Energy Cybersecurity Insurance Forum

In support of the *100-Day Plan to Address Cybersecurity Risks to the U.S. Electric System*

The Biden administration's 100-day plan to address cybersecurity risks to the U.S. Electric System includes a task to facilitate a forum to *explore and examine opportunities to incentivize participation in this Initiative and the adoption of industrial control system (ICS) cybersecurity monitoring technologies,* which includes the exploration of leveraging insurance products as incentive mechanisms. The Energy Cybersecurity Insurance Forum was held on July 7-8, 2021, to engage infrastructure and insurance stakeholders in discussions on the current state of insurance for ICS cyber risk in the electric sector, concepts for enhancing such coverages, and the potential for using insurance to incentivize investment in ICS cybersecurity. 397 people registered for the event. 270 attended day 1 and 198 attended day 2. This document provides a recap and key points from the event.

Keynote Session, July 7, 2021

Opening remarks from the Department of Energy and three keynotes framed the event and the problem space.

Speakers

- **Puesh Kumar,** Acting Principal Deputy Assistant Secretary (PDAS) for the US Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
- **Jim Trainor**, Senior Vice President, Aon Cyber Solutions
- **Constance H. Lau,** President and Chief Executive Officer, Hawaiian Electric Industries, Inc.
- **Rep. Jim Langevin**, Rhode Island 2nd Congressional District

Key takeaways

- The energy sector is integral to all other critical infrastructure sectors. We need better early detection of threats and shared situational awareness to address the risk.
- Government actions are needed to construct more consequences for cyber attackers, ensure the availability of capital for risk transfer options by evolving the Terrorism Risk Insurance Act (TRIA), and continued collaboration through information sharing.
- Insurance rates are rapidly increasing for property and cyber coverages. Cyber coverage for physical damage is needed, but its availability is limited. Broad war exclusion language also constrains property coverage.
- Cyber insurance policies are small-dollar and do not capture the enormous risks that underlie the disruption of critical infrastructure functions such as the generation and transmission of electric power. Cyber insurance will not help us recover from a widespread takedown of the grid, nor will it prevent it.
- The insurance industry can be instrumental in building a robust data sharing pipeline about cyber posture, threats, costs, and consequences.

Three Panel Sessions, July 8, 2021

Panel Session 1: How a government reinsurance program may incentivize insurance products for the energy sector
This panel explored the need for such a reinsurance program, explored what has or has not worked about TRIA, and shared perspectives on whether such a program would improve the availability of cyber coverage for electric infrastructure.

Panelists:

- **Tracie Grella**, Global Head of Cyber Risk Insurance at AIG
- **Bob Parisi**, Head of Cyber Solutions-North America at Munich Re (Group)
- **Robert Morgus**, Senior Director at Cyberspace Solarium Commission
- **Joe Meaney**, VP Global Insurance and Risk Engineering at AES
- **Phil Irwin**, President and CEO, Federated Rural Electric Insurance Exchange

Key takeaways:

- There was near unanimous consensus on the need to explore a government reinsurance program (an expansion or evolution of TRIA) to address catastrophic risks and excluded coverages such as state-actor infrastructure attacks.
- The insurance industry is committed to collaboration with the electricity sector to manage and transfer cyber risk.
- Cyber risk can be viewed in two buckets: "data and privacy" and "technology dependence". Technology

dependence is rapidly increasing and is where operational and infrastructure risk occurs, posing new challenges for the insurance industry.
- Cyber threats to electricity infrastructure exceed the resources of any one company. More offensive response or other consequences for adversaries from the federal government may be necessary to protect critical infrastructure.

Panel Session 2: The role of cyber statistics in cyber risk management, insurance products, and government policymaking
This panel addressed the need for cyber statistics to enable modeling of cyber risk, the potential and challenges for sourcing such data from cyber-related insurance claims, and the promise (or peril) of combining pre-loss posture data with cyber claims data to provide an evidence basis for the identification of critical cybersecurity controls.

Panelists:

- **Garin Pace**, Cyber Product Leader - Financial Lines & Property at AIG
- **Tom Johansmeyer**, Head of PCS at ISO Claims Analytics, a division of Verisk Insurance Solutions
- **Nick Leiserson**, Chief of Staff for Rep. Jim Langevin (D-RI-2)
- **Josephine Wolff**, Assistant Professor of Cybersecurity Policy at Tufts University - The Fletcher School of Law and Diplomacy

Key takeaways:

- There was strong consensus on the value of centralized, anonymized cyber statistics to enable better understanding of cyber risk, control effectiveness, and the availability of insurance capital for risk transfer.
- Total annual premiums for cyber insurance are ~$5 billion; 45% comes from companies with over $100 million in coverage. These amounts are quite small compared to other coverages, such as property insurance.
- Cyber statistics are needed to validate efficacy of cybersecurity controls and would facilitate frameworks that enable incentives for adoption of cybersecurity technologies and other controls.
- Pooling of cyber statistics, especially insurance claims data, would enhance understanding of the scope of cyber threats to the industry, help spur collective action among insurers, and provide an empirical basis for the creation of new policies.

Panel Session 3: Proposed insurance incentives to improve OT cybersecurity
This panel discussed what kinds of incentives are feasible in insurance coverages, how could the mechanics of such incentives be managed across the insurance industry, what are potential pitfalls, and which types of incentives would be most effective (e.g., coverage enhancements, limit expansions, or price relief)?

Panelists:

- **Patrick Thielen**, Senior Vice President, Financial Lines, Cyber at Chubb
- **Mike Kolodner**, US Power and Renewables Industry Practice Leader at Marsh Specialty
- **AJ Jacobs**, CISO at SMUD
- **Andrew J. Grotto**, Director, Stanford Program on Geopolitics, Technology and Governance, Stanford University

Key takeaways:

- Interconnectedness and reliance on shared technologies is increasing threats to the energy industry. Events are not as hypothetical now. Variability in outcomes of cyber events challenges the insurance industry's contributions.
- Energy industry adoption of new cyber technologies is out-pacing what the insurance industry can support.
- Possible insurance incentives for improving OT cybersecurity include providing premium discounts for participating in insurance-sponsored security assessments, supporting security certifications for critical infrastructure providers, and offering premium discounts for selecting and implementing tools endorsed by insurance carriers.
- Lack of demand for insurance products persists. The availability of insurance can help drive improved resiliency, but not if there isn't adequate demand.
- The increase in threats such as ransomware that cause first-party losses are transforming the way that insurance is perceived by front-line decision makers.