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

The InfoGram

Volume 20 — Issue 25 | June 18, 2020

Hospital operations during protests and civil unrest

The Technical Resource, Assessment Center, Information Exchange (TRACIE) released some resources for hospitals and EMS departments trying to manage response to the civil unrest and protests going on around the country.

The first document, Civil Unrest During a Pandemic: Notes from Minneapolis, is a list of challenges and considerations seen by a Minneapolis healthcare system after protests broke out. There is a section calling out problems specific to EMS operations and another on complications caused by COVID-19 safety requirements.

The second document is a Technical Assistance Request listing existing resources on protecting community hospitals and providing care during unrest. It provides resources published by TRACIE as well as a literature review of guidance from government agencies and medical journals.

The last page of the Technical Assistance Request focuses on managing patients who have been exposed to tear gas or pepper spray. It lists respiratory, eye and skin injuries and suggested treatment.

TRACIE also currently has extensive COVID-19 response and support information available for hospitals and pre-hospital agencies.

(Source: TRACIE)

CISA publishes cyber guides to support 9-1-1

State and local governments and agencies, including 9-1-1 departments, are very attractive targets to hackers. The data and systems on their networks are crucial to programs and day-to-day operations. These entities are more likely to pay out the ransom to “unlock” the systems. Hackers also know many jurisdictions have not secured themselves against such attacks, making them easy targets.

The Cybersecurity and Infrastructure Security Agency (CISA) developed a set of cybersecurity references for 9-1-1 centers and PSAPs to help you protect your centers and systems against cyberattack.

Several of the guides focus on Next Generation 9-1-1 (NG9-1-1) systems, which enable a level interconnectivity we have not seen before. NG9-1-1 enhances capabilities of 9-1-1 operations, but with new technology comes new threats and vulnerabilities. The information offered by CISA can help your jurisdiction prepare for these threats and incorporate suggested best practices into plans and training now.

- Cyber Risks to 911: Telephony Denial of Service.
- Cyber Risks to NG911 White Paper.
- NG911 Self-Assessment Tool.

Also provided is a PSAP Ransomware Poster you can brand with your department’s name and display in dispatch and 9-1-1 call centers for your staff to see. It lists recommended best practices your staff can take to protect your center, and what you should do if you suspect a cyberattack or infected computer.

(Source: FEMA)

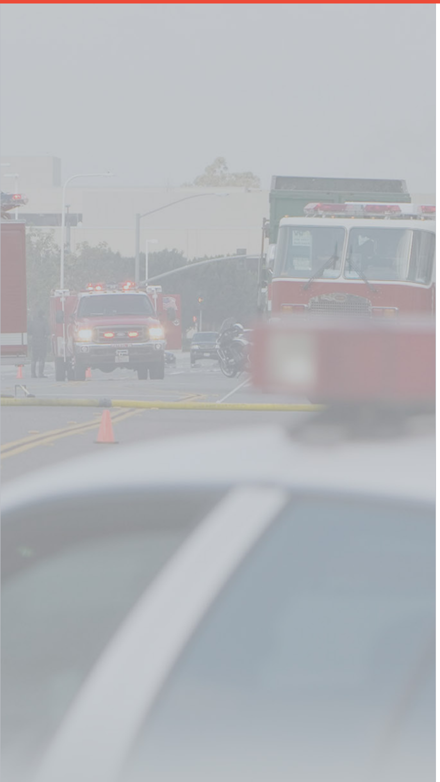
Highlights

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



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.

Fireworks safety and a stressed-out public

Every year around the Fourth of July, people are injured using fireworks at home. This year will be no different, but we add a few new twists to the mix: many people were stuck at home for weeks or months, bored and stressed. Their kids have likely been stuck at home as well since most schools were closed.

A lot of people are stressed and want to blow off some steam. Not a good combination with easily available consumer fireworks.

Fortunately, fire departments have plenty of resources available to them if they want to quickly and easily launch a public safety campaign.

The U.S. Fire Administration (USFA) and the National Fire Protection Association both offer pages dedicated to fireworks safety and related messaging. They offer pre-written messaging and images to share on social media, infographics, tip sheets and links to more information. The Consumer Product Safety Commission provides safety talking points, posters and statistical fireworks injury reports for past years.

This Fireworks Reminder tri-fold from the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) is more technical, reminding people about the regulation of fireworks. It discusses the legalities of transportation, distribution, storage and display of ATF-regulated fireworks.

Your department can take just a few minutes every day to post something on social media or working with local news stations to make a short audio or video clip. Consistent messaging over time can go a long way to saving lives.

