Institute and Faculty of Actuaries

GT GreenbergTraurig

Cyber Pricing

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

26 April 2019

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.

Institute and Faculty of Actuaries

GT GreenbergTraurig

Overview

- Cyber Risk
- Cyber Risk Pricing
- The Cyber Insurance Market
- Cybersecurity Regulation
- Data Breach Mitigation Strategies

Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

GT GreenbergTraurig

Cyber Risk

GT GreenbergTraurig

What are Cyber Risks?

- Risk caused by:
  - using technology in your operations, or
  - handling/collecting/storing confidential information

Institute and Faculty of Actuaries

Cyber Is An Evolving Risk
Many Factors, Many Attacks

GT GreenbergTraurig

DATA BREACH

For a decade, hackers have persistently and successfully targeted consumer data.

RANSOMWARE

WANNACRY and PETYA. (2017) targeted the "Eternal Blue" vulnerability for a legacy Microsoft protocol. Self-proliferating capability spreads ransomware worldwide.

NATION STATE ATTACKS

In 2014, North Korean targeting of a media company with "wiper malware," disabling networks for more than a week and triggering 7 class action data breach lawsuits.

DEPENDENT BUSINESS INTERRUPTION

DYN DDoS (2016) Attackers using the Marai botnet to target a DNS provider with the largest DDoS attack ever recorded, degrading cloud services and websites worldwide.

INDUSTRIAL CONTROL ATTACKS

CrashOverride (2016) Second known malware designed to disrupt physical systems. Highly adaptable to target specific industrial control systems.

INSIDER ATTACKS

GEORGIA PACIFIC INSIDER (2014) Terminated systems administrator for remotely hacks into his ex-employer's industrial control system and caused significant damage.

SYSTEM OUTAGES

Cyber attacks & system failures repeatedly create havoc for airline systems, affecting major carriers.

Institute and Faculty of Actuaries

Latest Cybersecurity Trends and Statistics

GT GreenbergTraurig

Breaches directly caused by unintentional actions of insiders[2]

76%

Median number of days from an intrusion to containment of a breach[4]

62

Cyber crime costs the global economy annually up to[6]

$575B

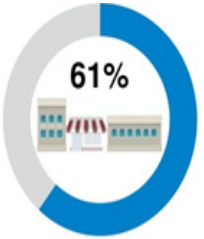
75% Breaches perpetrated by outsiders[2]

88% Same 9 patterns identified in 2014[2]

Ransomware infections have increased by[5]

36%

Percentage of breaches at companies with less than 1,000 employees



60% Breaches perpetrated by insiders[2]

Cost per Incident[7]
Global Average
$3.8M
23%
Increase over two years

105% Overall volume of malicious Android apps increased significantly[1]

98% Percentage of Denial of Service Attacks targeted large organizations[2]

1. Symantec, *Internet Security Threat Report 2017*
2. Verizon, *Data Breach Investigation Report 2017*
3. SANS Institute, *Combatting Cyber Risks in the Supply Chain*
4. Trustwave, *Global Security Report 2017*
5. Symantec, *Internet Security Threat Report 2017*
6. CSIS & McAfee, *Net Losses: Estimating the Global Cost of Cybercrime*
7. *IBM.*

Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

GT GreenbergTraurig

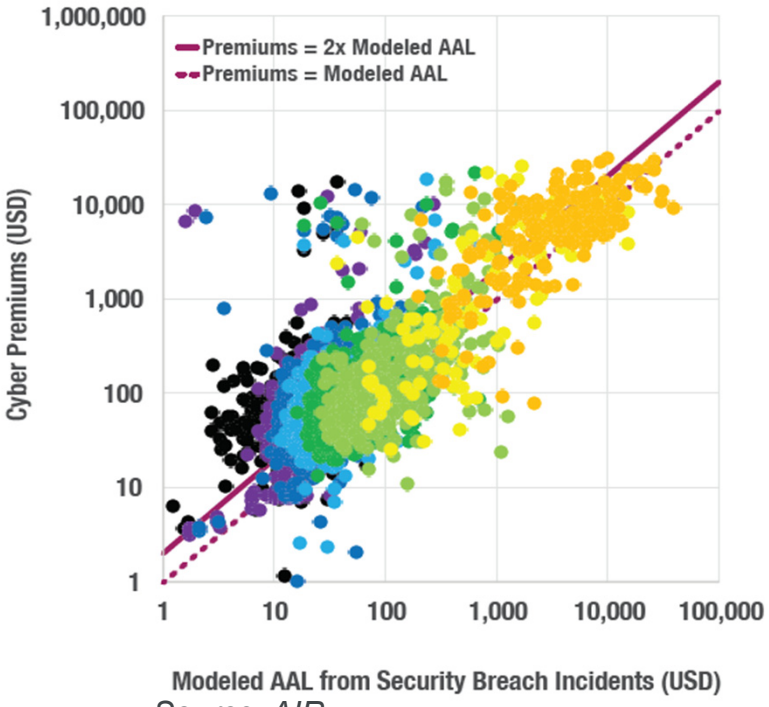
Cyber Risk Pricing

26 April 2019

GT GreenbergTraurig

Pricing Challenges

- Dearth of historical data
  - Existing data often includes non-cyber losses
  - Data often does not have useful information
  - "Silent cyber" risk
- Underwriters must rely more heavily on models to price cyber risk



Source: AIR

Institute and Faculty of Actuaries

GT GreenbergTraurig

Cyber Risk Models – Advantages

- Companies can better understand the full extent of their data breach vulnerability
  - Informs risk management strategies
- Incorporate both end-point security measures (passwords, firewalls, encryption, etc.) with the human element
  - The human element is the great factor in cybersecurity risk modeling
- Underwriting process may incorporate cyber risk assessment
  - Enables companies to proactively mitigate risks

