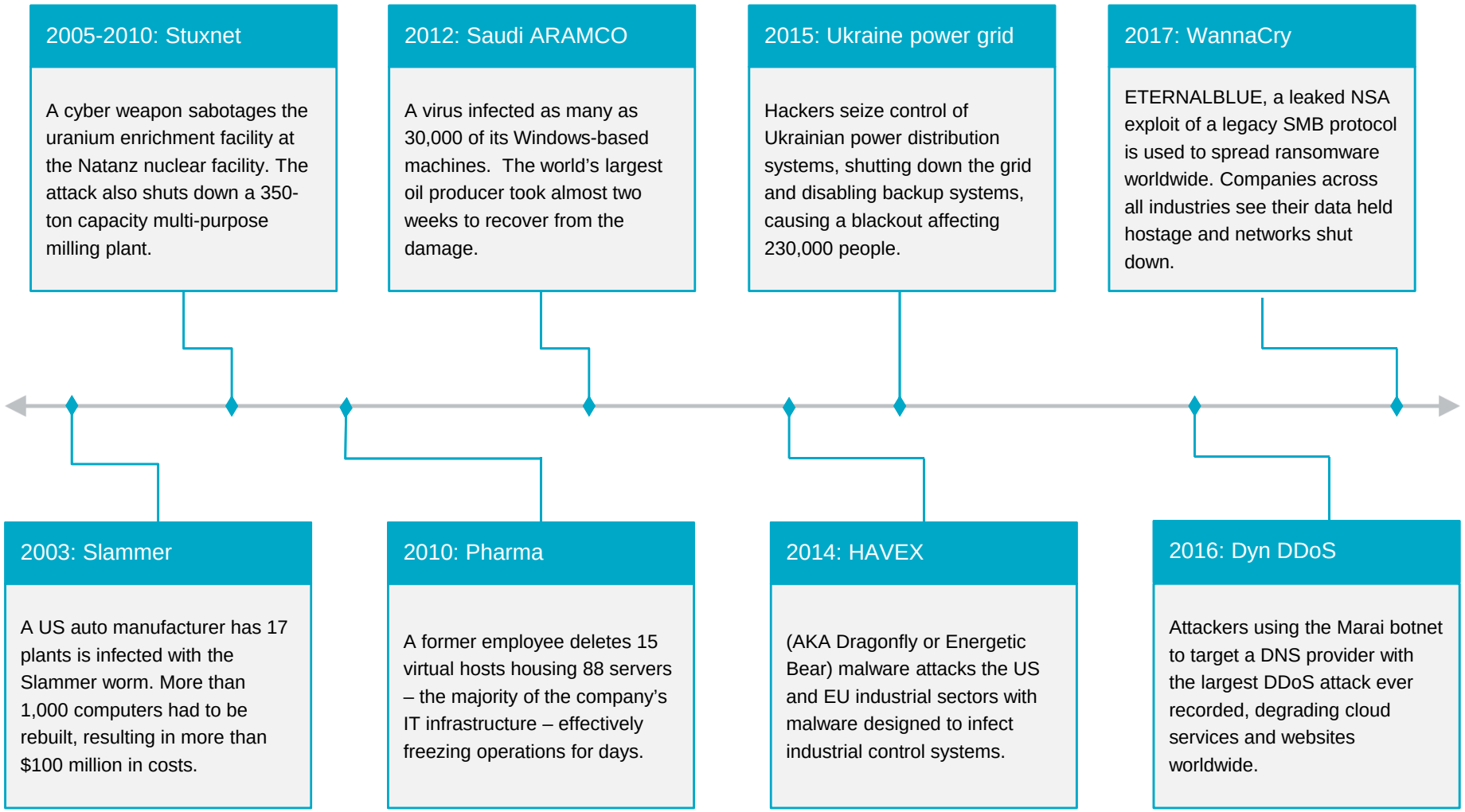
External
- Customers
- Authors, producers, publishers, competitors
- Business associates
- Vendors / Suppliers
- Foreign and domestic organized crime
- Hackers / Hacktivists

