Attachment A
Cybersecurity (H) Working Group
8/14/24

8/1/24

Cybersecurity (H) Working Group
Virtual Meeting
July 9, 2024

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met July 9, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair (VA); Julia Jette (AK): Mel Anderson (AR); Damon Diederich (CA); Wanchin Chou (CT); Daniel Mathis (IA C.J. Metcalf (IL); Shane Mead (KS); Mary Kwei (MD); Jake Martin (MI); T.J. Patton (MN); Tracy Biehn (NC); Colto Schulz (ND); Gille Ann Rabbin (NY); Don Layson (OH); Jodi Frantz (PA); Andrea Davenport (WI); and Lela Ladd (W

1. Adopted its May 20, March 27, and Spring National Meeting Minutes

The Working Group met May 20 and took the following action: 1) received an update on the Cybersecurity Event Response Plan (CERP); and 2) heard a presentation from CyberCube on cyber risk. The Working Group also me March 27 to hear an update from the White House Office of the National Cyber Director (ONCD) related to cybersecurity and cyber insurance.

Schulz made a motion, seconded by Peterson, to adopt the Working Group's May 20 (Attachment), March 27 (Attachment), and March 17 (see NAIC Proceedings – Spring 2024, Innovation, Cybersecurity, and Technology (H) Committee, Attachment Two) minutes). The motion passed unanimously.

2. Heard a Presentation from the FBI and 108 LLC on Their Approach to Cybersecurity Incidents

Ignace Ertilus (Federal Bureau of Investigation—FBI) said the presentation title, "Changing Landscape", was chosen because cyber is always changing. Just when a threat such as fraud and phishing feels handled, a new ¾;r³»º¾_¼£¸â /n_ Âûb»¾•À6hPÐ L “ £0} 3 D`Ð , ¡ ‡ã 8¦Xq áAvð 9v !}4#ãçš#¢‘ email compromise—a Áš#ó investment scams, and tech support. Ertilus said these four types of attacks accounted for the largest losses associated with reporting to the FBI's Internet Crime Complaint Center (IC3).

Ertilus said that ransomware is a f(o)4.2 (mr)]TJ </MCID 27.87 83 87 83 are exploiting some key

execute ransomware files. Companies have to think about what those

structure. In 2023, the FBI's IC3 received more than 2,800 complaints

osses of approximately $60 million. Separate studies have shown 50

–

80% of victims that paid the ransom experienced a repeat ransomware attack by either the same or different actors. Ertilus discussed multiple defensive best practices, including regular data backup and integrity verification, regular scans, application whitelisting, and physical and logical separation of networks. Another defensive best practice is providing awareness and training, such as teaching people within the company not to click on everything sent to them.

Ertilus said that business email compromise or account compromise is one of the most financially damaging online crimes. It exploits the fact that so many people rely on email to conduct both personal and professional business. These sophisticated scams are carried out by fraudsters compromising email accounts to conduct unauthorized transfer of funds. In a business email compromise (BEC)