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

The InfoGram

Volume 19 — Issue 30 | August 22, 2019

Lessons from one city's fight against the opioid epidemic

Huntington, West Virginia, has been called ground zero of the opioid crisis by the media. Opioid use and overdoses crept up in the mid-2000s, escalating around 2011 and increasing steadily until 2017 when the county of 95,000 had 1,831 non-fatal overdoses and 183 overdose deaths. That works out to over 15 deaths per month.

The chief of the Huntington Fire Department estimates the average firefighter in Huntington encountered five deaths per month in 2017 due to the opioid epidemic. Some of those were classmates, relatives or friends. The weight of seeing so many deaths in such a short time was overwhelming for many.

In two recent talks, Huntington Fire Department's chief outlined the problems of treating overdose victims, how firefighters in her department are being negatively impacted and what the community is doing about all of it. Huntington began several programs to tackle these problems:

- They started sending out Quick Response Teams (PDF, 434 KB) consisting of a paramedic, law enforcement officer, a recovery clinician and member of the faith community to visit overdose victims within 72 hours of resuscitation to offer treatment options, resulting in a 30 percent success rate.
- They opened ProAct, a one-stop clinic that works with individuals to develop treatment options. This gives first responders a place to take people who have refused to go to the hospital and reduces the load on emergency rooms.
- Huntington received money to develop Compass, a self-care program for first responders and their families. Compass reduces the stigma of mental health counseling, provides effective and fun programs for first responder families and embeds wellness coordinators within first response units.

And the outcome? The Huntington community reduced non-fatal overdoses by 41 percent in 2018 and overdose deaths even more. So far in 2019, overdoses are down more than 60 percent from the 2017 record. This is an incredible turnaround in such a short time.

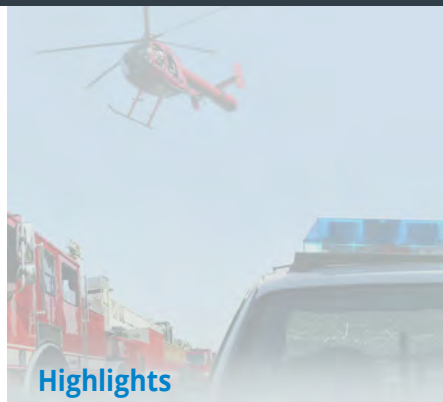
Addressing the opioid issue requires participation of many different departments and offices and better first responder training on substance abuse. Fortunately, the success Huntington has experienced can be mirrored in other communities through similar programs. As the chief states, the opioid epidemic is not a "one-and-done" emergency. This is an ongoing, long-term issue requiring different tactics and procedures than typically used in emergency response.

(Source: Compass)

Social Media & School Violence training for law enforcement

We now seem to live in two worlds – the real world and our online world. For many of us, social media plays a small role in our lives. Some, especially teens, rely on social media and apps for the majority of their interactions and communications. Incidents of school violence have been linked to social media postings, and many warning signs go unnoticed or unreported.

Law enforcement officers, especially school resource officers, need to know how



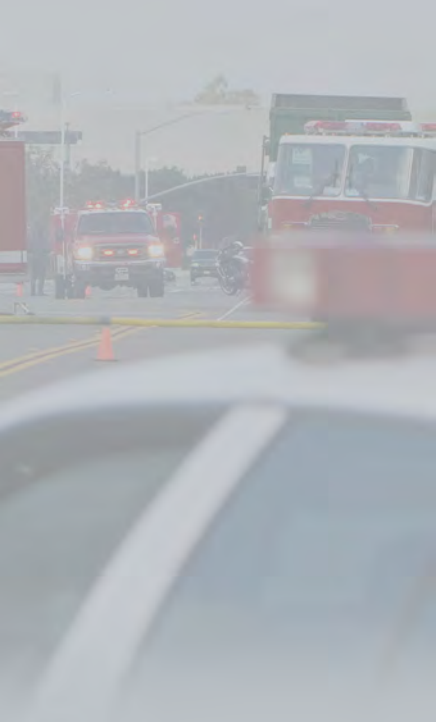
Highlights

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



students communicate on social media, be familiar with the current popular apps and platforms being used and know the common warning signs of potential violence.