Internal
- Rogue employees
  - Careless staff
    - BYOD

Old School
- Laptop theft
- Dumpster diving
  - Photocopier

Regulatory
- SEC, FTC, state attorneys general
- 48 State Breach notification laws
- NIST Cybersecurity Framework
- HHS, HIPAA & HIPAA HITECH
- Identity Theft Red Flags Rule
- Foreign Laws
- General Data Protection Regulation

Notable First Party Loss Events



Petya – Global Impact for Companies in All Industries
Counting the Costs

PETYA BACKGROUND

- Petya is a (purported) ransomware attack first reported in the Ukraine in June 2017
- The attack exploits a vulnerability in Microsoft Windows similar to an earlier ransomware attack known as WannaCry
- The malware spread through a software update to an accounting program, as well as other means
- Petya encrypts computer files and demands a $300 ransom in Bitcoin, though the ransom feature was not fully functional
- Petya spread across the world causing serious disruptions to government systems and multiple global businesses, including critical infrastructure
- Attribution is unclear but some researches speculate that this was a destructive attack disguised as ransomware against the Ukraine

Petya – Global Impact for Companies in All Industries

	Industry	News Article
Reckitt Benckiser	Manufacturing (Consumer Goods)	July 24, 2017 H1 Earnings Report July 6, 2017, Press Release
Saint Gobain	Manufacturing (Industrials)	2017 H1 Earnings Statement July 13, 2017 Press Release
Mondelez International, Inc (NASDAQ: MDLZ)	Food and Beverage Manufacturer	Aug. 2, 2017 Q2 Earnings Statement Release July 6, 2017 Press Release July 10, 2017 Yahoo News
WPP	Advertising/Media	June 29, 2017 Press Release
FedEx (TNT Express)	Logistics/Shipping	July 17, 2017 10-K Press Release July 6, 2017 Press Release
AP Moller-Maersk	Transportation/Logistics/Energy	2017 Q2 Quarterly Report June 28, 2017, Maersk Tweet June 29, 2017 Maersk Tweet
Merck (NYSE: MRK)	Pharmaceutical	June 28, 2017, Merck Tweet
Nuance Communications (NASDAQ: NUAN)	Communications	Aug. 8, 2017, Third Quarter Press Release July 21, 2017 Press Release July 5, 2017 Blog Post
DLA PIPER	Professional Services: Legal	June 28, 2017 Press Release
Deutsche Post DHL	Logistics/Shipping	Reuters Aug. 8, 2017 Article

Industry Trends

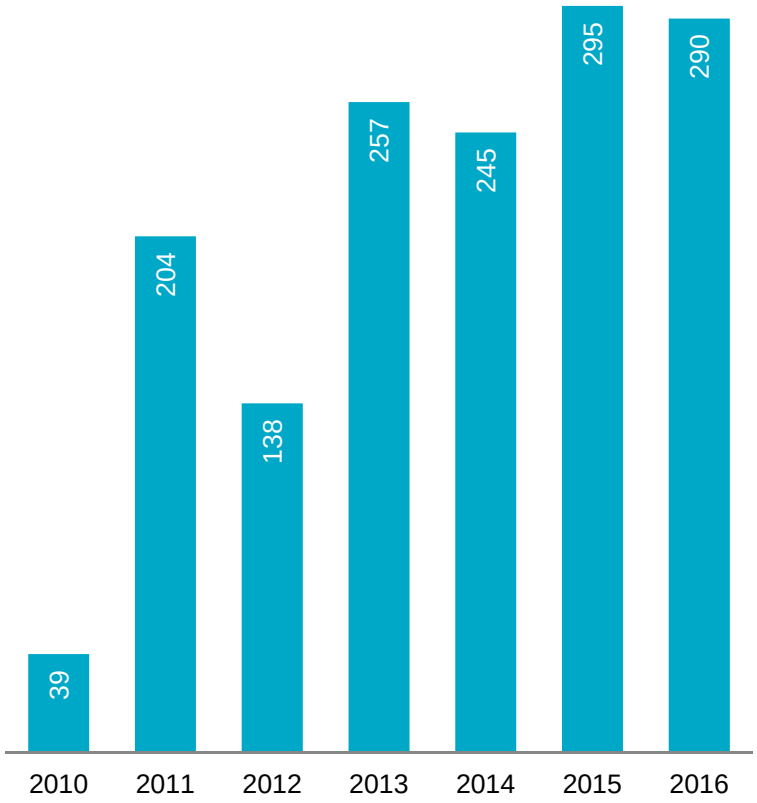
THE INTERNET OF THINGS (IoT)

