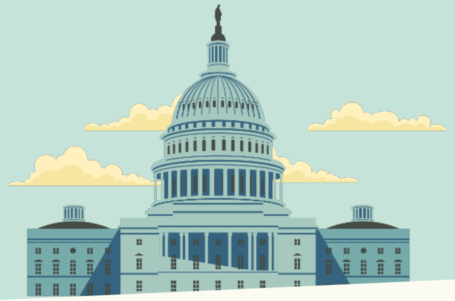


NEMA 2024 Mid-Year Forum | Washington, D.C.

NEMA Mid-Year Forum Tabletop Exercise

Private Sector Committee March 20, 2024

50 1974 · 2024 NEMA®

Scenario

January 31, 2024

- (CISA/FBI Congressional Testimony) Cybersecurity and Infrastructure Security Agency (CISA) Director Easterly and FBI Director Wray deliver a joint message to the Congressional Committee: “China’s hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities, if or when China decides the time has come to strike,”

February 7, 2024

- (Joint Cybersecurity Advisory) The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) assess that People’s Republic of China (PRC) state-sponsored cyber actors are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States.

- CISA, NSA, FBI are releasing an advisory to warn critical infrastructure organizations about this assessment, which is based on observations from the U.S. authoring agencies’ incident response activities at critical infrastructure organizations compromised by the PRC state-sponsored cyber group known as Volt Typhoon (also known as Vanguard Panda, BRONZE SILHOUETTE, Dev-0391, UNC3236, Voltzite, and Insidious Taurus).

Scenario Cont…

Wednesday, March 13, 2024

- (Phishing Email) An email appearing to come from a non-governmental organization requesting to add mission ready packages for aviation/airport support during severe weather emergencies into the Emergency Management Assistance Compact (EMAC) system. The email includes a list of resources via an attached .pdf file as well as a hyperlink for the same information.

Friday, March 15, 2024 - Morning

- (Winter Weather Advisory) The National Weather Service issues a winter weather advisory covering your community. Conference calls between state and county emergency management agencies with the local weather office help to facilitate the decision to open cold weather and functional needs shelters in many communities.

- (IPAWS Spoof) Several communities receive an earthquake warning via Wireless Emergency Alert (mobile device system) and local media urging residents to seek shelter.

- (EMAC Server Down) Later in the morning, the EMAC system goes offline.

Scenario Cont…

Saturday, March 16, 2024

- (Electric Utility Issues) The electric utility begins to experience "unexplained" fluctuations in output at various substations causing surges and temporary power losses.

Sunday, March 17, 2024

- (Water Pressure Alert) A system alarm alerts facility operators of a decrease in water pressure below 20 psi. Technicians attempting to access the malfunctioning ICS/SCADA devices notice administrative account credentials were changed without their knowledge, inhibiting their access to the devices. During physical inspection of the failed components, technicians discover there is no physical reason for the failure. Officials within affected communities decide to disseminate a boil water notice.

Sunday, March 17, 2024

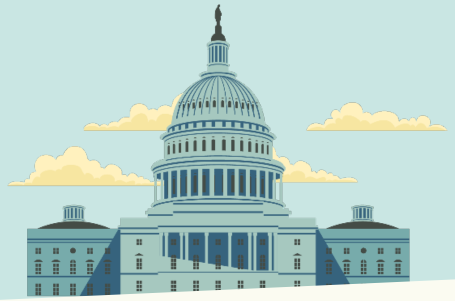
- Emergency managers attempt to disseminate the boil water notice through an IPAWs message via all alert sources without success.

Discussion Questions

1. How is cybersecurity information disseminated within your organization?

2. With basic public alert systems inoperative, discuss how you would communicate warnings or alerts within your organization and to your community?

   a. What would you consider to be an immediate priority?
   b. What are the contingencies listed in your Emergency Operations Plan/Cyber Incident Response Plan?
   c. Describe your Emergency Communications Plan and include your Primary, Alternate, Contingency and Emergency (PACE) considerations for notifications.



Discussion Questions Cont…

3. Discuss any mechanism your community has to request mutual aid via EMAC if your state cannot access the network.

4. Discuss any communications tools that could be enabled by the private sector to help facilitate disseminating emergency messages to the public.

Special Thanks to the team at CISA

- Robert Nadeau
- John French
- Joseph Larkin
- Rahul Mittal
- Benjamin Gilbert
- Joseph Kluczynski
- Monica Balzano
- Thomas Seo
- Michael Miller
- Louis Ritter