INSURED RETIREMENT INSTITUTE

IRI CYBERSECURITY FORUM 2016 REPORT

OVERVIEW

IRI recently hosted the Cybersecurity Forum, sponsored by Carlton Fields Jorden Burt and Ernst & Young. Attendees heard from industry leaders and regulators on updates to laws and regulations, insights into regulatory trends and activities, and advice on cybersecurity best practices to protect data and privacy for both the firms and their clients. Presentations from this highly engaging event are available here.

EVENT HIGHLIGHTS & TAKE-AWAYS

1. UPDATE FROM THE REGULATORS—NAIC, SEC, FINRA:

Eric Nordman, *Director of Regulatory Services and the Center for Insurance Policy & Research*, NAIC, reviewed and detailed developments and industry commentary for the NAIC Model Law. Based on commentary, uniformity emerged as the main industry goal. The revised Model Law draft will be available in advance of the NAIC Summer National Meeting in late August.

David Joire, *Senior Special Counsel*, SEC, commenting on the SEC's commitment to cybersecurity, including the recent appointment of a new Senior Advisor to the Chair for Cybersecurity Policy. Joire reviewed SEC guidance from 2015 asking advisors to focus on cybersecurity and perform a gap analysis of their cyber capabilities. Attendees heard about SEC suggestions for compliance, maintenance of process, recent enforcement actions and comments on SEC cybersecurity regulations like SCI.

John Brady, *Vice President Cybersecurity/CISO*, FINRA, closed out the panel with a number of highly informative observations and recommendations.

- Observations:
  - Cyber awareness is high.
  - No single "right" approach to cybersecurity.
  - Most firms have established risk management practices, but branches lag behind HQs
  - Response plans are not exercised regularly enough.
  - "One size fits all" cybersecurity solutions are exceedingly difficult to implement, and may not even be the most effective means of protecting consumer information.
- Recommendations:
  - Designate an individual responsible for cybersecurity.
  - Periodically test security controls through penetration testing.
  - Perform diligent record keeping.

2. CURRENT RISK ENVIRONMENT—IDENTIFYING RISKS AND MITIGATION STRATEGIES, IMPACT OF NEW THREATS AND NEW TECHNOLOGIES: Michael Wood, *Senior Manager*, Ernst & Young, led a session identifying the mitigation strategies available to combat threats from new technology.

- Factors Making Insurers Vulnerable to Cyberattacks :
  - Perception—namely, that insurers are perceived to be less secure than banks and asset managers.
  - Third-party vendors—reliance on these vendors for business and IT solutions leaves insurers susceptible to the weaknesses of third-parties with less security.
  - Outsourcing—data shared externally (data entry, third-party processors, etc.)
  - Brokers and agents—independent agents with remote access to key systems can be compromised by phishing or other means without oversight.
- New Technologies: New technologies like wearable technology, "smart" homes and cars, tracking sensors on commercial vehicles, and more sophisticated GPS software create more avenues for breach, and necessitate new plans and strategies. The "Internet of Things"—the interconnectivity of people, organizations and devices—creates new vulnerabilities for criminals to target.
- Impact of New Threats: Internet of Things threatens the insurance business in two main ways:
  - Digital trust: Consumers need to trust insurance companies to secure their personal information, and insurance companies need to trust the information from the consumers is valid and from a trusted source.
  - Product security life cycle: insurance companies need to secure the product development life cycle for products provided to consumers and/or industries.
- Three Lines of Defense
  - *First line:* Risk takers and enablers—identify the risks.
  - *Second line:* Risk monitors—send feedback to first line of defense.
  - *Third line:* Risk assurers—provide a view beyond micro-level risk management to promote a culture of security and staying ahead of the game.

3. BREACH PREPARATION AND RESPONSE—BEST PRACTICES: Susan Giuliano, *Vice President—Compliance*, Prudential, shared a number of strategies for breach preparation and response.

- In-house phishing exercises are very effective in testing both employee readiness, as well as the proficiency of the response strategy and execution.
- While smaller firms may lack some resources that the larger firms have, coordination and reaching every member of the firm is a built-in advantage for the smaller firms.
- Business construction plans should be aligned with the cybersecurity plan.
- Not everyone in your company needs to have access to everything.