- IoT describes the trend of traditionally non-networked devices being networked, making them susceptible to attack. IoT devices run the gamut from toasters and webcams to industrial control systems and power distribution components.
- Attacks on IoT devices can cause wide-ranging business interruption, and are not geographically constrained like a fire or earthquake.

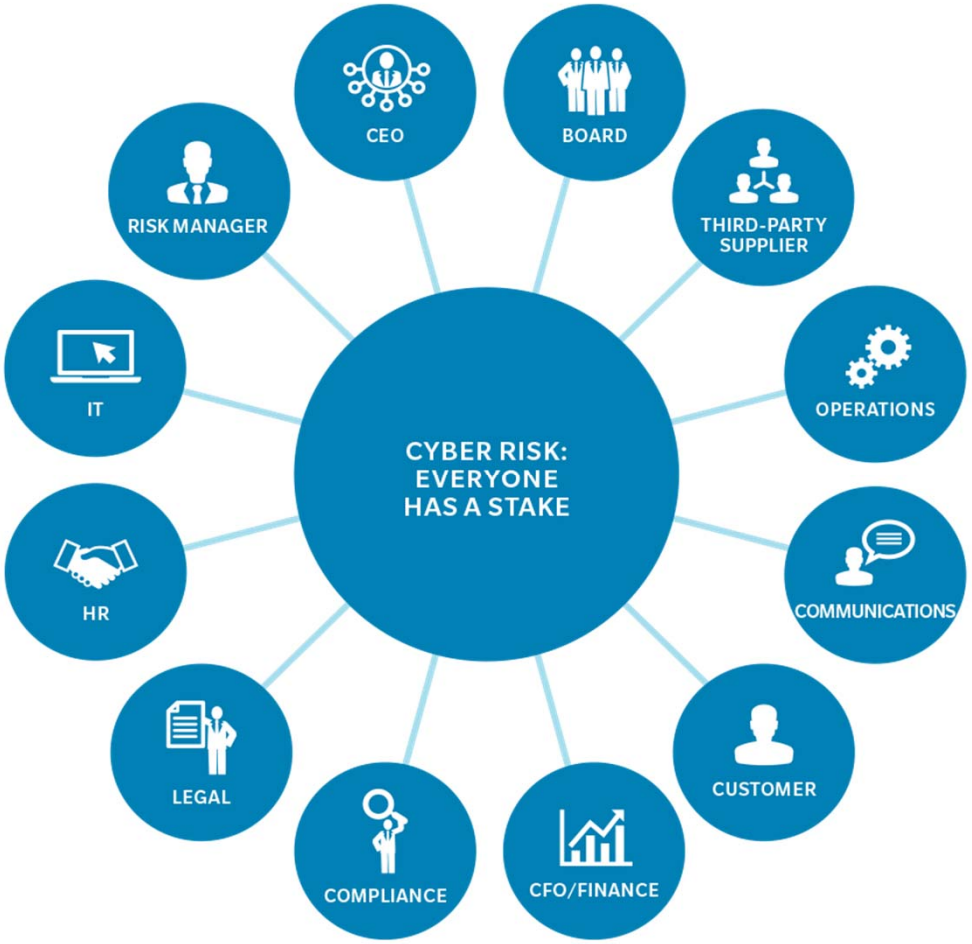
INCREASING MANUFACTURING RISK

- IBM's 2015 Xforce research report found that manufacturing became the second most-attacked sector, with attacks on automotive manufacturers being the single largest segment at 30%.
- Since forming in 2010, ICS-CERT – a division of the US Department of Homeland Security tasked with improving cyber security for the nation's critical infrastructure – has seen a steady increase in attacks against industrial systems.

