Draft: 4/2/24

Cybersecurity (H) Working Group
Phoenix, AZ
March 17, 2024

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Phoenix, AZ, March 17, 2024. The following Working Group members participated: Cynthia Amann, Chair, and Brad Gerling (MO); Michael Peterson, Vice Chair (VA); Chris Erwin (AR); Wanchin Chou (CT); Daniel Mathis (IA); Ryan Gillespie and Erica Weyhenmeyer (IL); Craig VanAalst (KS); Kory Boone (MD); Jeff Hayden (MI); T.J. Patton (MN); Colton Schulz (ND); Christian Citarella (NH); David Cassetty and Nick Stosic (NV); Avani Shah/Sumit Sud (NY); Matt Walsh (OH); John Haworth (WA); and Tim Cornelius and Rebecca Rebholz (WI). Also participating was: David Buono (PA).

1. Adopted its 2023 Fall National Meeting Minutes

Haworth made a motion, seconded by Peterson, to adopt the Working Group's Nov. 16, 2023, minutes. (*see NAIC Proceedings – Fall 2023, Cybersecurity Insurance (H) Working Group, Attachment Three*). The motion passed unanimously.

2. Adopted the Cybersecurity Event Response Plan (CERP)

Amann recognized Peterson for spearheading the Cybersecurity Event Response Plan (CERP) and Rabin for working with Peterson on the document. She said the CERP is intended to be guidance for departments of insurance (DOIs) when they must respond to a cybersecurity event. The plan will also help new DOI employees understand the response process. If a state has adopted its own version of the NAIC *Insurance Data Security Model Law* (#668), the information in the guidance will need to be updated to comply with the state's law. Additionally, states can change the document information to meet their needs. The document includes topics such as communication among various stakeholders, understanding and receiving notifications, required information that needs to be provided to a DOI, and a process that can be used to respond to cybersecurity events defined in the Model #668. The document also includes a sample template that can be used by a DOI when requesting information from the breached party. The Working Group worked closely with interested parties to incorporate their suggestions into the CERP. The document was exposed twice, and suggested changes were made where applicable.

Peterson made a motion, seconded by Haworth, to adopt the CERP (Attachment Two-A). The motion passed unanimously.

3. Heard a Presentation from the Academy on its Cyber-Risk Activities

Richard Gibson (American Academy of Actuaries—Academy) gave an informational presentation to the Working Group. The Academy is the only U.S.-based actuarial organization solely focused on serving the public and the entire actuarial profession. The Academy encompasses all practice areas and ensures the profession's ability to self-regulate by housing the actual board for counseling and disciplining, the joint committee on the code of professional conduct, and the committee on qualifications. Chou is the chairperson of the committee on cyber risk.

The Academy is engaged in public policy issues. The Academy's Casualty Practice Council (CPC) is the umbrella committee for major property/casualty (P/C) insurance issues. The CPC provides objective technical expertise to policymakers and regulators. The Academy does not work for insurers or regulators. The Academy has a committee on cyber risk that monitors the actual aspects of cyber risk. There are more than 20 members on this team, all of which are volunteers. A majority of the volunteers on the committee are working in cyber on a regular basis.

The Academy has been working on a cyber risk toolkit for the last three to four years and continues to update the toolkit on a regular basis. The toolkit includes papers that address issues pertinent to cyber risk and exposures that are now impacting most lines of business. Cyber exposure extends to many other coverages. Each part of the toolkit is a standalone paper, but it provides a cohesive overview of the challenges posed in the cyber insurance market. The cyber insurance market is constantly evolving with respect to new threats, new coverages, and new crises. The toolkit will be updated periodically to reflect new and emerging work from the Cyber Risk Committee.

The key papers within the Cyber Risk Toolkit include *An Introduction to Cyber*; *Cyber Threat Landscape*; *Silent Cyber*; *Cyber Data*; *Cyber Risk Accumulation*; *Cyber Risk Reinsurance Issues*; *Ransomware*; *War, Cyberterrorism, and Cyber Insurance*; *Autonomous Vehicles and Cyber Risk*; *Personal Cyber: An Intro to Risk Reduction and Mitigation Strategies*; *Digital Assets and Their Current Roles Within Cyber Crime*; and *Cyber Risk Resource Guide*.

The Cyber Risk Committee is currently in the process of a cyber vendor model review. While the committee is not able to review all of the existing cyber models, it is trying to get a sense of how cyber models are working and how they are evolving. The Academy is not endorsing models but trying to understand the parameters and the output they provide, as well as the model's usefulness.

The Cyber Risk Committee is also working on an outline for international cyber considerations and delving deeper into cyber personal lines insurance and the rating on the personal lines side of cyber insurance. An outline about cyber insurance and directors and officers (D&O) coverage is also in the works. In 2020, the Academy published a report on cyber breach reporting requirements, which provides an analysis of laws across the U.S. This document can be found on the Academy's website.

The Academy is working with a business school in Paris, France, to estimate the economic value of cyber risk. The methods being used consider both the heavy-tailed distribution of extreme events and the rapid changes in the underlying hazard. The hope is to get access to the Federal Bureau of Investigation's (FBI's) database on cyber events so work can move forward and be reproduced for the U.S. The Working Group will continue its interaction with the Academy.

4. Heard a Presentation from CyberAcuView About its Organization

Monica Lindeen (CyberAcuView) said the cyber-insurance market continues to mature. Following a health care data breach in 2015, the cyber-insurance market began to harden. In 2016 and 2017, a lot of new carriers entered the cyber-insurance market, and coverage began expanding. While 2018 and 2019 saw lower rates, ransomware severity increased.