Grady Marshall, *Special Agent, Cyber Investigations*, U.S. Secret Service, encouraged firms to have a preexisting relationship with law enforcement in the event of a cyberattack. Marshall and Giuliano agreed that "the team" to handle cyber threats and attacks should consist of:

- Legal, Compliance, Business, IT, Outside Counsel, Law Enforcement, PR

Shawn Fohs, *Senior Manager, Cyber Investigation & Forensic Technology,* Ernst & Young, added each part of the team should have a defined role during an investigation. Documentation during the investigation is key (chain of custody, actions taken by response team, indicators, and information lost).

4. ***ENFORCEMENT AND LITIGATION UPDATE:*** Joseph Swanson, *Co-Chair, Data Privacy and Cybersecurity Task Force*, and Kristin Shepard, *Shareholder*, Carlton Fields Jorden Burt, led an informative presentation about recent events in the enforcement and litigation space.

- Attorney Client Privilege and Attorney Work Product: Swanson gave an overview of the kind of materials protected, as well as the nuances between attorney client privilege and work product. Both protections played a role in recent enforcement actions and lawsuits.
- State Enforcement: All but three states (Alabama, New Mexico, and South Dakota) have laws requiring notification to affected individuals in breach situations, and states have begun enacting laws governing cybersecurity standards for numerous industries, including financial institutions.
- Market Conduct Examinations: State insurance regulators investigate compliance with rules and regulations, with a focus on conduct in product distribution and claim settlement. Some jurisdictions have routine examinations, while others look for indicators. All respond to big events like a massive breach.
- Date Breach Litigation: Different classes of plaintiffs; can be consumers, employees, or financial institutions. The circuit courts are split on the issue of Article III standing; the issue seems ripe for Supreme Court review in the near future.
- Cybersecurity Information Sharing Act: CISA has many benefits, including no disclosure under FOIA, no enforcement based on information provided, and no antitrust exposure, among others. A final guideline on CISA was issued in June 2016.
- Shareholder Derivative Litigation: When a shareholder of the corporation brings an action against directors and/or officers when the corporation has refused to take action, breached fiduciary duties, bad faith and other forms of mismanagement.

5. VENDOR AND SUPPLY CHAIN RISK—BEST PRACTICES: Chris Ritterbush, *Executive Director*, Ernst & Young, shared results from Ernst & Young's Third Party Risk Management Survey. Key trends include:

- Top three focus points for regulatory reviews were (1) oversight and governance, (2) enterprise critical third parties, and (3) information security/business continuity assessments.
- Alignment of oversight activities and Board reporting.

- Hybrid and centralized operation models.
- Development of assessment frameworks and models.
- Increase in Service Organization Controls (SOC) Report reliance.

Timothy Nagle, *Former Vice President and Chief Privacy Counsel,* Prudential Financial, offered the in house perspective for third-party risk management. Steps include:

- Initial due diligence and vendor selection.
- Assessment and agreement negotiation.
- Ongoing supervision.

6. ***LATEST DEVELOPMENTS IN CYBER RISK INSURANCE:*** Bert Helfland and John Pitblado, *Shareholders,* Carlton Fields Jorden Burt, gave an overview of the evolution of cyber coverage, and how as cyber risks increased, policies evolved to included exclusions, cyber-specific coverage and others. Today there still remains areas of uncertainty in the cyber insurance realm:
   - Lack of Data.
   - Lack of Standards—no standard policy language yet.
   - Regulatory Uncertainty—variations in state remediation laws, underwriting problems.

Christopher Liu, *Head of Financial Institutions Cyber,* AIG, covered how to insure against cyber events:

- <u>Areas of Cyber Insurance Coverage</u>
  - First Party Losses
    - Data Breach Expenses (cost of: forensic investigation, legal advice, notice and remediation, and public relations services)
    - Data Restoration Replacement
    - Business Interruption Losses
    - Extortion Payments
    - Losses from Fraud and Theft
  - Third Party Losses
    - Privacy Liability
    - Network Security Liability
    - Technology Services Liability
    - Media Liability/Content Liability
    - Social Media Liability

The main takeaway from the panel can be summed up in a few words: the best cyber defense is self-defense. The better an organization's cybersecurity program, the better coverage they can receive. Better preparation and coverage mitigates the risks of an event, and reduces the cost of responding to an attack, in addition to making compliance with regulators much easier.