Chicagoland Risk Forum | October 9, 2017 | Cyber Presentation

Theme: An Integrated Approach to Cyber Resilience

Jon Laux & Sam Tashima

- **Context: we are actuaries speaking with risk managers – not going to pretend to be cybersecurity experts, but we'll talk about some of the themes from those disciplines and why it's important to take an integrated approach to cyber risk management**
- **The challenge of managing cyber risk**
  - Cyber presents a challenge to risk management because it doesn't fit neatly in boxes
    - Financial damage & tangible damage, 1st party & 3rd party
    - Importance of business interruption risk affecting all industries – wider than data breach
  - Example: NotPetya attack
    - Several examples of companies impacted, both directly & indirectly
  - Organizationally, cyber presents challenges too
    - CIO / CISO vs. CRO / risk manager – if not coordinated, easy to see cyber as just a technology problem etc.
  - Vision of cyber resilience as an integrated process between cybersecurity & insurance
    - 4 steps (Jim Trainor framework)
- **State of the cyber insurance market**
  - What cyber insurance is – what's covered, what's not, how it relates to other P&C coverages
    - Highlight coverage gaps / challenges with property insurance, etc.
  - Coverage trends
  - Claims
  - Pricing
  - Profitability
    - Recent historical results
    - Note – no insurer is doing a cat load for cyber premium - now that we are beginning to look at this, cyber doesn't look as profitable!
  - What's contentious / what's valuable to you
- **Modeling cyber risk**
  - Including how insurers think about you as a risk
    - E.g. I've heard small business owners say insurers don't' know anything about my cybersecurity – they don't' need to – at that company size, it's just a bet for them.
    - Could highlight some cool market entrants in the space though that are using tech to lightly evaluate risk for SME's
    - Note I'm not sure if this is a separate section or not
  - The challenges
    - Debunking the myth of no data
  - Evolving hazards
  - Modeling framework
    - (I'm using Exposure / Hazard / Vulnerability from the nat cat world – let's merge this or port over to the Aon Cyber 360 framework)
    - Key assets
    - Threat actors
    - Cyber triggers (note these are the things your cybersecurity team should be watching)
    - Events / impacts
  - What drives exposure

        - Company size & industry – tie to motivation of threat actors

- **What you can do**
    - Coordinate across functions: CEO, CIO/CISO, CRO/risk manager, CHRO…
    - Risk assessment
    - Incident response plans
        - (tie to financial impact of being well coordinated vs. not – old NetDiligence study cites this)
    - Buy the right amount of insurance coverage for your organization