CyberAcuView was created by insurance industry leaders, and the organization acts as a thought leader on issues surrounding cyber insurance. CyberAcuView was formed to help increase innovation and competition in the cyber-insurance market and to help combat the increasing threat of cyberattacks. Since CyberAcuView's establishment, it has been working to help insurers provide better value and service to its policyholders and their cyber-risk

mitigation. The organization also has been helping to provide leadership in fighting cybercrime to improve resilience to cyber risk, as well as helping to ensure a competitive cyber-insurance market. CyberAcuView believes the cyber-insurance market will continue to mature with access to experience data, stronger underwriting, capital market investments, the development of cyber definitions and standards, engagement with law enforcement, and collaboration of systemic resolutions that will benefit both the policyholders and society.

Mark Camillo (CyberAcuView) said the core reason for CyberAcuView being formed was data aggregation. There are currently more than 20 members that participate in CyberAcuView, which represents approximately 60% of the cyber-insurance market. However, not everyone in the market reports data. Prior to the formation of CyberAcuView, there was not a platform that insurers had to benchmark how they were performing against their peers and how their loss ratios were looking in various industries and segments. CyberAcuView began to collect and aggregate data. CyberAcuView's collection of the data and aggregation provides a benchmark to insurers. On a quarterly basis, claims data is aggregated, anonymized, and provided to CyberAcuView's members. To get data out of the pool, the insurer must provide data, as the data services are voluntary. CyberAcuView enables insurers to retain the value of their own data by being a statistical reporting agent. Statistical reporting services are available in all states, as required.

CyberAcuView is also working on cyber-data standards. It developed an incident response claims taxonomy for both cyber exposures and cyber claims data. CyberAcuView also publishes standards as an open cyber standard that is governed by CyberAcuView and can be accessed and used by all market participants. CyberAcuView has started collecting data in 2019 and has data through the end of the third quarter of 2023. Over 30,000 claims have come in since 2019, and a little over $4 billion in payments, with about $500 million in reserves. Less than one-third of the claims are for ransomware. However, more than half of those losses were actually caused or driven by ransomware. CyberAcuView collects the top ransomware variants in terms of ransomware claims. It also provides information about the industry groups and tracks the number of claims notices.

CyberAcuView runs quarterly workshops to stimulate discussion and help insurers develop a better understanding of events that drive systemic risk. They also discuss how insurers can help the areas of systemic risk, and how to help increase society's resilience to systemic cyber risk. Past workshops have focused on cloud failure and outages, issues confronting cyber insurance-linked securities (ILS)/alternative capital markets, systemic risk extensions that have been introduced in the marketplace, and cyber risk modeling considerations.

Lindeen leads the efforts on regulatory collaboration, acting as a resource for organizations.

Camillo addressed the potential federal cyber backstop. CyberAcuView will continue to evaluate the potential of a federal cyber backstop.

CyberAcuView has a head of law enforcement engagement that works closely with the FBI through its public/private partnership with the National Cyber-Forensics and Training Alliance (NCFTA). The group is developing a pilot program to actively disrupt and seize ransomware payments by coordinating with other technology companies.

CyberAcuView developed a policy form that can be used by market participants to define risks more precisely, remove ambiguities, and attract more capacity into the market. The cyber war exclusion language was accepted and posted to the Legal Marketing Association (LMA) website. Several insurers are currently going through the process of updating their war language and using the CyberAcuView war exclusion language as a template.

CyberAcuView has endorsed the Cybersecurity and Infrastructure Security Agency's (CISA's) bad practices list as a voluntary minimum cybersecurity best practice to improve policyholder security maturity. It also has expanded outside of the U.S., with its first international data call in the United Kingdom (UK) and Canada.

CyberAcuView collaborated with Pan-European Insurance Risks Information System (PERILS) in Europe to create a U.S. cyber loss index to help accelerate the growth of the cyber ILS and industry loss warranty (ILW) markets. PERILS does work similar to CyberAcuView for the European market on the natural catastrophe side.

The only 2023 event CyberAcuView continues to track is the MOVEit vulnerability. Based on the data they were able to gather and collect in the first quarter of 2024, the losses are below the $500 million reporting threshold. CyberAcuView will continue to monitor to see if the cost rises above the threshold. The methodology can be found by visiting https://cyber.perils.org/#methodology.

5. Discussed the Working Group's Work Plan

The Working Group will look at the current *Cybersecurity Supplement* to see what other information might be advantageous to collect. The Working Group also will discuss some of the following issues in the next year:

- The impact of both hardware and software legacy systems.
- Reviewing the European Union's (EU's) recent Artificial Intelligence Act to the extent that it impacts cyber.
- Data modernization and standardization.
- Third-party vendor oversight.
- Educating its fellow regulators and the insurance industry.
- The knowledge among regulators regarding cyber is disparate, so the Working Group will make sure information is being brought to it from experts.
- Two panels at the Insurance Summit.
- One-to-many reporting.
- Ensuring that both small and large businesses are aware of what their cyber coverage actually covers.
- Working with the Information Technology (IT) Examination (E) Working Group.
- Tracking Model #668 adoptions, as well as changes by the states adopting the model law.
- Panels with an insurer, broker, and reinsurer.
- Hearing from the Center for Insurance Policy and Research (CIPR).
- Hearing from CyberCube.

Peterson is a member of the Financial Stability Board (FSB) for discussions about cybersecurity event notifications standardization.

6. Discussed Other Matters

Amann reminded the Working Group of the Working Group's call on March 27.

Having no further business, the Cybersecurity (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_Spring/WG-Cybersecurity/Minutes-CyberWG031724-Final.docx

