RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: CXO-W03

Can Cyber Insurance Be Linked to Assurance?

Larry Clinton
President and CEO
Internet Security Alliance
@ISalliance

Dan Reddy
Adjunct Faculty: Engineering & Technology
Quinsigamond Community College
@danlj28

Rethinking Cyber Security

- Cyber security is NOT an “IT” issue
- We are not worried (just) about hackers
- The system is weak and getting weaker
- We can’t secure the perimeter
- We should probably stop blaming the victims
- We can’t mandate security
- *Assuring* security requires economic sustainability

The Economics of Cyber Security

- Breaches and stock value
  - Sony stock UP 26% since their attack
  - Target UP 22% since their attack
- Modern technology and business practices can undermine security
- The economics of cyber security are out of balance
- How do we make security profitable/affordable?

The Government Turns Around

- 2002 National Strategy to Secure Cyber Space - everything is going to be alright…
- 2012 Leiberman-Collins proposed legislation
  - DHS should mandate standards with SOX-like penalties for non-compliance
  - It failed miserably !
- 2013 President Obama's Cybersecurity Executive Order
  - A social contract with industry
  - Consensus standards (NIST) motivated through market incentives including insurance

Brief History of Cyber Insurance

- Traditional Insurance Policies to Cover Business Loss
  - Business Personal Insurance Policies (first-party loss)
  - Business Interruption Policies
  - Commercial General Liability (CGL) or Umbrella Liability Policies (for damage to third parties)
  - Errors and Omissions Insurance (for Corp. Officers)
- **1970s** - Development of specialized policies that typically extended crime insurance to cover against outsider gaining physical access to computer systems
- **1998** - Advent of Hacker Insurance Policies
- **2000** - Early Forms of Cyber Insurance (1st and 3rd Party) Appear
  - 1st Party – Generally, covers destruction or loss of information assets, Internet business interruption, cyber extortion, DDoS loss, PR reimbursement, fraudulent EFTs
  - 3rd Party – Generally, covers claims arising from Internet content, security, tech errors and omissions as well as defense costs

Benefits of Cyber Insurance (Nation)

- **Ecosystem Benefits –**
  - ***Reduction of Externalities -*** Insurers require some level of security as a precondition of coverage, and companies adopting better security practices receive lower insurance rates; this helps companies to internalize both the benefits of good security and the costs of poor security, which in turn leads to greater investment and improvements in cyber-security
  - ***Evolving Standards*** - Insurers have a strong interest in greater security, and their requirements are continually increasing
  - ***Smoothing Mechanism*** - Insurance provides a smooth funding mechanism for recovery from major losses, helping to businesses to return to normal and reducing the need for government assistance

Benefits of Cyber Insurance (Policy Holder)

- **Firm Benefits –**
  - In addition to the obvious benefit of legal and first-party expense reimbursement, the purchase of a specific cyber risk policy has a number of other indirect benefits, including:
    - The ability to obtain an objective, usually free, review of a company's network security by a third party (i.e., the insurer or its agent)
    - A better ability to understand the company's risk level by working with brokers and discussing policy options including what can and cannot be insured
    - Better quantification of net financial risk
    - Finally, the demonstration of the successful ability to purchase insurance could be a favorable factor with state regulators or the SEC who have published guidance on this topic

Challenges to Cyber Insurance

- **Actuarial Data** - Insurers have little actuarial data on which to base premium rates and make those rates competitive; they have attempted to overcome this hurdle by collecting relevant data and reaching out to research organizations, such as CSI and Verizon, that can provide contextual statistics on cyber risk.

- **Complex Regulatory Environment** - New federal data breach regulations are currently under consideration and consumer protection laws vary from state to state; liability for cyber incidents is sometimes ill-defined, and as a result litigation of a cyber insurance case is likely to be far more murky than a conventional one.

- **“Monoculture” of Computing Technologies** - Monoculture refers to low diversity of technologies deployed across enterprises thus making attacks easier to design for multiple targets.

(More) Challenges to Cyber Insurance

- **Interconnectivity -** Networked systems have the potential to infect one another in a cascading effect, as was the case with the *Conficker* worm. Again, in this case, insurers cannot use conventional risk models to analyze their exposure

- **Traditional CAT (Catastrophic) Modeling Does Not Work** – This is because it is based on geographic parameters which are not applicable to a cyber risk event

- **Lack of Universal Demand** – some segments of cyber market are growing rapidly (like PII) but catastrophic coverage remains difficult

Cyber Scenario #1: Government is the Insurer of Last Resort – but…

- Insurers provide coverage but their own limits are backed up by Governments
  - As with Acts of God, Government has role for catastrophic damages
- **Pros:** Provides an outer limit for Insurer's exposure. May create more reasonable costing in middle.
- **Cons:** Political concerns (not likely in post " Gov't Bailout" climate). Moral hazard. Not fair to the taxpayer.

Key Dynamics in the Scenarios

- What is covered, what is not?
- Cost of Premiums
  - What can lower my premiums? (Secret sauce handled by brokers)
- How measureable are the preventative offsets to lower premiums?
  - Is it better for the insurance industry and policy holders to have simplicity or more assurance?
- How can limits be established?
- Is the coverage suitable for businesses of all sizes?
  - How do industry profiles feed into the coverage and risks?