ICS-CERT INCIDENT RESPONSES BY YEAR
Source: ICS-CERT annual reports



When It Come to Cyber Risk Management, Everyone Has a Stake



The Next Evolution of Cyber Risk

Moving from Cyber Security to Cyber Risk Management

Cyber Security

- Cyber Security is a problem to be solved
- Cyber Security issues can be prevented
- Cyber Security is a technology problem
- Cyber Security is a problem for the IT department
- Cyber Security is a temporary issue
- Cyber Security is all about (data breaches | cyber terrorism | <insert other scenario here>)

Cyber Risk Management

- Cyber Risk is a race without end
- Cyber Risk cannot be eliminated
- Cyber Risk Management encompasses people, processes, and technology.
- Cyber Risk Management engages the entire enterprise
- Cyber Risk Management is a permanent entry on the risk register
- Cyber Risk is a multitude of issues reflecting the pervasive nature of technology

First Party Coverages

COVERAGE	DESCRIPTION	COVERED COSTS
Network Business Interruption	Interruption or suspension of computer systems due to a network security breach. Coverage may be limited to security attacks or broadened to include general system failure.	▪ Loss of Income. ▪ Costs in excess of normal operating expenses required to restore systems. ▪ Forensic expenses to value a loss. ▪ May include dependent business interruption as well.
Data Restoration	Costs to restore, recreate, or recollect your data and other intangible assets that are corrupted or destroyed by a cyber attack.	▪ Restoration of corrupted data. ▪ Vendor costs to recreate lost data.
Event Management/Breach Response	Costs resulting from a network security or privacy breach.	▪ Forensics. ▪ Notification. ▪ Credit Monitoring. ▪ Call Center. ▪ Public Relations. ▪ Sales Discounts.
Cyber Extortion	Threat to compromise network or data if ransom not paid.	▪ Forensics and related investigation costs. ▪ Costs to negotiate and pay any ransoms demanded.

Third Party Coverages

COVERAGE	DESCRIPTION	COVERED COSTS
Privacy Liability	Failure to prevent unauthorized access, disclosure or collection, or failure of others to whom you have entrusted such information, for not properly notifying of a privacy breach.	▪ Liability and defense costs. ▪ Commercial litigation – e.g., bank suits. ▪ Consumer litigation – e.g., class-actions. ▪ Third-party costs for notification and investigation. ▪ PCI fines and penalties.
Network Security Liability	Failure of system security to prevent or mitigate a computer attack. Failure of system security includes failure of written policies and procedures addressing technology use.	▪ Liability and defense costs. ▪ See above.
Privacy Regulatory Defense Costs	Privacy breach and related fines or penalties assessed by Regulators.	▪ Liability and defense costs. ▪ Regulatory investigations. ▪ PHI fines and penalties. ▪ Prep costs to testify before regulators.
Media Liability	Defense and liability for online libel, slander, disparagement, misappropriation of name or likeness, plagiarism, copyright infringement, negligence in content to those that relied on content.	▪ Liability and defense costs. ▪ Commercial litigation – e.g., bank suits. ▪ Consumer litigation – e.g., class-actions.

