Attachment 3

Cyber Insurance

An Analysis of Trends, Data, and Market Dynamics

Koty Henry
Cybersecurity Policy Advisor
October 30, 2024

NAIC NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

Introduction & Overview

- Purpose and Scope
- Data Sources: NAIC's Property & Casualty Annual Statement Cybersecurity and Identity Theft Supplement, and Alien Surplus Lines Data

Market Overview

- Global Premium: $ 16.66 Billion
- U.S. market share: 59% ($9.84 Billion)
- Growth trends and market stabilization with smaller rate increases and, in some cases, flat renewals according to Gallagher
- The U.S. cyber insurance market is the largest in the world, driven by increasing demand and evolving cyber threats

Key Metrics

- Direct Written Premium
  - U.S. domiciled insurers wrote $7.25 billion
  - Alien surplus lines wrote $2.59 billion

- Number of Policies in Force
  - Increase of 11.7% in 2023 to 4,369,741 policies
  - Reflects growing demand for cyber insurance coverage

Claims and Losses

- **Claims Data**
  - Number of claims: 33,561 in 2023
  - Trends in claims frequency and severity, particularly ransomware and business email compromise
- **Loss Ratios**
  - Analysis of loss ratios for top insurers

Market Dynamics

- **Demand and Take-Up Rates**
  - Increasing demand among small and medium-sized enterprises
    - 72% of SMEs without cyber insurance say a major cyberattack could destroy their business
  - Factors driving demand: cyber incidents, regulatory requirements, and improved cyber hygiene
- **Pricing and Rate Changes**
  - Stabilization of rates
  - Impact of systemic risk management: Insurers focusing on managing systemic risk to limit aggregate exposure.

Cybersecurity Threat Landscape

- **Ransomware and Ransomware as a Service (RaaS)**
  - Continues to be a major threat
- **Business Email Compromise (BEC)**
  - Significant financial losses due to fraudulent wire transfers and other deceptive practices
  - FBI IC3 reported more than $2.9 billion in 2023
- **Data breaches and their impact**
  - High impact on sectors like healthcare and financial services due to the sensitive data they handle
  - Associated costs usually include notification expenses, legal fees, regulatory fines, and credit monitoring services for impacted consumers

Policy Features and Exclusions

- **Exclusionary Language**
  - Common exclusions: war, terrorism
  - Coverage for non-malicious events like human error

Regulatory and Industry Insights

- **Role of State Insurance Regulators**
  - Monitoring market trends
  - Ensuring policyholder protection
- **Industry Practices**
  - Underwriting improvements
  - Enhanced cybersecurity hygiene

Conclusion

- **Summary of Key Findings**
  - Market growth and stability
  - Importance of cyber insurance in risk management
- **Outlook**
  - Expected trends and challenges

Questions?

Please email khenry@naic.org if you have questions or concerns after this meeting adjourns