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

The InfoGram

Volume 20 — Issue 32 | August 6, 2020

Investigators blow up house to dispose of homemade explosives

First responders need to anticipate the unexpected every day. Sometimes that involves extremely dangerous situations posing a threat to not only authorities but to the lives of the general public as well.

A Utah man opened fire on a SWAT team as they arrived to investigate him for posting threatening messages on social media. The suspect is legally barred from having firearms and eventually surrendered; he's been charged with two counts of attempted criminal homicide and three counts of use of a weapon of mass destruction.

Investigators found explosive chemicals in the house. Some were detonated outside, but some material couldn't be safely moved – bomb experts exploded it in the basement, destroying the home. Over 168 homes and business were evacuated prior to detonation.

Two important things can be learned from this situation. First, suspicious activity reporting works. Someone reported threatening text messages and social media posts the suspect allegedly made to authorities. Items found in the suspect's home suggest a planned event that could have killed or maimed many people. It is a good idea to continue to promote the See Something, Say Something campaign in your community.

Second, law enforcement, first responders, emergency managers and private sector partners can all benefit from Office for Bombing Prevention (OBP) training. OBP offers in-person, virtual instructor-led and computer-based training, ensuring wider availability to meet the needs of more people.

OBP offers such courses as Improvised Explosive Device (IED) Search Procedures; Bomb-Making Materials Awareness Program Outreach Course; Homemade Explosives and Precursor Awareness; and IED Construction and Classification.

Those interested in OBP training should contact their local Protective Security Advisor or email the OBP at OBP@hq.dhs.gov for more information.

(Source: OBP)

Succession planning for public safety communications roles

Working in public safety communications requires dedicated personnel and a unique skill set. When personnel leave communications roles, organizations often experience difficulties maintaining the same level of knowledge and expertise within their organization. This is a consistent problem within all the fields making up the Emergency Services Sector.

To help retain communications skill sets and plan for the loss of personnel, SAFECOM developed the Succession Planning Resources for Public Safety Communications: A Planning and Program Guide for Public Safety Communications Personnel.

This document provides helpful templates to document and track communications systems and training. An included toolkit recommends the creation of a collateral duty, titled the "public safety communications coordinator," to liaise between operational and governance personnel and train in all aspects of the public safety

Highlights

U.S. Fire Administration

The U.S. Fire Administration operates 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.

Subscribe here

communications ecosystem.

SAFECOM developed this document with support from the Cybersecurity and Infrastructure Security (CISA). It reflects the expertise and knowledge of SAFECOM members and coordination efforts of CISA in bringing stakeholders together to share information, best practices and lessons learned in public safety communications. Direct all questions on this document to SAFECOMGovernance@cisa.dhs.gov.

(Source: SAFECOM)

Next Generation 911 (NG911) Roadmap Progress Report

The NG911 Roadmap Progress Report, a follow-up resource to the 2019 NG911 Roadmap, tracks and shares progress made at the national level – by a variety of stakeholders – toward a nationwide NG911 system.

As 911 leaders and organizers forge ahead in creating interconnecting 911 systems, technical and nontechnical tasks need to be completed at the national level to ensure information sharing and avoid duplication of efforts. This collaborative tool:

- Identifies primary goals and specific national-level tasks that need to be accomplished by the 911 community to achieve full migration to NG911.
- Shares the community's progress toward completing identified tasks.
- Highlights opportunities where contribution from leaders like you is still needed.

If you or your organization has made progress in any of the tasks, please let the program know by emailing nhtsa.national911@dot.gov.

(Source: 911.gov)

Webinar: Mass Violence and Terrorism Volunteer Management

Join the Department of Justice's Office for Victims of Crime webinar Mass Violence and Terrorism Volunteer Management for an in-depth look at the Volunteer Management victim assistance protocol. This webinar is part of the Terrorism: Planning, Response, Recovery, and Resources Toolkit web training series. Note there are two offerings of this webinar:

- Monday, August 10, 2020, from 1-2:30 p.m. Eastern.
- Monday, August 17, 2020, from 1-2:30 p.m. Eastern.

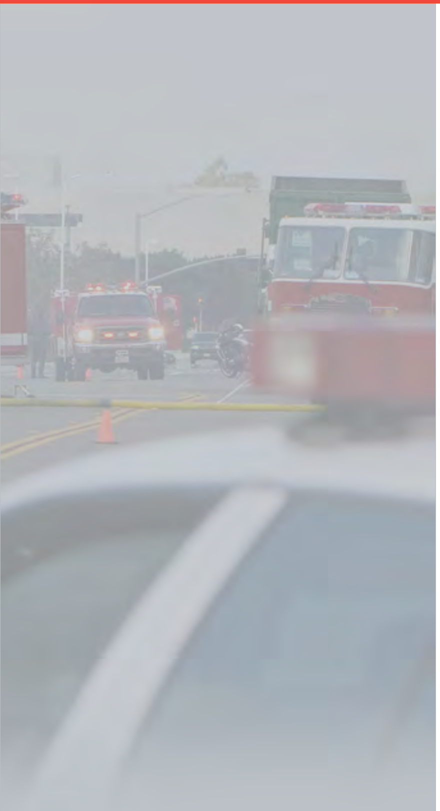
Volunteers play a key role in communities in the aftermath of crises, disasters, emergencies and incidents of mass violence. Many government, nongovernmental, nonprofit, faith-based and philanthropic agencies and organizations rely on volunteers to supplement their existing staff to increase their capacity to respond.

