Draft: 8/5/25

Cybersecurity (H) Working Group
Virtual Meeting
July 15, 2025

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met July 15, 2025. The following Working Group members participated: Michael Peterson, Chair (VA); Julia Jette (AK); Leo Liu (AR); Bud Leiner (AZ); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Elizabeth Nunes and Matt Kilgallen (GA); Lance Hirano (HI); Daniel Mathis and Travis Grassel (IA); C.J. Metcalf (IL); Shane Mead (KS); Nina Hunter (LA); Mary Kwei (MD); Jeff Hayden (MI); Bubba Aguirre and T.J. Patton (MN); Kim Dobbs (MO); Troy Smith (MT); Tracy Biehn (NC); Martin Swanson (NE); Christian Citarella (NH); Ned Gaines (NV); Gille Ann Rabbin (NY); Matt Walsh and Don Layson (OH); David Buono (PA); Bryon Welch and John Haworth (WA); Rebecca Rebholz (WI); and Lela D. Ladd (WY).

1. Discussed the Chief Financial Regulator Forum Referral Response

Peterson opened the meeting by introducing the *Insurance Data Security Model Law* (#668) compliance and enforcement guide, which was drafted as a response to the referral received from the Chief Financial Regulator Forum. The referral asked the Working Group to consider and provide further information on the regulatory compliance and enforcement of Model #668. This effort aimed to eliminate duplicative work across departments of insurance (DOIs) and provide a method for foreign departments to gain assurance that the domestic regulator is adequately enforcing the model law. He explained that the guide offers a method for a gap analysis between Model #668 and another standard, like Exhibit C or another state's adopted version of Model #668. Peterson encouraged confidential state-to-state collaboration to ensure efforts are properly aligned and comparable.

Peterson stated the documents would be shared for a public comment period and expressed appreciation for the states that participated in the drafting group. The goal of the guide and the public comment period is to create a seamless regulatory environment where the domestic regulator is trusted to fulfil the role of primary regulator. He recognized a lack of an accreditation process for reviews of Model #668 compliance, so it is necessary to perform a gap analysis after assembling all relevant documents. He stated that the most efficient way of communicating compliance with a state's adopted version of Model #668 would be through Section 4(I) or the Certificate of Compliance. While this could be satisfactory for representing compliance, only a gap analysis could definitively confirm.

Peterson explained that the broader effort is to support regulatory convergence and alignment. The Model #668 compliance and enforcement guide follows in the footsteps of the Cybersecurity Event Response Plan (CERP) in helping states provide a predictable regulatory environment, even in an unpredictable space like cybersecurity. He reminded the Working Group that the portal project being designed for everyone's review is another major part of the broader effort. Its successful implementation promises to relieve substantial regulatory risk from regulated entities by improving the ease of compliance.

2. Heard a Presentation from Coalition on Scattered Spider

Peterson said that in light of recent cybersecurity incidents observed across the country, Coalition offered to provide a briefing tailored to the insurance industry. He said Joe Toomey (Coalition) serves as Coalition's head of security engineering and has a vast background in cybersecurity and protecting organizations' most sensitive systems.

 

Toomey introduced the presentation topic, Scattered Spider, as a fluid collective of young, native-English-speaking, online threat actors. He said these 15–17-year-old hackers are unique and troublesome, but they are not usually well-funded; however, because they are native English speakers, their social engineering skills are strong. He said they are motivated by money and notoriety, and they target well-known Fortune 500 companies, deploying double extortion models meant to exfiltrate data and then encrypt systems with ransomware. He said the group often receives ransom payments and then threatens to release the exfiltrated data if an additional payment is not received to ensure compliance.

