Addressing Cyber Risk

May 11, 2017
“Take-up rate” refers to the overall percentage of clients that purchased standalone cyber insurance coverage.
US Cyber Insurance Growth Rates

"Growth rate" refers to the percentage increase from 2015 to 2016 in the number of clients purchasing standalone cyber insurance coverage.
Marsh’s recent survey of capacity for large purchasers indicates cyber capacity — stated but not necessarily deployed — is approximately $1 billion. Through the first quarter of 2017, many large towers placed of between $200 million and $500 million in limits have been placed. Insurers are increasingly willing to deploy large lines either in single layers or with ventilation.

**Cyber Insurance Market Capacity**

- **2014**
  - US: 59%
  - Bermuda: 20%
  - London: 20%
  - Reinsurance: 1%
  - Total Cyber Capacity: +$890 million

- **2017**
  - US: 63%
  - Bermuda: 15%
  - London: 21%
  - Reinsurance: 1%
  - Total Cyber Capacity: +$1.4 billion
Evolving Cyber Coverage

Basic Cyber Coverage

- Privacy Liability
- Network Security Liability
- Network Business Interruption
- Cyber Extortion
- Data Asset Restoration

Expanded Cyber Coverage

- Dependent Business Interruption
- System Failure
- Supply Chain Interruption

Broader terms of coverage for economic impact due to network outages.

Extension of Cyber Coverage

- Cyber Related Property and Casualty Loss

Provides coverage for physical outcomes from network security incidents.
Heartbleed

- Heartbleed is a configuration vulnerability
- Heartbleed affected approximately 500,000 websites
- Prominent websites, online banking, VPN, phones, routers, medical devices, TVs, embedded IoT and millions of other devices
Systemic Cyber Risk
Single Points of Failure

- DYN is a major DNS Service provider.
- October 2016 - Mirai Botnet Attack launches massive Distributed Denial of Services Attacks
- Affected approximately 145,000 domains (Twitter, Reddit, CNN, PayPal)

Source, Level3
Systemic Cyber Risk
Cascading Consequences

- Imagines a "sensational" cyber attack that triggers a widespread blackout
- Outage reaches 15 states and Washington DC (93 million people without power)
- Shuts commercial activity responsible for 32% of the US economic production.

Key Findings
- Cyber attack is a peril that could trigger losses across multiple sectors of the economy.
- The insurance industry should enhance the quality of data available and to continue the development of probabilistic modelling.

Source, Lloyd’s 2015
Protecting Against Cyber Risk Aggregation

Tools to prevent cyber risk aggregation include:

- Policy Language
- Underwriter Submissions
- External Assessments

Tracking “Silent Cyber”

Source, AIR Worldwide
Improving Cyber Resilience through Behavioral Change

Cyber insurance can create important incentives that drive behavioral change

- Causes third-party assessments of cyber practices
- Ties insurers to insureds through financial incentive
- Aligns mitigation, response and recovery tools
- Partnership between industry and government is essential for building cyber resilience

Pursuant to Executive Order 13636, the Departments of Treasury, Homeland Security and Commerce produced separate reports on cyber incentives. Each identified cyber insurance as a potential incentive for adoption of better practices.