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); Colton Schulz (ND); Gille Ann Rabbin (NY); Don Layson (OH); Jodi Frantz (PA); Andrea Davenport (WI); and Lela Ladd (WY).

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 met 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 10-8 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 technology comes about like artificial intelligence (AI) and completely changes the threat landscape. Cyber actors categorically fall into six definitions: 1) hacktivism; 2) crime; 3) insider; 4) espionage; 5) terrorism; and 6) warfare. Historically, there was a clear distinction between the different cyber actors. Now there appears to be more of a blend. North Korea has nation-state actors, but a lot of reporting out on North Korea suggests more actors' involvement with ransomware. This is where the actors can make money for the regime and is an example of where a nation-state actor can fit into multiple categories. The crime category actors are typically after personally identifiable information (PII), which can be used to sell on websites for others to commit tax fraud or identify theft.

Of the various types of attacks, the presentation focused on ransomware, business e-mail compromise, 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 form of malware that encrypts files on a victim's computer or server. Ransomware has been around for quite some time, but around 2018, its frequency increased. Expected targets of ransomware include state and local governments and industries that need immediate access to their data, such as the health care industry. Ransomware is a tool that cyber actors use, but they are exploiting some key vulnerabilities in systems to be able to execute ransomware files. Companies have to think about what those vulnerabilities could be for their own infrastructure. In 2023, the FBI's IC3 received more than 2,800 complaints identified as ransomware with adjusted losses 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 e-mail 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) scam, criminals send an email message appearing to come from a known source making a legitimate request, such as a company CEO asking an assistant to make a quick purchase or wire transfer. Common preventative measures include using multifactor authentication (MFA) and reviewing hyperlinks for misspellings or domain names for typos. Some companies implement multi-tier authentication for fund transfers to avoid a single point of failure in their security.

Ertilus said that investment scams are the largest cause of loss of any crime type tracked by IC3. These deceptive practices induce investors to make purchases based on false information. Investment fraud rose 38% in 2023 to $4.57 billion. Investment fraud with reference to cryptocurrencies rose from $2.57 billion in 2022 to $3.96 billion in 2023, an increase of 53%. These scams can start with a simple text message from an unknown source, designed to entice targets with the promise of lucrative returns on their investments.

Cyberthreat actors are increasingly using tech support and government impersonation avenues to target victims. In order to increase the possibility of success, threat actors introduce a sense of urgency or fear. Two examples are: 1) claiming the victim has a critical error with their computer, requiring immediate attention; or 2) alleging the victim missed jury duty in a message appearing to come from the local sheriff. In such instances, victims are inclined to the respond to avoid future issues.

Gregory Crabb (10-8 LLC) discussed the company's "Mastering the Six Steps to Effective Threat Intelligence" program. The approach integrates threat intelligence into security strategy and focuses on understanding and countering an adversaries' tactics, techniques, and procedures. The six steps are: 1) identify and understand the threats; 2) define intelligence needs; 3) prioritize assets and services; 4) collect and analyze information; 5) make informed decisions and communicate effectively; and 6) continuously improve the threat intelligence program.

Crabb said the benefits of this six-step cybersecurity approach are observable in the organization being ready, responsive, and resilient. Using the six steps empowers an organization to effectively anticipate and counteract cyberthreats.

Chou requested additional information regarding the 10-8 cyber arena offering, expressing interest in the opportunity.

Miguel Romero (NAIC) reminded the Working Group of its work plan for the year. He said the Working Group plans to meet with experts and understand their perspectives to shape policy discussions, as well as hear presentations on federal updates and from AM Best.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_Summer/WG-Cybersecurity/Minutes-CyberWG070924.docx