Engaging volunteers in mass violence incident response enhances your ability to serve the needs of victims, survivors and the community. Learn:

- Factors related to using volunteers in disaster response.
- The importance of recruiting, vetting, training and managing volunteers.
- Ways volunteers can address the needs of survivors, families and responders.
- The process of coordinating response agencies and volunteers.

This webinar is part of the Terrorism: Planning, Response, Recovery, and Resources Toolkit training series.

(Source: DOJ OVC)

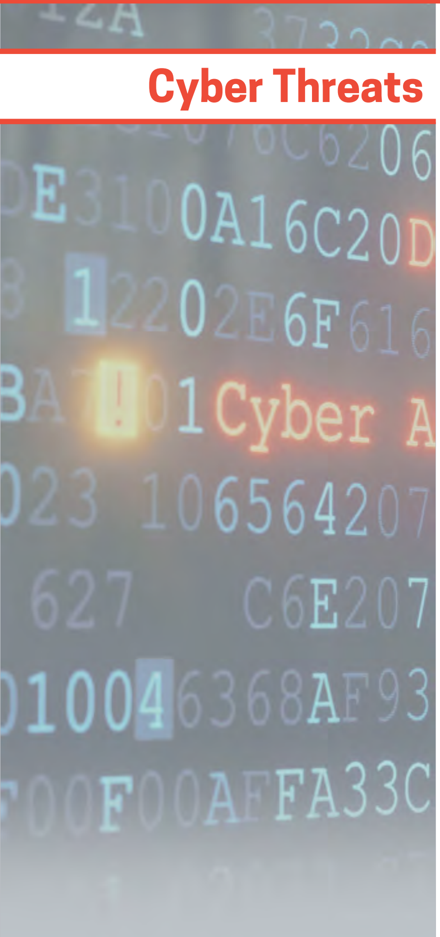


Fair Use Notice:
This InfoGram may contain copyrighted material that was not specifically authorized by the copyright owner.

The EMR-ISAC believes this constitutes "fair use" of copyrighted material as provided for in section 107 of the U.S. Copyright Law.

If you wish to use copyrighted material contained within this document for your own purposes that go beyond "fair use," you must obtain permission from the copyright owner.

Disclaimer of Endorsement:
The appearance of external hyperlinks does not constitute endorsement of the linked websites or the information, products or services contained therein. Reference to any specific commercial products, process or service by trade name, trademark, manufacturer or otherwise, does not necessarily constitute or imply its endorsement, recommendation or favoring by the EMR-ISAC or the U.S. government.



Cyber Threats

Survey finds hackers using more aggressive and destructive tactics

A survey of security professionals finds hackers are getting more aggressive as information technology and security teams continue their internal turf battles.

The increase in counter-incident response – mostly destruction of logs (50 percent) and diversion (44 percent) – signal attackers' increasingly punitive nature and the rise of destructive attacks. A researcher said this shows attacks have shifted from being burglaries to home invasions.

(Source: TechRepublic)

Tens of gigabytes of data made public following ransomware attack

The operators of the Maze ransomware published tens of gigabytes of internal data from the networks of enterprise business giants LG and Xerox following two failed extortion attempts.

The hackers leaked 50.2 Gb they claim to have stolen from LG's internal network, and 25.8 Gb of Xerox data.

Based on screenshots shared by the Maze gang last month and by file samples downloaded and reviewed by ZDNet today, the data appears to contain source code for the cloud-source firmware of various LG products, such as phones and laptops. Based on a cursory review of Xerox data leaked online, it appears the Maze gang stole data related to customer support operations.

(Source: zdnet)

NSA offers advice on how to reduce location tracking risks

The National Security Agency (NSA) today has published guidance on how to expose as little location information as possible while using mobile and Internet of Things devices, social media and mobile apps.

As the agency explains, protecting your geolocation data can be the difference between being tracked wherever you go or knowing that your location can't be used to monitor your movements and daily routine.

Devices like smartphones and tablets use a combination of methods to determine a user's location including Global Positioning System and wireless signals such as Wi-Fi, cellular and Bluetooth.

Disabling these can drastically reduce the exposed location data by blocking devices from sharing real-time geolocation information with cellular providers or rogue bases stations when powered on or during use.

This can also prevent threat actors from determining your device's location with the help of wireless sniffers which calculate it based on signal strength. However, even if disabled, when some device radios are re-enabled they may still transmit saved location information.

(Source: Bleeping Computer)

Cyber Information and Incident Assistance Links

MS-ISAC
SOC@cisecurity.org
1-866-787-4722

IdentityTheft.gov

IC3

Cybercrime Support Network

General Information Links

FTC scam list

CISA alerts

Law Enforcement Cyber Center

TLP Information