Cybersecurity (H) Working Group Update

Cynthia Amann, Chair of Working Group

Miguel Romero, NAIC Staff Support of Working Group

NAIC NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

Objective for 2024

Meet with subject matter experts to understand data and what the data says about cybersecurity and cyber insurance trends

NAIC NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

Richard Gibson–American Academy of Actuaries

- The Academy's Casualty Practice Council has a Committee on Cyber Risk that monitors the actuarial aspects of cyber risks.
- The Committee has created the Cyber Risk Toolkit, which includes papers addressing issues related to cyber risk insurance and cyber exposure.
  - This toolkit is intended to be a resource available for stakeholders to provide an overview of the challenges in the cyber insurance market, with periodic updates to reflect new and emerging issues.
- The Committee is currently working on a cyber vendor model review, to understand parameters and the output provided as well as an outline of cyber insurance and directors & officers coverage.

Mark Camillo and Monica Lindeen- CyberAcuView

- CyberAcuView was created by insurance industry leaders, to act as thought leader on issues surrounding cyber insurance.
- Their core activities include data aggregation, reporting and standards; systemic risk evaluation; regulatory collaboration; law enforcement coordination; and other priorities to improve market efficiencies.
- CyberAcuView shared the results of a data call focused on 2019-2023 third-quarter data.
  - Notably, its clients include approximately 60% of the cyber insurance market.
  - 30,000 claims have been submitted since 2019.
  - Approximately $4 billion in payments, more than half of the losses were

Stephen Viña- Office of the National Cyber Director

- ONCD developed the National Cybersecurity Strategy, representing a fundamental shift in rebalancing the responsibility to defend cyberspace and realigning incentives to favor long-term investments.
- ONCD and Treasury Department continue the study of a cyber insurance federal backstop.
  - Including responses to their 2023 request for input.
- ONCD has observed ransomware payments have become less common, but more severe.
  - Indicating threat actors are seeking larger payouts for their activities.
  - Ultimately, the federal government strongly discourages payments, to avoid encouraging continued activity by the threat actors.

Rebecca Bole and Jon Laux- CyberCube

- CyberCube seeks to provide analytics to quantify cyber risk and partners with insurance regulators, rating agencies, and government agencies to create frameworks for governance.
- Cyber risk data is abundant, everything digital is tracked in a way the physical world is not. Detailed analysis of information signals can indicate an organizations risk posture.
- Understanding an insurers use of data, level of testing, and adaptability to change are important criteria for underwriting maturity.
  - Organizations are using a combination of external and internal network scanning tools to inform decision-making.
  - Underwriting questionnaires should be used to fill in the gaps.
- Many carriers are seeking mitigation strategies via active risk monitoring.
  - Developing alerts and notifications to policy holders to improve resilience.

Sezaneh Seymour and Daniel Woods- Coalition

- Coalition, Inc., utilizes an active insurance model to approach the cybersecurity risk of their policyholders.
  - Data suggests their policyholders experienced 64% fewer claims than the market average.
  - Coalition has a team of security experts available to provide technical assistance throughout the lifecycle of the policy.
- Academic and industry research identify technical controls such as, patch cadence, multi-factor authentication, attack surface management, and boundary devices as the most important technical predictors of an organizations likelihood to suffer claims.
- Cyber insurance has become a market-based tool to drive security improvements across businesses and infrastructure.

Ignace Ertilus and Gregory Crabb- FBI/10-8, llc

- On July 9th, the Cybersecurity Working Group will hear a briefing from Ignace Ertilus of the FBI and Gregory Crabb of 10-8, LLC about the operations of the FBI IC3 division, their approach to cybersecurity incidents, and insights into threat-informed defense strategies.

What's Next

- As the Working Group reflects on insights gained throouhgout the year, the Working Group may:
  - Send referrals suggesting updates to Handbooks or related to other publications
  - Work with NAIC staff to develop additional training on the topics of cyber insurance and cybersecurity
  - Enhance the *Cybersecurity Event Response Plan (CERP)*

Questions?