Cybersecurity & Insurance Companies

Financial Stability Task Force
2014 Fall National Meeting, NAIC

Erez Liebermann, Vice President & Senior Counsel
Prudential Insurance Company of America
The Threat

• “From criminal syndicates, to terrorist organizations, to foreign intelligence groups, to disgruntled employees and other malicious intruders, the range of entities that stand ready to execute and exploit cyber attacks has never been greater.”

“There are only two types of companies: those that have been hacked and those that will be.”

- Former FBI Director
  Robert Mueller
Staggering Costs & Losses

• Last 6 months
  – Over 450,000,000 stolen credit and debit card numbers

• Past Year
  – Over $575,000,000 spent by corporations after data breaches
  – Over $1 Trillion estimated in IP theft
Awful Year for Cybersecurity
# Threat Actors

<table>
<thead>
<tr>
<th>ACTOR</th>
<th>TARGET</th>
<th>INSURANCE INDUSTRY</th>
</tr>
</thead>
</table>
| **NATION STATES**   | • Business plans  
                      |   • Trade secrets  
                      |   • Disruption                | • International Plans  
                      |                      | • Access to Services |
| **FOR-PROFIT HACKERS** | • Account numbers  
                      |   • Personally Identifiable Information  
                      |   • M&A data for insider trading    | • Customer Profiles  
                      |                      | • Account numbers |
| **HACKTIVISTS**     | • Disruption of operation  
                      |   • Embarrassment                        | • Critical for business operations and  
                      |                      |                            | business continuation |
| **INSIDERS**        | • Theft of intellectual property  
                      |   • Disruption of critical systems       | • Client lists  
                      |                      |                            | • Business continuity |
Industry Response
Shifting Focus On Cyber

• Holistic approach
  – Not only for information security personnel
• Board of Directors
• CEOs
• Counsel
• Public Relations
• Business Leads
Defending the Attack Vectors

• Historically: Hacking was an intellectual sport
  – Method: Defeat tough encryption
  – Defense: Better encryption

• Today: Hacking is a business
  – Method: Get around encryption
    • Social engineering
    • Attack the weak link (often vendors)
  – Defense:
    • Intelligence based security
    • Information sharing
Third Parties

• Smaller companies/vendors = bigger targets

• Solution
  – Increased due diligence
  – Contractual provisions requiring cyber security standards and notice of breaches
  – Information sharing

• Example:
  – Holding conferences for third parties to educate on the threat and require minimum standards
Preparedness

• What happens if “Target style” breach occurs?
  – Multiple parties ready to respond
  – Escalation processes
  – Security vendors and counsel

• True Preparedness
  – Incident response plan
  – Tabletop exercises
  – Board briefings
Types of Cyber Personnel

- Chief Information Security Officer
- IT Risk
- Cybersecurity Counsel
- Privacy Counsel
- Incident Response
Questions?

Erez Liebermann
Vice President, Prudential Financial, Inc.

973-802-5732

Erez.Liebermann@prudential.com