Attachment 1
Cybersecurity (H) Working Group
10/30/24

Draft: 10/28/24

Cybersecurity (H) Working Group
Virtual Meeting
October 8, 2024

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met Oct. 8, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair (VA); Julia Jette (AK); Leo Liu (AR); Bud Leiner (AZ); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Matt Kilgallen (GA); Daniel Mathis (IA); C.J. Metcalf (IL); Shane Mead (KS); Mary Kwei (MD); Jeff Hayden (MI); Troy Smith (MT): Tracy Biehn (NC); Colton Schulz (ND); Christian Citarella (NH); Scott Kipper (NV); Gille Ann Rabbin (NY); Don Layson (OH); David Buono (PA); Andrea Davenport (WI); and Lela Ladd (WY).

1. Adopted Its Sept. 4 Minutes

The Working Group met Sept. 4 and took the following action: 1) heard a presentation from AM Best on the cyber insurance market, which assigned a stable outlook on the global cyber insurance market.

Schulz made a motion, seconded by Buono, to adopt the Working Group's Sept. 4 (Attachment XX) minutes. The motion passed unanimously.

2. Heard a Presentation from the FBI Internet Crime Complaint Center (IC3)

Rachel Yurkovich (Federal Bureau of Investigation—FBI) introduced the IC3 program and discussed its inclusion in the Cyber Division and the Criminal Investigation Division of the FBI and how those roles intersect. She explained how the FBI's mission priorities have increasingly focused on cyber threats, including ransomware, intrusions, and tracking cyber adversaries. IC3 provides a central reporting mechanism for the public and the FBI regarding cyber intrusions and scams. For law enforcement, it provides remote access to a database of complaints received since 2000. Its website (ic3.gov) offers public service announcements, consumer alerts, and annual reports. Yurkovich described the IC3 partnerships with private sector entities and various government agencies at all levels.

Yurkovich explained that nearly every complaint received by IC3 is reviewed, confirming crime types, loss reporting, and adjusting where necessary in the case of fraud scams. The organization receives an average of 2,900 complaints a day. She described the increasing trend of extortion emails, which include pictures scraped from Google Maps, suggesting that the scammer has proof of the victim in a compromising act and/or visiting bad websites, and the scammer demands payment in Bitcoin. In addition to complaint processing, the IC3 provides case support, complaint aggregation, and reporting, as well as call centers supporting fraud claims. 2024 has already exceeded the $12.5 billion dollars of loss reported in the year 2023. Yurkovich described how the number of complaints received seemingly averaged while the losses significantly increased over the last five years. She stated that losses reported often do not include the cost of recovery, such as a business or an individual having to start over.

Introducing the term "pig butchering," Yurkovich explained it is a type of crypto-based confidence investment fraud where a victim meets someone online and builds a relationship with them. She clarified that the relationship does not necessarily have to be romantic; it could be a professional relationship stemming from a LinkedIn connection, for example. Eventually, the scam artist, turned friend, convinces the victim to invest in crypto. This type of fraud usually develops over a period of a month. The victims start by investing a little bit at a time, and the fraudster portrays positive earnings and might even allow a small payout in order to build trust. Yurkovich said at some point in time, the victim attempts to collect, and that is when the veil is lifted. They realize everything is gone. Reporting victims come from all age ranges. However, 30- to 49-year-olds have been the most impacted, and devastatingly, some of these victims lose their entire savings and retirements to these scams.

Discussing major cyber threats observed by the IC3, Yurkovich stated they received 1,193 complaints from organizations belonging to a critical infrastructure sector that were affected by a ransomware attack in 2023. Of the 16 critical infrastructure sectors, IC3 reporting indicated 14 had at least one member that fell victim to ransomware last year. The most targeted sectors were 1) healthcare and public health, 2) critical manufacturing, and 3) government facilities. IC3 typically receives ransomware complaints from victims after systems have been infected but prior to a ransom being paid. The FBI does not encourage ransom payments but realizes businesses have an obligation to get their systems back up and running as soon as possible.

Tom Wetzel (Wetzel and Associates) asked if there was any uptick in crime observed in the wake of any natural catastrophes. Yurkovich explained there is always an uptick, especially charity fraud, with people posing as legit charities to elicit monetary donations.

Smith asked for an explanation of “advance fee and overpayment” as labeled on a graphic of reported crime categories. Yurkovich said some people are applying for government grants or loans online, and they are given upfront fees and taxes to be paid ahead of time to get the funds. It is a common weak point in the industry, and fraudsters know it, so they take advantage of it, accepting the upfront payments and disappearing. Conversely, overpayment and non-delivery fraud seek to send “extra” money in hopes of collecting. Yurkovich gave the example of someone selling an item on eBay for $500. The fraudster purchases the item but sends a check for $2,000 with instructions for the seller to give the $1,500 of overpayment funds to the person picking up said item. Once complete, the check bounces, and the seller turned victim is out $2,000, their item, and whatever fees are demanded by their bank.

Diederich asked whether ransomware is primarily targeting financial gain or if the exfiltration of information is the underlying objective of the intrusion. Yurkovich expounded on the topic of ransomware trends, specifically explaining the double extortion tactic where the ransomware groups lock down or encrypt files while simultaneously exporting and storing them. They then demand a ransom, and if the company pays, they unlock the files. Having stored the data, the group comes back to the victim company a few months later, demanding a ransom or the data will be released on the web. Yurkovich observed a growing trend of multiple groups, especially more prominent groups, targeting the same victim with different types of ransomware variants.

Yurkovich explained how business email compromise is a type of scam carried out by a subject compromising legitimate business or personal email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds. Either through monitoring active email traffic or reviewing past requests, they identify who is allowed to approve payments and who is allowed to request payments be sent somewhere different. Yurkovich suggested only after extensive research or the use of tools, the subjects formulate emails impersonating the appropriate individuals to request payment reroutes. 2024 has seen an increase in business email compromise targeting the real estate sector, with cyber criminals portraying the real estate agency to reroute down payment wires.

Debra Decker (Stimson Center) asked what the benefits of reporting to the FBI are for businesses and the public, across all crimes and ransomware cases. Reiterating that reporting to IC3 is voluntary, Yurkovich explained that increased awareness of reporting could help the FBI understand and track the trends of reported crimes. Observing an aggregated condition, such as a specific area reporting real estate-related activity, allows the FBI to redirect resources and allocate case agents effectively.

In 2018, the IC3 started the recovery asset team, which is specifically for business email compromise scams. However, Yurkovich explained they have expanded to include any crime type reported as a complaint to the IC3. She added that if the complaint is submitted within 10 days of a wire or an ACH transfer and meets certain thresholds, the recovery team can assist in recalling the funds for the victim. In 2023, they reported a 71% success rate, recovering $538 million for more than 3,000 incidents.

Yurkovich explained the IC3 partners with U.S. government agencies, foreign law enforcement, as well as private sector organizations, such as the National Cyber-Forensics and Training Alliance (NCFTA). She also provided reporting resources:

- Internet Crime Complaint Center
  - www.ic3.gov
- National Threat Operations Center
  - www.tips.fbi.gov
  - 1-800-CALL-FBI (225-5324)
- National Elder Fraud Hotline
  - 833-372-8311

Chou asked how the American Academy of Actuaries (Academy) could get access to the IC3 data-sharing protocols. Yurkovich explained that the remote query-sharing program is temporarily paused for organizations outside of sworn law enforcement. IC3 is conducting an internal review and overhaul of the remote query access to ensure maximal security for victim information.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_Fall/WG-Cybersecurity/2024 1008Interim-Meeting/Minutes-CyberWG100824.docx