Typical Cyber Gaps for Traditional Insurance Programs

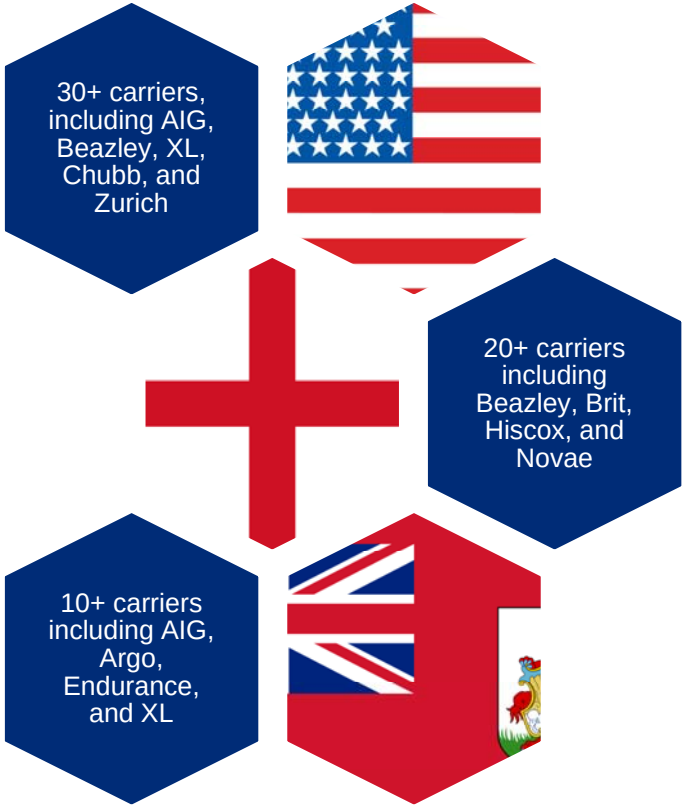
Cyber Peril	Traditional Insurance Policies				Potential Cyber Insurance Solutions
	Property	General Liability	Crime Policy	D&O	
Corporate IP					
Confidentiality of Corporate IP					Specialty IP Infringement Policies
Integrity & Availability of Corporate IP					Data Restoration Coverage
Third-Party Data					
Confidentiality, Integrity, and Availability of Third-Party Data					Comprehensive Cyber Policy
Technology Infrastructure					
Availability of Operational Technology, Core and General Information Systems					Network Business Interruption / Extra Expense Coverage
Availability of Outsourced Information Systems					Dependent Business Interruption Coverage
Relationship Capital					
Integrity (Value) of Relationship Capital (B2B & B2C)					Specialty Reputational Risk Policies
Financial Assets					
Availability (Theft) of Financial Assets					Cyber Crime Policies & Endorsements
Cyber-exposed Physical Assets					
Integrity (Physical Damage) of Cyber-exposed Physical Assets					Specialty Cyber Property Damage Policies

Marketplace

GLOBAL REACH, EXPANDING CAPACITY

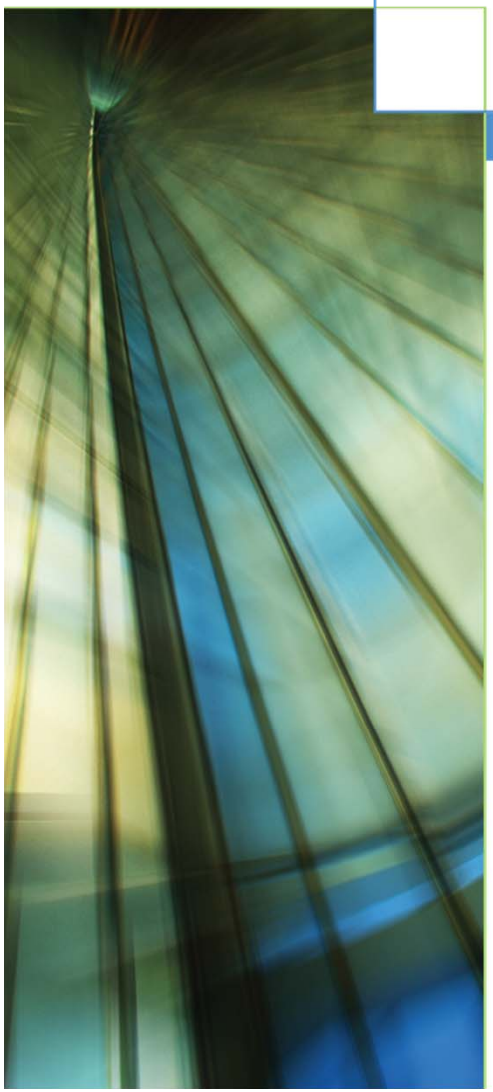
MARKET CAPACITY CONTINUES TO EXPAND

- Global capacity now exceeds US $1.6 billion.
- The largest programs are now US $600 million and higher.
- London and Bermuda markets are a key source of capacity.
- Industry focus is on business interruption coverage.