The National White Collar Crime Center (NWC3) has a 6-part training video series available entitled "Social Media and School Violence." The training is targeted toward law enforcement, specifically school resource officers, as a way to understand the junction between social media and school violence. The six training segments are:

- Case Study: Jeff Weise.
- Historical Perspective.
- Evolution of Online Social Networks.
- Interactions with Internet Service Providers.
- Emerging Trends.
- Interacting in Social Communities.

Training is available through a NWC3 membership, which is free. Law enforcement agencies or other government agencies involved in the prevention, investigation or prosecution of economic crime, cybercrime and terrorism may request membership.

(Source: NWC3)

USFA report: Fire-Related Firefighter Injuries (2015-2017)

The U.S. Fire Administration (USFA) recently released "Fire-Related Firefighter Injuries," a 15-page topical report detailing data reported to the National Fire Incident Reporting System (NFIRS) from 2015-2017.

Nearly 26,000 fireground firefighter injuries were reported each year, mostly at structure fires, resulting in 46 percent lost work time for the firefighters involved. Of those transported to hospitals, 70 percent were career firefighters.

The majority of these 26,000 incidents were preventable injuries. Please see the report for full details on injuries by age, gender, affiliation, physical condition, type of incident and location when injury was sustained.

(Source: USFA)

Webinar: Shaken Fury 19: tools and technologies used by stakeholders

On August 29, 2019, the National Information Sharing Consortium (NISC) will host "Shaken Fury 19: Tools and Technologies for Information Sharing and Situational Awareness," a webinar overview of the Shaken Fury 2019 exercise and technology solutions used by the Central United States Earthquake Consortium (CUSEC), CUSEC member states and other partners during the exercise.

Topics covered include the Regional Information Sharing Portal (RISP) used for whole-of-community information sharing; implementation of FEMA's Community Lifelines; and more. Webinar attendees will learn how these technology solutions supported information sharing and situational awareness at the federal, state and local levels during Shaken Fury 2019.

The webinar is scheduled for Thursday, August 29, 2019, from 1-2 p.m. Eastern. Registration is required to attend. See the Shaken Fury 2019 fact sheet (PDF, 1 MB) for more information about the exercise.

(Source: NISC)

Cyber Threats

FBI proposes plans for large-scale collection of social media data

The Federal Bureau of Investigation (FBI) is planning to **step up its efforts to monitor social media platforms more aggressively in order to detect potential threats**.

The law enforcement agency is said to be seeking technological solutions from third-party contractors that would make it possible to harvest publicly-available information en masse from Facebook, Twitter, and other social media platforms.

(Source: TheNextWeb)

New data breach has exposed millions of biometrics records

It has been coming for some time, but now **the major breach of a biometric database has actually been reported** — facial recognition records, fingerprints, log data and personal information has all been found on "a publicly accessible database." The damage is not yet clear, but the report claims that actual fingerprints and facial recognition records for millions of people have been exposed.

The issue with biometric data being stored in this way is that, unlike usernames and passwords, it cannot be changed. Once it's compromised, it's compromised. And for that reason this breach report will sound all kinds of alarms.

(Source: Forbes)

Remotely exploiting bugs in building control systems

Security researchers have found a zero-day vulnerability in a popular building controller used for managing various systems, including HVAC (heating, ventilation, and air conditioning), alarms or pressure level in controlled environments.

Discovered using the automated software testing technique called "fuzzing," **the point of failure gives an attacker on the network full control of an unpatched system**. They would be in a position to manage the various building controls connected to the vulnerable device.

(Source: BleepingComputer)

Android users menaced by pre-installed malware

How does malware find its way on to Android smartphones and tablets? By some margin, it's by way of Google's Play Store, which despite repeated efforts to clean it up remains a recurring source of dodgy apps that sit somewhere between suspiciously misleading and downright malicious.

But according to a Black Hat presentation, there's another route that's nearly impossible for users to defend themselves against – **apps that have been factory pre-installed and are carrying malware**. Criminals only need to subvert one of those, which has become a particular problem for cheaper smartphones using the Android Open Source Platform (AOSP).

(Source: NakedSecurity)

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.