(Sources: Various)

Webinar: Post-Traumatic Stress Injuries, Self-Medicating and Coping

First responders experience higher levels of job-related stress, burnout, depression and mental health problems due to repeated exposure to trauma and dangerous situations. Pandemic response only adds to this load. USFA has a dedicated section of its website for COVID-19-related burnout, tips for self-care and links to resources on coping and stress from other partners.

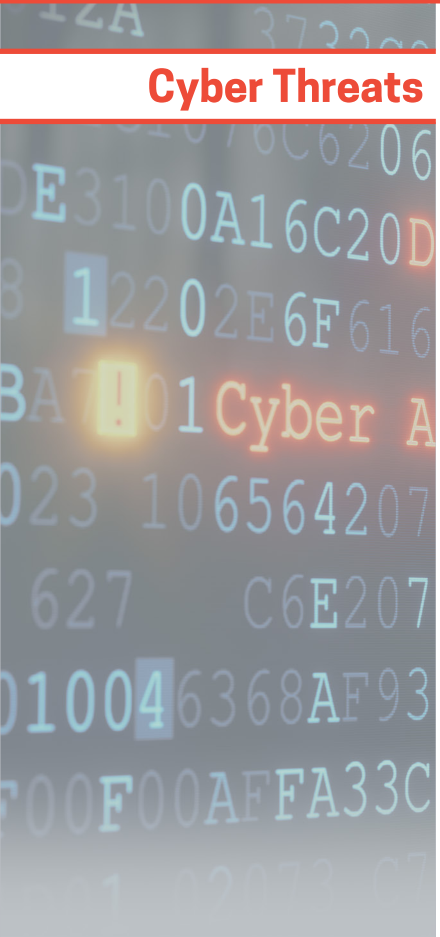
The International Public Safety Association (IPSA) is hosting an upcoming webinar on this topic. Join them on Wednesday, June 24, 2020, from 1-2 p.m. Eastern for First to Respond, Last to Seek Help: Post-Traumatic Stress Injuries, Self-Medicating to Cope and Resiliency.

First responders become accustomed to acute trauma, causing physical, mental and emotional exhaustion of the body and mind. In response to the high intensity of their jobs and the accumulation of traumatic stress injuries, drug and alcohol use can become a means of coping, leaving first responders at risk for developing substance abuse disorders along with mental health issues like stress disorders, depression and anxiety.

During this webinar, the presenter will examine causes, signs and symptoms of post-traumatic stress, how it affects you and your family and what can be done to heal and prevent further damage.

Visit IPSA's website for a full list of upcoming webinars.

(Source: IPSA)



Cyber Threats

ISIS publishes magazine to teach jihadists better cybersecurity

A new 24-page cybersecurity magazine for ISIS supporters walks jihadists through step-by-step security for smartphones – while encouraging them to use a computer instead for more secure terror-related business – and warns of "nightmare" Windows collecting user data from geolocation to browsing history.

The inaugural issue of "The Supporter's Security," published in English and Arabic versions, was produced by the Electronic Horizons Foundation, which launched in January 2016 as a help desk of sorts to walk ISIS supporters through how to encrypt their communications and otherwise avoid detection online while coordinating with and recruiting jihadists.

(Source: HSToday)

Passwords are a government security nightmare

The Small Business Administration blamed an internal error for its recent leak of at least 8,000 Economic Injury Disaster Loan applications. Whether or not a "glitch" is to blame (many officials doubt that it is), this latest headline-making blunder reminds government agencies to review how they're preventing sensitive data from ending up in the wrong hands.

Such news stories attract hackers to government agencies like moths to a flame; it tips them off to which agencies are likely still using antiquated techniques to protect their treasure trove of Social Security numbers, employee credentials, tax IDs and more. Hackers also know agencies have been forced to quickly shift to remote work during this global pandemic and are scrambling to maintain security in a new, complex environment.

There's a simple security measure that could take phishing attacks out of the equation and remove one of hackers most useful tools: getting rid of passwords.

(Source: Government Computer News)

Helping remote workers overcome remote attacks

Because remote workers' devices are all connected to a home network, they don't even need to be attacked directly. Instead, attackers have multiple avenues of attack that can be exploited.

Cybercriminals are experts at making the most of whatever they're given. The current pandemic is no different, and they have been quick to profit from their victims' fears. Adaptability has always been the hallmark of malicious actors, and the proliferation of "remote-everything" attacks is a prime example of the nimbleness of the cybercrime ecosystem. To survive, organizations must be able to match and exceed that agility.

Interestingly, there has been a corresponding drop in more traditional attack methods. This suggests that cybercriminals are adjusting their attack strategies in order to take advantage of the current crisis.

(Source: Threat Post)

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

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