Risks Not Generally Covered By Cyber Insurance

Exposure	Losses not covered	Considerations
Reputational Damage	• Reduced value of Company's brand.	Global Brand Recognition.
Remediation Costs	• Costs to remediate systems or improve the network or controls beyond that which existed prior to a cyber-attack or data breach. • Costs to coordinate with law enforcement efforts.	No coverage for costs related to post-event system improvements.
Theft of Intellectual Property	• Theft of any intellectual property. • Lost or diminished value.	Publication of IP to public internet (Sony Pictures hack).
Cyber Crime	• Theft of funds from Company.	No coverage for employee initiated loss to Company or customer accounts.



Cybersecurity: Are You Prepared to Respond and Defend?

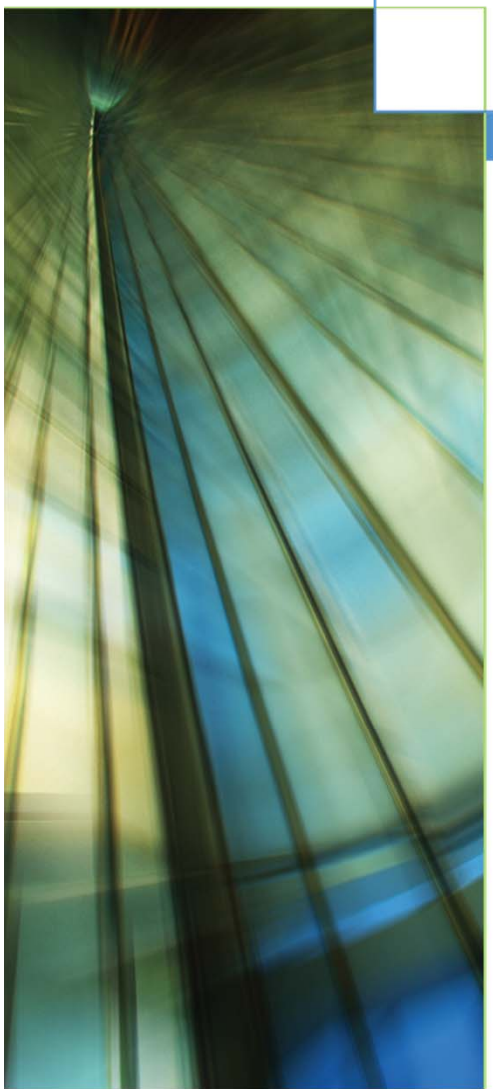
Annual Conference of the Conference on Consumer Finance Law

November 3, 2017

Lori Nugent
Shareholder
Cybersecurity, Privacy and Crisis Management
nugentl@gtlaw.com

GT GreenbergTraurig

- Beyond the Tipping Point
- Responding Well Matters
- Are You Prepared Financially?



Beyond the Tipping Point

GT GreenbergTraurig

Cyber Crime is Big Business

- Cyber Crime is the FBI's #3 Priority
  - Behind Terrorism and Espionage
- Top Hackers Subcontract
- Regulators "Help" Companies Understand that Cyber Threats Require Attention

GT GreenbergTraurig

Regulatory Hot Tin Roof

- Federal Agencies After OPM Breach
- State Regulator Coordination
  - Winning Since 2009
    - TJX Settlement by 41 AGs for $9.75 Million
- International Regulators' Scrutiny
  - Post-Snowden Mistrust
  - Different Values and Approaches
- **Regulators are Cash Positive**

GT GreenbergTraurig

Which Regulator is Most Aggressive?

- SEC
  - Sweeps
- FTC
  - Consent Decrees with Audits for 20 Years
- HHS
  - Hospice of Northern Idaho
- EU General Data Protection Regulation (GDPR)
  - Up to €20 Million or 4% of Annual Global Turnover
- State Attorneys General

GT GreenbergTraurig

State Regulators

California

- "Reasonable Security Procedures and Practices"
- Failure to Implement All of the Applicable CIS Critical Security Controls Constitutes "Lack of Reasonable Security"

New York

- NYDFS Cybersecurity Regulation
  - Requires Annual Compliance Certification
  - Fines up to $75,000 Per Day, Per Violation
  - Notice of Breach Within 72 Hours

