FACI

Cyber Risk Discussion
What does cyber mean to us?
Companies must leverage **internal** and **external** relationships and **expertise** to get the most accurate picture of their cyber exposure:

They must understand:

- Value of data assets at risk
- Actual cost to rebuild or replace data assets
- Impact of cyber attack
- Organizational record count **PHI/PCI/PII**
They must understand:

- Where contractual indemnities are provided or not provided
- Cultural awareness of privacy training implementation, data security, & social engineering
- How many ‘at risk records’ lie within one database or application
Develop an Incident Response Plan

Why?

To be prepared to respond with a unified & impactful approach

Use internal resources & outside support as needed
Cyber Enterprise Risk Management

Cyber Risk strategy built on the fundamentals of the NIST framework:
Hackers Are Becoming More Sophisticated
Data Theft – Economic & Political Advantage

North Korea to U.S.: Show evidence we hacked Sony

By Madison Park and Dana Ford, CNN

D.N.C. Hack Raises a Frightening Question: What’s Next?

The Interpreter
② By AMANDA TRUB - JULY 29, 2018

CYBER RISK DISCUSSION
Cyber Criminals – Financial Gain

Hackers hold hotel's keys hostage for bitcoin ransom

By Madaline Heilcombe, CNN
Updated 2:19 PM ET, Mon January 30, 2017
WikiLeaks claims to reveal how CIA hacks TVs and phones all over the world
Distributed Denial of Service (DDoS) Attack

DDoS attack that disrupted internet was largest of its kind in history, experts say.

Dyn, the victim of last week’s denial of service attack, said it was orchestrated using a weapon called the Mirai botnet.
Assets = Exposure

Understand your threat environment

Identify & protect your mission critical assets
Threats Dependent on Organization

- Intellectual Property & Corporate Confidential Information
  - Patents
  - Trademarks
  - Industrial Design
  - Trade Secrets

- Personal Data
  - Personally Identifiable Information
  - Personal Health Information
  - Payment Card Data

- Physical
  - Operating control systems remotely through corporate IT network creates vulnerabilities to physical assets
What Is the Insurance Industry Doing About It?
Challenges for the Insurance Industry

• Lack of actuarial data
• Risk aggregation
## Evaluation of Risk Transfer

### Quantitative Factors
- Contracts
- Geography
- Industry Sector
- Cyber Threat Landscape
- Privacy
- Data Type and Amount
- Breach Scenario Costs

### Qualitative Factors
- Information Technology Security
- Privacy
- Risk Tolerance
- Peer Benchmarking
- Cost of Capital
- D&O Macro Market
- Budget
Risk Transfer Process

- Identify
- Discuss
- Prepare
- Execute
- Support
How can the government help?
Our Mission

To be the worldwide value and service leader in insurance brokerage, risk management, employee benefits, and retirement services

Our Goal

To be the best place to do business and to work