Toomey explained that Scattered Spider, as a collective organization, tends to act as an initial access broker to breach networks, selling network access to other criminal groups while operating online forums. He said most groups today are not developing their own ransomware because it is too expensive to develop internally. Scattered Spider first grew in notoriety around 2023 when it attacked MGM Resorts International and Caesars Entertainment, leveraging Subscriber Identity Module (SIM) swapping. Scattered Spider called the phone company and assumed the identity of the victim customer to bypass account security. Toomey described the progression in targeting. He said that from the attacks on Snowflake customers, Scattered Spider discovered the lack of multi-factor authentication (MFA) across customer accounts and targeted hundreds of companies in 2024. Now, Snowflake always requires MFA across all accounts. He explained that starting in April 2025, the group began targeting retail companies like Harrods and supply distributor Peter Green Chilled before targeting U.S. insurance carriers in June.

Toomey explained that the Erie Insurance and Philadelphia Insurance Companies attacks compromised millions of policyholder records while halting new policy underwriting and digital claims processing for a period. The targeting of insurance providers is not unique to Scattered Spider; other groups like the Russia-based Conti ransomware group have found insurers to be good targets because they pay.

Toomey transitioned to explain the more technical portion of the presentation. He said the tools, techniques, and procedures are how cybersecurity personnel learn to detect and prevent attacks by certain threat actors. He described how Scattered Spider employs the art of deception to facilitate initial access. Toomey said the group uses reconnaissance and open-source information to gather names, titles, and personal details to make impersonation attempts, such as phishing and voice calls, to target employees and information technology (IT) help desks. The core tactic in help desk exploitation is convincing help desk staff to reset passwords and enroll new MFA devices, effectively bypassing security controls. Toomey described a similar tactic in which the group "push bomb" users with repeated MFA notifications, hoping for an accidental approval.

Toomey said threat intelligence suggests that Scattered Spider exfiltrates and then encrypts target systems using legitimate tools and partnerships with ransomware organizations like BlackCat, also known as ALPHV. He offered guidance for hardening, including the mandate of robust, out-of-band identity verification for all MFA resets, training employees, and reinforcing technical defenses with immutable backups and response plans that have been tested.

Toomey said Coalition's research also supported implementing IT security awareness training that specifically simulates the various forms of phishing campaigns. He also encouraged organizations to scrutinize the supply chain by vigorously assessing the security of third-party vendors and managed service providers (MSPs), as they are a primary vector of entry for these attacks. He stated that the basic information security hygiene items, like patching critical systems, reducing attack surface, and network segmentations, are critical and often overlooked.

Peterson thanked Toomey for his insightful and timely presentation on the evolving threat landscape posed by groups like Scattered Spider. He acknowledged the importance of continued vigilance and collaboration across the industry in response to these cyber threats.

 

Peterson extended his appreciation to the attendees for their time and engagement and reminded the Working Group that the next opportunity to continue this discussion will be during the Working Group's session at the Summer National Meeting.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2025_Summer/WG-Cybersecurity/Minutes-CyberWG071525.docx

 

Draft: 03/31/25

Cybersecurity (H) Working Group
Virtual Meeting
March 13, 2025

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met March 13, 2025. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair (VA); Sian Ng-Ashcraft (AK); Chris Erwin (AR); Bud Leiner and Alena Caravetta (AZ); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Elizabeth Nunes and Matt Kilgallen (GA); Lance Hirano (HI); Daniel Mathis and Travis Grassel (IA); C.J. Metcalf and KC Stralka (IL); Shane Mead (KS); Mary Kwei and Kory Boone (MD); Jeff Hayden (MI); Bubba Aguirre and T.J. Patton (MN); Troy Smith (MT); Tracy Biehn (NC); Jon Godfread and Colton Schulz (ND); Christian Citarella (NH); Nick Stosic (NV); Gille Ann Rabbin (NY); Matt Walsh (OH); Sebastian Conforto (PA); John Haworth (WA); Andrea Davenport (WI); and Lela D. Ladd (WY).

1. Discussed the 2025 Cyber Work Plan

In lieu of meeting at the Spring National Meeting, the Working Group chairs facilitated an opportunity to review the key initiatives planned for the year and a chance for members and interested parties to contribute to the plan. Amann summarized the work accomplished in 2024 as excellent, drawing attention to the two streams under the Working Group's purview by engaging with both cybersecurity and cyber insurance subject matter experts to provide foundational education and awareness for state insurance regulators. The intent for 2025 is to further build the knowledge base and continue to be aware of important market trends as well as technological developments to keep fellow regulators informed of all that is developing.