GT GreenbergTraurig

NYDFS Cybersecurity Regulations

- Effective March 17, 2017
- Enforcement commences February 18, 2018
- Penalty Range:
  - Penalties assessed per day, per violation
  - $2,500 penalty for each violation
  - $15,000 penalty for violation if recklessly engaged in unsafe or unsound practice
  - $75,000 penalty for violation committed knowingly and willfully

GT GreenbergTraurig

NYDFS Cybersecurity Regulations

Requirements:

- Cybersecurity Program
- Cybersecurity Policy
- Appoint CISO
- Penetration Testing and Vulnerability Assessments
- Maintain Audit Trails
- Limit Access Privileges
- Application Security Procedures
- Conduct Risk Assessment

GT GreenbergTraurig

NYDFS Cybersecurity Regulations

Requirements:

- Utilize Qualified Cybersecurity Personnel and Intelligence
- Implement Third Party Service Provider Security Policy
- Use of Multi-Factor Authentication
- Policies and Procedures Limiting Data Retention
- Provide Cybersecurity Training and Monitoring
- Encrypt Nonpublic Information
- Develop Cybersecurity Incident Response Plan

GT GreenbergTraurig

Litigation Floodgates Opening

- **Standing:**

  Threatened Injury Certainly Impending and

  Fairly Traceable to Defendant

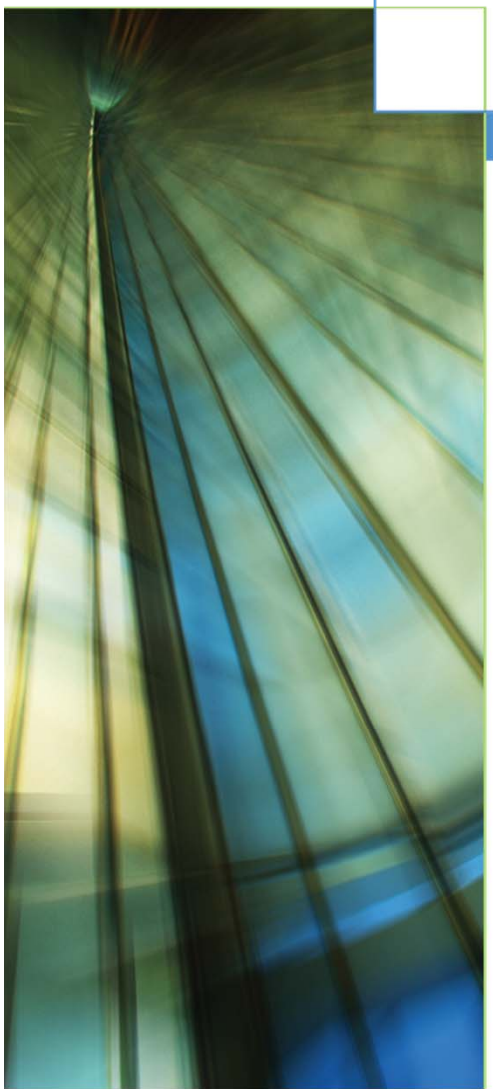
- **Neiman Marcus:**
- "At this stage in the litigation it is plausible to infer that plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."

GT GreenbergTraurig

Data Breach Class Action Claims:

- Negligence
- Breach of Contract
- Fraud
- Unfair Trade Practices/Consumer Protection
- Directors and Officers' Breach of Fiduciary Duty

Prepare for Defense on the Merits



Responding Well Matters

GT GreenbergTraurig

Your Response Impacts Your Outcome

- Sets that Tone for:
  - Public Perception
  - Regulatory Investigation
  - Litigation
- Act Quickly and Prudently to Protect:
  - Customers/Consumers
  - Shareholders and other Stakeholders
  - Brand
  - Cash Flow

GT GreenbergTraurig

Equifax Cybersecurity Breach

- 143M people affected
- Data exposed: full name, social security number, address, birth dates, and in some cases, driver's license numbers
  - Credit card information for approximately 209,000 people
  - Dispute documents with PII for approximately 182,000 people
- How it happened:
  - Known security flaw in web application development tool
  - Developer reported vulnerability to system users March 10, 2017
  - Breach took place mid-May 2017
  - Equifax waited until it "observed additional suspicious activity" a day after it discovered the breach to take the web application offline