Institute and Faculty of Actuaries

GT GreenbergTraurig

Cyber Risk Models – Potential Issues

- Inadequate pricing
  - Unknown maximum extent of potential cyber catastrophes
- Geographic scope of cyber risk
- Third party and network risk
  - Human element

Institute and Faculty of Actuaries

GT GreenbergTraurig

Cyber Risk Models – Potential Issues

- Nation state risk
  - Difficult to measure capabilities of nation state actors
  - Highly adaptable risk constantly changes
- New technologies
  - Difficult to keep up with changing technologies and consumer habits

Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

GT GreenbergTraurig

Cyber Insurance Market

GT GreenbergTraurig

Cyber Insurance Marketplace

- Annual premium volume information about the Cyber insurance market is hard to come by, but in reviewing the market, it is estimated that the annual gross written premium is anywhere from $2.0 billion to $4.0 billion (2017)
- The industry is divided by size (gross written premium) as follows:
  - A limited number of very large writers, with premiums in excess of $100 million
  - Several carriers in the $50-100 million range
  - Several carriers and large managing general underwriters in the $25-50 million range
  - Numerous carriers and smaller managing general underwriters in the $10-25 million range
  - Numerous entities writing in the $5-10 million and $1-5 million range

Institute and Faculty of Actuaries

GT GreenbergTraurig

Cyber Insurance Coverage Overview

Coverage	Description
Network Interruption/ Extra Expense	▶ Loss of income and/or extra expense resulting from interruption, partial disruption or suspension of computer systems due to a failure of technology. ▶ Dependent business interruption: Loss of income and extra expense as a result of a cyber breach on a critical vendor's network. ▶ Supply Chain Disruption: Loss of income and extra expense as a result of a cyber breach that affects a counterparty (scheduled to the policy) who is outside of your network.
Data Asset Protection	Costs to restore, recreate, or recollect your data and other intangible assets (i.e., databases, software, applications) that are corrupted or destroyed by a computer attack.
Data Breach Event Management	Costs to provide the following costs resulting from a privacy breach: Forensic service; Breach notification services (including legal fees, call center, etc.); Identity/fraud monitoring expenses; public relations.
Cyber Extortion	Costs of consultants and extortion monies for threats related to interrupting systems and releasing private information.
Privacy Liability	Defense and liability for failure to prevent unauthorized disclosure of confidential information (including failure of others to whom you have entrusted data). Coverage extends to personally identifiable information and confidential information of a third party.
Network Security Liability	Defense and liability for failure of system security to prevent or mitigate a computer attack including but not limited to spread of virus or a denial of service. Failure of system security includes failure of written policies and procedures addressing technology use.
Regulatory Defense Costs	Costs to defend a regulatory action or investigation due to a privacy breach, including indemnification for any fines or penalties assessed.
Media Liability	Defense and liability for media tort from online publication (libel, disparagement, misappropriation of name or likeness, plagiarism, copyright infringement, negligence in content).

Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

GT GreenbergTraurig

Cybersecurity Regulation

GT GreenbergTraurig

Cybersecurity Compliance

- More information = greater risk
- Sources of legal requirements:
  - Gramm-Leach-Bliley
  - HIPAA/HITECH
  - State law

Institute and Faculty of Actuaries

GT GreenbergTraurig

Cybersecurity Compliance

- New York Department of Financial Services: Cybersecurity Requirements For Financial Services Companies
  - Chief Information Security Officer responsibilities
- National Association of Insurance Commissioners: Insurance Data Security Model Law
  - Reporting standards
  - Interaction with New York's requirements

Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

GT GreenbergTraurig

Data Breach Mitigation Strategies

GT GreenbergTraurig

Threat Mitigation

- Data breaches:
  - Preparation and response
  - Legal defensibility
  - Cyber liability insurance
  - Class-action liability
  - Shareholder claims
  - Board duties and director liability

Institute and Faculty of Actuaries

GT GreenbergTraurig

Heightened Role of Board with Cybersecurity

- Addressing Cybersecurity risks can be unfamiliar territory for Directors
- Board must implement policies and oversight processes that focus on impending cyber threats and emerging regulatory developments
  - Establish clear communications and reporting of matters involving cyber risk
  - Appoint appropriate individuals to manage the organization's cybersecurity

Institute and Faculty of Actuaries

GT GreenbergTraurig

Scope of Risks

- Internet-exposed infrastructure (Companies & Vendors)
- Legal Defensibility Strategies
- Effective Business Continuity Plans – Are systems in place to deal with evolving threats?
  - "Red Teaming" – Cybersecurity firm identifies shortcomings before an attack occurs
  - Preemptive efforts to signal that board and management are paying attention to these risks

Institute and Faculty of Actuaries

GT GreenbergTraurig

Focus On Enterprise-wide Digital Footprint

- Data entry-point: Who gets the data?
  - Employees, third-party vendors, etc.
- What kind of data is obtained?
  - More private information is publicly available
- How is information used?

Institute and Faculty of Actuaries

GT GreenbergTraurig

Questions

Comments

Institute and Faculty of Actuaries

GT GreenbergTraurig

Contact Information

Fred E. Karlinsky, Esq.

Shareholder and Co-Chair, Insurance Regulatory & Transactions Practice

Greenberg Traurig, P.A.

401 E. Las Olas Blvd. Suite 2000

Fort Lauderdale, Florida 33301

(954) 768-8278

Karlinskyf@gtlaw.com

Institute and Faculty of Actuaries