Cyber Security Forum Initiative (CSFI)

www.csfi.us

Cyber Exercise in Spain

CSFI's Mission

To provide Cyber Warfare awareness, guidance, and security solutions through collaboration, education, volunteer work, and training to assist the US Government, US Military, Commercial Interests, and International Partners.

What Makes CSFI Different

Our collaboration efforts have helped to break down stovepipes and "closed networks" that exists inside government and industry to enable greater information sharing and increased capabilities. 3 main pillars supporting CSFI's mission: Collaboration, Knowledge-Sharing, and Training/Education.

Purpose of CSFI Cyber Tabletop Exercise

The purpose of the Cyber Tabletop Exercise is to highlight the need for leveraging relationships and fostering collaboration to strengthen the cyber security posture of the international community. The lessons learned from this tabletop exercise will be applied by the cyber security community in an effort to create and change policies.

CSFI Exercise in Spain

Using the CSFI cyber tabletop format, the purpose of this exercise is to explore new cyber confrontation scenarios that pertain specifically to the Spanish cyber context. The result will be put together in the form of a brief and will be presented to Spanish officials dealing with the vulnerabilities and risks addressed in the scenario. The completed scenarios will later be presented to the CSFI participants and invited guests from the Spanish government.

CSFI's Proprietary Cyber *Tabletop* Format

CSFI Tabletop exercises are designed to simulate realistic theoretical cyber scenarios and incidents. These scenarios are not limited to strictly cyber vector scenarios; they can also include, but are not limited to: physical vulnerabilities in critical infrastructure, the role of partnerships, and the relationship between the government and its citizens during a cyber incident. CSFI stays true to its mission and values the participation of people from different backgrounds in efforts to bring something unique to the table. The CSFI tabletop format is flexible and can be conducted in compressed-time format as well as across several time zones.

Scenario Examples
A: Attack on a critical infrastructure (refinery, public transport, water supply)
B: The relationship between the government and the media during a cyber incident

Who should participate?
Anyone interested in cyber security and contributing to a safer cyber environment.

Contact: If you are interested in the exercise or would like to know more about it, get in touch with CSFI's Communications and Outreach Coordinator for Europe Dr. Lydia Kostopoulos: Lydia.K@csfi.us

Dr. Lydia Kostopoulos