GT GreenbergTraurig

Equifax Cybersecurity Breach

- More than 60 class action lawsuits filed over data breach
- Securities lawsuit:
  - Named Equifax, chairman of board and CEO, CFO as defendants
  - Stock price dropped from $145.43 per share in August to $93 per share in October
  - Top executives trade $1.8M in shares before breach publicly reported
  - Allegations:
    - Failed to disclose that Equifax did not maintain adequate data protection
    - Failed to maintain adequate monitoring systems
    - Failed to maintain proper security systems
    - Because of failures, financial statements are materially false
  - Equifax Board forms panel to review executives' share sales

GT GreenbergTraurig

What do Regulators Expect?

- Proof that You Care
- Timely Notification
- Quick, Accurate Count of the Impacted Individuals Resident in Each Jurisdiction
- Services for Impacted Individuals
- Clear, Fair Communication

GT GreenbergTraurig

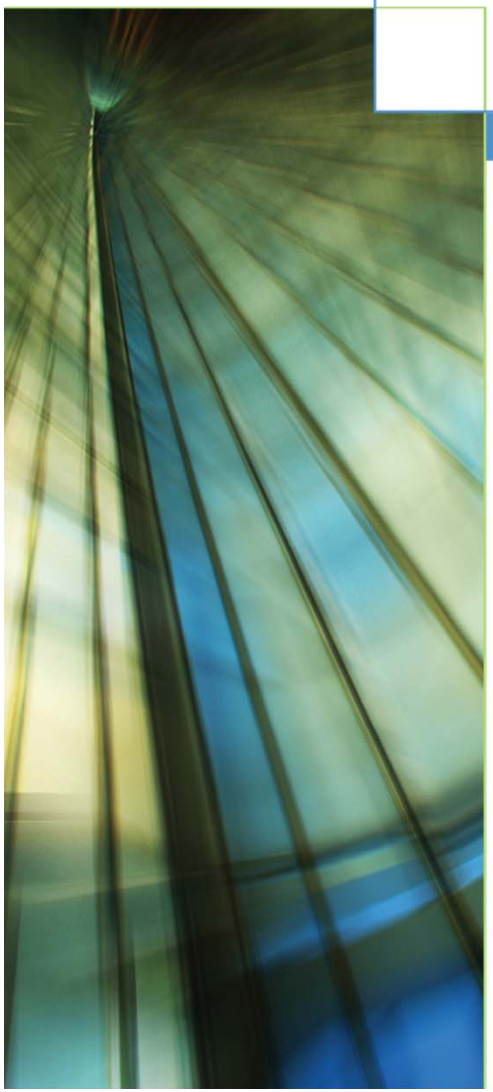
Who Needs a Seat at the Table?

- Responding Well Requires an Enterprise-Level Plan
  - IT
  - Legal
  - Compliance
  - Finance
  - Risk Management
  - Human Resources
  - Public Relations
  - Each Operating Unit

GT GreenbergTraurig

Strong Incident Response Plans Include:

- Agreed Upon Authority and Roles
- Stakeholder Communication Plans
- Prudently Engaged Management
- Board Involvement Consistent with Fiduciary Duties



Are You Prepared Financially?

GT GreenbergTraurig

Average Cost of a Breach (2017)

- The average cost of a breach is $225/record
  - Not all records are created equal:
    - Health Care: $380/record
    - Financial: $336/record
    - Educational: $245/record
    - Retail: $177/record
- The average cost of a data breach in the USA is $7.35 million dollars

GT GreenbergTraurig

Are You Prepared Financially?

- Do You Know Your Maximum Probable Loss and Likely Frequent Losses?
  - Maximum Probable Loss
    - $225- $380 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

GT GreenbergTraurig

Breach Scenarios to Consider:

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

Are You Ready to Respond?

GT GreenbergTraurig

GT GreenbergTraurig

Contact Information

Fred Karlinsky

KarlinskyF@gtlaw.com

Karl Pedersen

Karl.Pedersen@marsh.com

Lori Nugent

NugentL@gtlaw.com