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

26 April 2019
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.
Overview

• Cyber Risk
• Cyber Risk Pricing
• The Cyber Insurance Market
• Cybersecurity Regulation
• Data Breach Mitigation Strategies
Cyber Risk
What are Cyber Risks?

- Risk caused by:
  - using technology in your operations, or
  - handling/collecting/storing confidential information
Cyber Is An Evolving Risk
Many Factors, Many Attacks

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

RANSOMWARE

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.
## Latest Cybersecurity Trends and Statistics

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Percentage</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breaches directly caused by unintentional actions of insiders</td>
<td>76%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breaches perpetrated by outsiders</td>
<td>75%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ransomware infections</td>
<td>88%</td>
<td>Same 9 patterns identified in 2014</td>
<td></td>
</tr>
<tr>
<td>Percentage of breaches at companies with less than 1,000 employees</td>
<td>61%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breaches perpetrated by insiders</td>
<td>60%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost per Incident</td>
<td>$3.8M</td>
<td>Global Average</td>
<td></td>
</tr>
<tr>
<td>Overall volume of malicious Android apps increased significantly</td>
<td>105%</td>
<td>23% increase over two years</td>
<td></td>
</tr>
<tr>
<td>Percentage of Denial of Service Attacks targeted large organizations</td>
<td>98%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overall volume of malicious Android apps increased significantly</td>
<td>105%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber crime costs the global economy annually up to</td>
<td></td>
<td>$575B</td>
<td></td>
</tr>
</tbody>
</table>

2. Verizon, Data Breach Investigation Report 2017
3. SANS Institute, Combating Cyber Risks in the Supply Chain
4. Trustwave, Global Security Report 2017
6. CSIS & McAfee, Net Losses: Estimating the Global Cost of Cybercrime
7. IBM
Cyber Risk Pricing
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
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
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
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
Cyber Insurance Market
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
### Cyber Insurance Coverage Overview

<table>
<thead>
<tr>
<th>Coverage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Interruption/Extra Expense</td>
<td>▶ Loss of income and/or extra expense resulting from interruption, partial disruption or suspension of computer systems due to a failure of technology.</td>
</tr>
<tr>
<td></td>
<td>▶ Dependent business interruption: Loss of income and extra expense as a result of a cyber breach on a critical vendor’s network.</td>
</tr>
<tr>
<td></td>
<td>▶ 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.</td>
</tr>
<tr>
<td>Data Asset Protection</td>
<td>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.</td>
</tr>
<tr>
<td>Data Breach Event Management</td>
<td>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.</td>
</tr>
<tr>
<td>Cyber Extortion</td>
<td>Costs of consultants and extortion monies for threats related to interrupting systems and releasing private information.</td>
</tr>
<tr>
<td>Privacy Liability</td>
<td>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.</td>
</tr>
<tr>
<td>Network Security Liability</td>
<td>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.</td>
</tr>
<tr>
<td>Regulatory Defense Costs</td>
<td>Costs to defend a regulatory action or investigation due to a privacy breach, including indemnification for any fines or penalties assessed.</td>
</tr>
<tr>
<td>Media Liability</td>
<td>Defense and liability for media tort from online publication (libel, disparagement, misappropriation of name or likeness, plagiarism, copyright infringement, negligence in content).</td>
</tr>
</tbody>
</table>
Cybersecurity Regulation
Cybersecurity Compliance

• More information = greater risk

• Sources of legal requirements:
  – Gramm-Leach-Bliley
  – HIPAA/HITECH
  – State law
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
Data Breach Mitigation Strategies
Threat Mitigation

• Data breaches:
  – Preparation and response
  – Legal defensibility
  – Cyber liability insurance
  – Class-action liability
  – Shareholder claims
  – Board duties and director liability
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
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
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?
The views expressed in this presentation are those of invited contributors and not necessarily those of the IFoA. The IFoA do not endorse any of the views stated, nor any claims or representations made in this presentation and accept no responsibility or liability to any person for loss or damage suffered as a consequence of their placing reliance upon any view, claim or representation made in this presentation.

The information and expressions of opinion contained in this publication are not intended to be a comprehensive study, nor to provide actuarial advice or advice of any nature and should not be treated as a substitute for specific advice concerning individual situations. On no account may any part of this presentation be reproduced without the written permission of the IFoA and Greenberg Traurig, P.A.
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