Amann introduced the first initiative as the cyber data wish list for both cybersecurity and cyber insurance. Expounding on a quote from Commissioner Jon Godfread (ND), she said that bad policy comes from bad data, adding that both cybersecurity and cyber insurance have a similar problem. The data may not be necessarily bad but is often not understood. Ensuring the two tracks remain in front of mind, Amann opined that this effort would require work with groups who have similar mandates. The Working Group leadership engaged in preliminary discussions with Christian Citarella (NH), Chair of the NAIC's Casualty Actuarial and Statistical (C) Task Force and Sandra Darby (ME). The development of a regulator data wish list could enhance the current cyber blank as well as the cyber insurance report published annually by the NAIC. One goal for the first half of 2025 will be to coordinate a presentation from AM Best to cover its recent survey report, which included additional data on the cyber insurance marketplace. Amann expressed interest in public input on other presenters in the same vein, where data is collected and used in ways that can help drive the conversation further.

Chou reminded the group of the ongoing work at the American Academy of Actuaries (Academy), to collect and review some of the cyber modelling data as well as the definitions being used. Chou offered to provide an update when applicable and expressed willingness to invite them to talk about cyber data, its quality, and where it is sourced from.

Amann introduced the cybersecurity event notification portal as the second initiative, reminding the Working Group of the motion made during the 2024 Fall National Meeting. The motion, which is to work with NAIC staff to explore the feasibility of creating a centralized portal to receive cybersecurity incident notifications at the NAIC, is aimed at streamlining the reporting process when companies experience a cybersecurity incident. Amann provided a short update, informing the group that NAIC staff had issued a survey to regulators and once complete, the analysis will ignite healthy discussion on the needs for the portal.

 

Peterson explained that this project is a source of potential synergy and efficiency, to reduce costs and improve the licensee experience. The survey asked important questions about how the portal should be structured and the collective need in the industry and will help to ensure the project has a focused approach.

Amann described the cybersecurity tabletop exercises, which started at the NAIC several years prior with the help of the U.S. Department of the Treasury. She explained that during these events, regulators of a host state meet with regulated companies, law enforcement officials, as well as NAIC staff to talk or walk through a cybersecurity scenario with active participation from all involved to explain how they would react during a real-life situation. Amann suggested the exercises could be facilitated in a virtual or in-person setting, using interest from the Working Group as a gauge to determine which format is best. Schulz said that North Dakota would be interested in being a host state.

Amann reminded the members of the referral received from the Chief Financial Regulator Forum, which asks the Working Group to weigh in on whether there is a way to improve compliance questions and recording procedures related to the *Insurance Data Security Model Law* (MDL #668). She explained that given the very detailed information technology (IT) reviews during financial examinations, brainstorming has led to robust discussions, and a draft response will be circulated to receive input later this year. Peterson reiterated that the open question nature of the referral is an opportunity to develop a framework that ensures alignment, reducing the risk of duplicative efforts, and offers guidance that utilizes existing work that is done by the IT review function for financial condition examination. He said one of the important considerations to keep in mind is that this process has to make sure that risks are being identified and investigated but not investigating a risk that had already been looked at through a perfectly reasonable lens.

Mead and Amann provided a short update on the Information Technology (IT) Examination (E) Working Group's review of the IT general controls and exhibit C for cybersecurity maturity evaluation considerations. The drafting group will continue to meet and discuss to determine the most appropriate and logical approach, which could be a cyber handbook or a best practices framework

Amann discussed future meetings in 2025, which will include, presentations on cybersecurity trends as well as an opportunity to hear from fellow regulators about the state of New York and its cyber regulation update.

Stephen Packard (Unaffiliated), Amann, and Peterson discussed cyber insurance, the ransomware problem, and effective loss controls.

Chou supported the work plan's inclusion of education and awareness, describing it as important because of the different experiences each person brings to the table.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2025_Spring/WG-Cybersecurity/Minutes-CyberWG031325.docx

 