



Robert Barreras, Jr.
County of San Diego
Office of Emergency Services
San Diego, CA

Sharing Information
Enhancing Preparedness
Strengthening Homeland Security

**Lessons Learned
Information Sharing**

INNOVATIVE PRACTICE

County of San Diego Cyber Disruption Response Team

May 16, 2016

SUMMARY

In 2013, the County of San Diego Office of Emergency Services (San Diego OES) convened cybersecurity, law enforcement, and emergency management subject matter experts to establish a regional Cyber Disruption Response Team (CDRT). The CDRT is responsible for managing the region's response to cyber disruptions as defined in San Diego OES's cyber disruption response plans. In a 2015 full-scale cybersecurity exercise, the CDRT successfully responded to a cyber disruption that affected regional power infrastructure.

DESCRIPTION

Formed using \$190,000 in State Homeland Security Program funds, the CDRT is a specialized group of regional emergency management, cybersecurity, and law enforcement personnel that respond to cyber disruption events affecting the region's life safety and cyber assets. The CDRT includes representatives from San Diego OES, San Diego Law Enforcement Coordination Center, San Diego County Sheriff's Department, and Federal Bureau of Investigation (FBI). When San Diego OES detects a cyber disruption event on the region's networks, CDRT members assemble to investigate the threat and take appropriate action to mitigate further damage. The CDRT uses an incident command system framework to integrate the capabilities of the cybersecurity and emergency response team members.



CRDT members investigate the impacts of a cyber disruption event during the 2015 San Diego Capstone Full-Scale Exercise (San Diego OES)

In 2015, San Diego OES hosted the San Diego Capstone 2015 Full-Scale Exercise to evaluate the region's response to a long-term power outage resulting from a cyber disruption. The exercise scenario involved a cyber attack by a foreign adversary directed at the San Diego Gas & Electric Company's Supervisory Control and Data Acquisition system, creating an extended regional power outage. In response, the CDRT analyzed exercise injects and developed an incident action plan outlining the steps required to address the cyber events, such as sending malicious thumb drives to FBI for forensic analysis and blocking 15 malicious Information Protocol addresses. The plan also included the CDRT's short- and long-term goals for the response; for example, maintaining communication with regional partners. Moreover, the CDRT quickly shared actionable information on the extent of the attack, allowing regional stakeholders to respond effectively. The CDRT will participate in the 2016 National Level Cyber Guard Exercise to further test its response capabilities.

REFERENCES

San Diego OES, Email correspondence with FEMA National Preparedness Assessment Division, April 11, 2016.

County of San Diego Capstone 2015 After Action Report, provided by the County of San Diego Office of Emergency Services, last accessed January 20, 2016.

DISCLAIMER The Lessons Learned Information Sharing Program is a Department of Homeland Security/Federal Emergency Management Agency's resource for lessons learned and innovative ideas for the emergency management and homeland security communities. The content of the documents is for informational purposes only, without warranty, endorsement, or guarantee of any kind, and does not represent the official positions of the Department of Homeland Security. For more information please email FEMA-LessonsLearned@fema.dhs.gov.