What's a Company to do? Some Questions to Ask

- How much data are you willing to put at risk?
- What risks will you avoid, accept, mitigate, or transfer?
- Do you already have insurance covering cyber?
- What will a new policy cover?
- How are losses measured?
- Does it cover ID theft?
- Is there directors and officers liability **(**D&O) exposure?

Your Coverage May Vary

- First party
  - Breach management - actual incremental direct costs
  - Coverage on intangible assets (reputation, tarnished brand, etc.)
  - Business interruption
  - Response and remediation re: network protection & info assets
  - Cyber extortion
  - Ongoing protection against future threats
- Third party
  - Liability against law suits
  - 1st party direct costs to 3rd parties (Identity theft & credit enrollments)
  - Cyber privacy - disclosure
- Exclusions
- Limits

Cyber Scenario #2: Ride the Wave

- Working reasonably well for insurers and policy holders
  - Brokers sometimes stuck in middle
- Requirements to qualify - quite surmountable
- Breach focused
  - Costs are known: e.g., ID and credit protection
- More due diligence won't change dynamics
- **Pros:** Claim rate within acceptable range; some company peace of mind
- **Cons:** May not scale for long term

Cyber Scenario #3: Detailed On-site Assessment to Qualify

- Cyber experts (think red-team) conduct audit of defensive posture
- Tied to business size/profile
- External response team available for event management
- **Pros:** Risk better understood by insurer. Client starts improvements knowing the cost/benefit. Crisis resources available.
- **Cons:** Heavy up front lift by insurer. Harder to make scalable

Cyber Scenario #4 – Survey Approach

- Insurers and policy holders want simplicity
  - The more the merrier. Can it follow the 80/20 rule for workability?
- Client completes questionnaire with 100 key indicator questions
  - Experts in company each contribute answers (technical, legal, business)
  - Weighted analysis of responses puts clients in banded tiers of risk
- Premiums and limits set accordingly
- **Pros:** Some scalability means larger pools. Models are adjustable.
- **Cons:** Heavy reliance on survey & models. Must create meaningful tiers.

Cyber Scenario #5 – "FICO®-like" Cyber Score

- 3rd party calculates security rating score to reflect security posture of companies:
  - Uses externally available indicators (e.g., security events & configurations) fed into algorithm to create a normalized score
  - Scores used in profiling for insurance
  - Theory seems to be "If you are sloppy in your company's external web world then you may be susceptible elsewhere."
- **Pros:** It's uniform and consistent. Doesn't require engagement with the company being rated. Just fighting to correct your score may actually improve your readiness.
- **Cons:** The indicators are debatable as whether they have a strong correlation to your cyber security posture. In cloud or outsourced service world, the purchased infrastructure may not be reflective of your company's protection.

Cyber Scenario #6 – Organization (Policy Holder) gets Certified or Assessed Using Standards

- Organization complies to security standards as part of profile assessment
  - Examples:
    - Critical infrastructure complies with Cybersecurity Framework (NIST)
    - Audited using ISO 27001/27002 security standards
- **Pros:** Allows organization to manage their own work, can be measurable without heavy investment by Insurer. Cost/benefit becomes more evident.
- **Cons:** Not simple or fast. (may take year+ to complete). Many controls may not be cost effective.

Reference Models for Cyber Assurance?

- ISO/IEC 27001/27002
- Management practices and security controls
- 27001 alone: 114 security controls in 12 groups
- Applies to any organization

- NIST Cybersecurity Framework
- 5 Functions
- 22 categories
- 98 subcategories
- Applies to “Critical Infrastructure”

- SANS Top 20 controls
- Consensus guidelines
- Many agree “Just do these 20 things”

- “Economics of Cybersecurity”
  [AFCEA Cyber Committee;
  [Australian Department of National Defence’s (DND)]
- 4 controls that are most cost effective
  1. Restricting user installation of apps - “whitelisting”
  2. Ensuring that the operating system is patched with (security) updates
  3. Ensuring that software apps have current updates
  4. Restricting administrative privileges

Recommended Composite for More Assurance

- Start with evidence that cost effective controls have been implemented.
  - Offer incentives to stretch beyond cost effective controls (4) to get next set of reasonable controls.
    - Qualification to get better tiers of coverage (more coverage beyond breach and privacy loss)
    - Significant premium reduction
- **Pros:** Practical. Organizations should be doing cost effective controls anyway. Reasonable stretch can actually raise all boats . Simple enough and scalable.
- **Cons:** Doing anything with focus is hard (even top 4). Could still be hard to measure consistently. (e.g., how often should updates be applied?)

Apply It: Consider Your Use Case

- Buyer Persona :
  - What is your carrier/broker doing to have you qualify or to offset premiums?
    - Bring what you learned from scenarios
  - What's covered and what's not?
    - Consider the post breach focused world
- Insurance Carrier Persona: What are you expecting from buyers?
  - Simple model or complex evaluation to qualify or set premiums?
  - Seeing this potential are you more encouraged about the market?
  - Are your brokers on board with you?
- Government/Industry Persona: Will more cyber insurance generate more prevention activities? Can it encourage more voluntary investments?
  - What role does government play?