



## Cyber Today

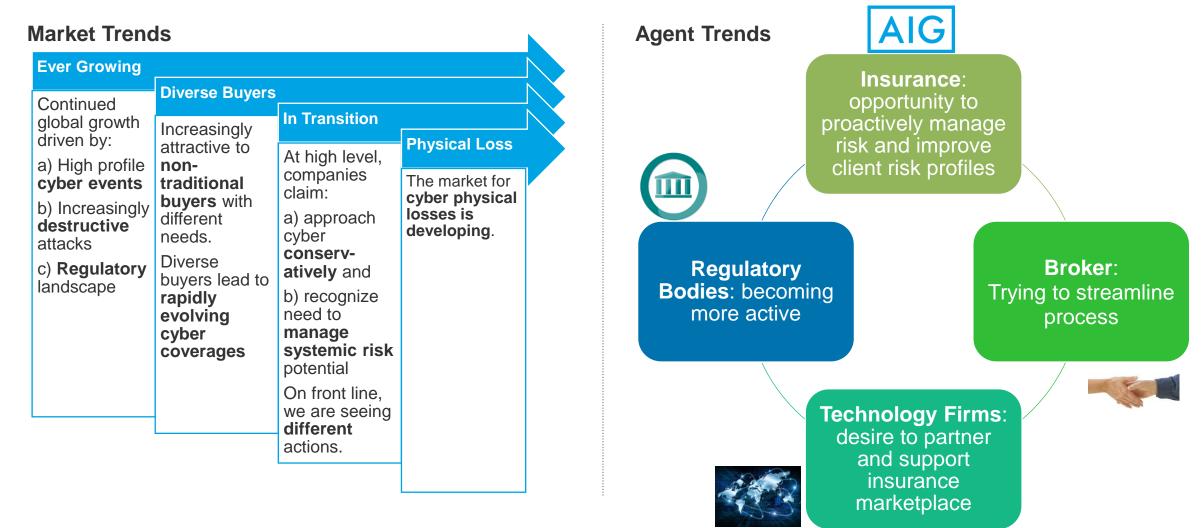
Outlook, Underwriting Challenges and Recommendations Thursday, August 17, 2017



Tracie Grella
Global Cyber Practice Leader
+1 212 458 1875
Tracie.Grella@aig.com

## Outlook

The cyber security market is rapidly evolving to meet the commercial sector's growing dependence on information networks to conduct business





## **Underwriting Challenges**

Underwriting challenges are evolving as the nature of cyber risk expands. High quality data, risk management and partners are essential to ensure the insurance industry's ability to meet cyber security risks.

#### **Data Quality**

#### Risk Management

#### **Partners**

Quality data is crucial to the sustainability of expansive cyber insurance

- Data required to properly differentiate risk is extensive
- There is a lack of visibility on supply chain, which makes risk analysis more difficult

Aggregation risk and coverage expansion require dedicated, data-equipped risk management

- Managing systemic cyber risk across all coverage lines
- Management of resources and expertise as non-physical cyber coverage expands into traditional physical loss based policies
- Identification, evaluation and modeling of the nodes of aggregation

Coverage comparability and education are essential to healthy competition

- As more carriers enter the market, coverage comparison becomes more challenging for brokers
  - Brokers are responding with broker forms and a desire to streamline the process
- There is a significant education gap as more brokers, clients and underwriters enter the cyber insurance market,



## Recommendations

Proper education, risk management and cyber security incentives can lay the foundation for national cyber security as the threat landscape continues to grow and evolve.

Education

- Scenario Planning Workshops AIG prepared to facilitate across industries
- Cybersecurity Education more training of cybersecurity professionals and research funding
- Public Service Campaign raise awareness of cyber hygiene and distribute recommendations



Risk Management

- Geopolitical Risk Management Federal agencies take lead on geopolitical cyber protection
- Software and Hardware Security Standards create independent organization seconded to developing cyber security standards and certifying devices



Incentives

- Tax Incentives for Cybersecurity Investment to help companies invest in cyber security
- Government Intelligence Sharing enhance Information and Security Analysis Centers (ISAC)
- Legal and Regulatory Immunity to promote cyber security innovation and technology





# Q&A

