Emergency Management and Response - Information Sharing and Analysis Center (EMR-ISAC)

The InfoGram

Volume 18 — Issue 8 | February 22, 2018

Hospital emergency plans not enough during 2017 disasters

Response to hurricanes, shootings and wildfires revealed some gaps in hospital emergency plans in 2017. Hospital staff discuss the problems they uncovered in a USA Today article, along with the ways they are adapting plans to address the lessons learned.

Hospitals in California made the critical decision to evacuate all patients as wind-driven fires threatened last fall. Because power and communications were affected, and because regional hospitals don't have an interoperable records management system, receiving hospitals often didn't know what to expect when patients arrived.

Patient tracking was also affected during the wildfire evacuations. Staff began taking photos of patient wristbands with smartphones as a last resort. Las Vegas hospitals had patient tracking issues after the Mandalay Bay shooting and also resorted to photos. They are considering if creating a centralized information hub is a viable solution for the future.

After the Bronx-Lebanon Hospital shooting last summer, staff found the facility more locked down than their drills and training had anticipated. Staff was unable to easily get surgical supplies, move patients or get to the surgical suite to perform emergency medical tasks. They have since updated their plans, drills and training, and have worked to streamline the clearing process with police.

(Source: USA Today)

Partnering with private sector security on protests and civil unrest

Private sector businesses and facilities are strongly impacted by incidents of civil unrest and protests. Often, businesses are blindsided by these events and have no choice but to ride them out, evaluate any damage and pick up the pieces.

This past summer, security officials from the Mall of America joined New York University's International Center for Enterprise Preparedness (InterCEP) to give the briefing "Civil Unrest, Flash Mobs, and Protests: A Private Sector Perspective." In it they describe the facility and the challenges they face as well as how policies and security measures changed in response to several events starting in 2011.

Even though the Mall of America is unique in its size and security capabilities, there are many lessons to be learned from its experience dealing with both non-violent protests and violence incidents.

- Outreach to federal, state and local law enforcement was vital to developing effective preparedness and response plans.
- Enacting parental escort policies for teens was initially met with negative attitudes but was eventually embraced as crime went down and attendance up.
- For large public spaces such as this, social media monitoring may be a good way to anticipate and prepare for flash mobs or protests.

The summary and recording of the briefing are available on the InterCEP website.

(Source: InterCEP)

Highlights

U.S. Fire Administration

The InfoGram is distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures.

2018 cybersecurity outlook for SLTT governments

The Multi-State Information Sharing and Analysis Center (MS-ISAC) recently released its 2018 SLTT Government Outlook detailing the types of cyber threats it expects to be prevalent in 2018.

The 6-page document predicts a larger role for state, local, tribal and territorial (SLTT) governments in cybersecurity, in part because they will be targeted by cybercrime more. Further:

- Cybercrime against SLTT governments will again be motivated primarily by financial gain.
- Network boundaries will be broken as new cybercrime will increasingly target apps, cloud computing, Internet of Things, cryptocurrencies and supply chain.
- Cybersecurity workforce demand will climb and likely outpace supply. SLTT governments will have a hard time competing with private sector salaries and drawing qualified workers.
- New technology (body cameras, drones, apps) will continue to change how chief information security officers do their jobs.

The MS-ISAC offers SLTT governments free cybersecurity resources and information on prevention, protection, response and recovery. It also assists with incident response through its 24/7 Security Operations Center. Visit the MS-ISAC website to learn more.

(Source: MS-ISAC)

SchoolSafetyInfo.org resources for safer kids

SchoolSafetyInfo.org provides a clearinghouse of information on a variety of school safety problems and initiatives, including but not limited to acts of violence. Resources provided come from a variety of sources including federal and SLTT governments, universities, professional organizations and the private sector.

Directed toward public safety officials and school administrators, the site provides:

- Lessons learned and success stories from other schools and jurisdictions.
- A library of publications, research and other resources.
- Community resources to help schools remain safe.
- Proactive strategies administrators and law enforcement can utilize.
- A calendar of related meetings, conferences and other events nationwide.

This website can be another tool for keeping communities safe. The site is provided by the Justice Technology Information Center, part of the United States Department of Justice.

(Source: SchoolSafety.org)

DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the local FBI office and also the State or Major Urban Area Fusion Center.

For information specifically affecting the private sector critical infrastructure contact the **National Infrastructure Coordinating Center** by phone at **202-282-9201,** or by email at **nicc@dhs.gov.**

The U.S. Fire Administration maintains the Emergency Management and Response – Information Sharing and Analysis Center (EMR-ISAC). For information regarding the EMR-ISAC visit www.usfa.dhs.gov/emr-isac or contact the EMR-ISAC office at: (301) 447-1325 and/or emr-isac@fema.dhs.gov.