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

The InfoGram

Volume 19 — Issue 46 | December 19, 2019

"If You Don't Feel Well, Don't Make it Your Farewell" campaign

The International Association of Fire Chiefs (IAFC) introduced a new firefighter survival campaign recently. "If You Don't Feel Well…Don't Make It Your Farewell" focuses on recognizing the potential warning signs of cardiac problems.

Heart attacks accounted for 33 of the 82 firefighter fatalities in 2018. Most cardiac events have early warning signs, sometimes weeks or months ahead of time. The problem is many of these signs can be easily explained away. "It's just heartburn." "I must have picked up a bug somewhere." "I just feel off, but it'll pass."

Ignoring these signs is dangerous. Firefighters must be aware of the signs and symptoms of cardiac problems – and look for them not only in themselves but also in colleagues who "just doesn't feel well." Seek medical attention early and quickly. If it turns out to be nothing, great; better to "waste time" than have a bad outcome.

The "If You Don't Feel Well…Don't Make It Your Farewell" initiative aims to reduce the number of life-ending cardiac events through awareness, tools and other resources. The IAFC will roll the full program out in early 2020.

For now, firefighters who have experienced a cardiac incident should fill out the IAFC's short online survey. The survey asks about your incident, where you were, what symptoms you experienced, how long before someone took action and other details. It should take less than 2 minutes to fill out. Please share the link with other current and former fire service personnel who may be eligible to complete the survey.

Too many firefighters ignore chest pain and other symptoms. In some cases it winds up being their last call. Know the warning signs of heart attack and get medical attention immediately for yourself or a coworker if these signs are present.

(Source: IAFC)

GIS data requirements for NG911

Next Generation 911 (NG911) is deploying nationwide and it brings big changes to emergency dispatch and response. One of the biggest changes involves geographic information systems (GIS).

NG911 is much more data-rich and will have the benefit of improved call routing thanks to GIS data. Location information will be more complete allowing dispatchers to direct responders to the correct location. However, it all depends on good GIS data.

The National Emergency Numbers Association (NENA) developed the Standard for the NG911 GIS Data Model, defining the structure of GIS data necessary for NG911. As the standard says, "Spatial (GIS) data drives NG911." Information points are useless without the proper structure guiding its use and usability. NENA's standard works through this problem.

Jurisdictions should strongly consider reviewing the NENA standard. It will help you structure GIS data, ensure the data is complete and consistent, and enhance interoperability and data sharing while also reducing ambiguity and confusion

Highlights

"If You Don't Feel Well, Don't Make it Your Farewell" campaign

GIS data requirements for NG911

Conducting wildland fire assessments

Healthcare Challenges in Chemical Incidents, fourth generation agents

Cyber Threats

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.

resulting from unstandardized data.

This is a very technical document defining the terminiology, definitions, keywords and structure of the GIS data model layers. 911 leadership should work with GIS professionals to ensure location layers and GIS data fields meet the needs of NG911.

(Source: NENA)

Conducting wildland fire assessments

The Fire Adapted Communities Learning Network (FAC Net) offers a variety of community wildfire adaptation resources for community leaders and residents, such as a blog, newsletter and interactive map. One useful resource is a network connecting FAC practitioners with each other to share success stories.

Another feature is the Fire Adapted Communities Self-Assessment Tool (FAC SAT), created to help communities assess and track their level of adaptation and create an action plan. This tool can assist a variety of community sizes from neighborhoods to cities and even entire counties, but is not for national tracking. The FAC SAT User and Facilitator's Guide outlines who should be involved in the process and how long it will likely take to go through it.

Fire departments interested in bolstering community wildfire resilience should think about doing home wildfire assessments in their communities. The Wildland Fire Assessment Program is a joint U.S. Forest Service/National Volunteer Fire Council program. It consists of in-person or online training and has available a toolkit, online checklists, certificate template, liability waiver, press release samples and other resources to help fire departments make their communities safer.

(Source: Fire Adapted Communities)

Healthcare Challenges in Chemical Incidents, fourth generation agents

Chemical incidents overseas, both accidents and attacks, highlight the need for improved planning by responders and healthcare facilities.

In 2018, a military-grade nerve agent was used in a poisoning attack in the United Kingdom (UK). Several other people, including two police officers and a number of paramedics, were also sickened by the poison. Emergency services spent nearly £900,000 (over $1.1 million) replacing contaminated ambulances and police vehicles.

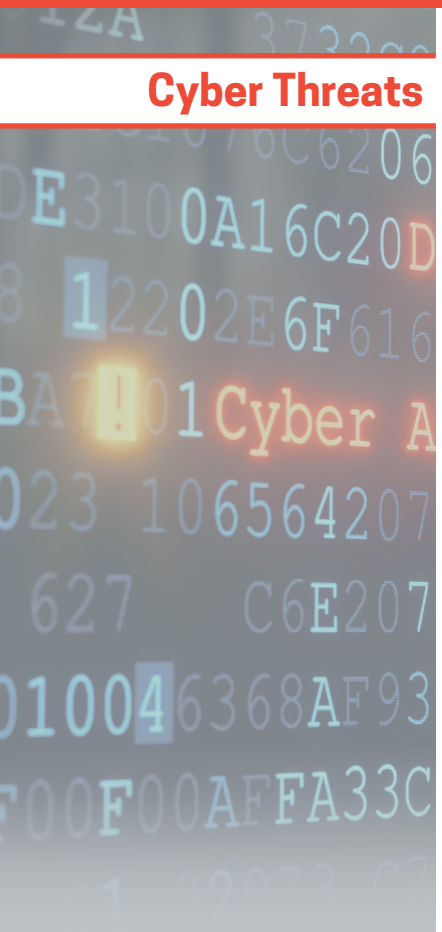
The Technical Resources, Assistance Center, and Information Exchange (TRACIE) is hosting the webinar "Healthcare Challenges in Chemical Incidents" (PDF, 326 KB) on January 14, 2020, from 1:30-3 p.m. Eastern. Speakers will discuss the potential effects of a chemical incident, planning considerations, recent guidance and lessons learned in assessing, triaging and treating patients. Space is limited for this webinar and registration is required.

The webinar will also discuss fourth generation agents including organophosphorus compounds such as those used in the United Kingdom incident.

After the UK attacks, the United States began developing guidance for emergency response professionals to aid in response planning, patient treatment and officer safety. For more information on response to chemical attacks and fourth generation agents, see the Health and Human Services website for Chemical Hazards Emergency Medical Management (CHEMM) or the Virginia Department of Health website.

(Source: CHEMM)

Cyber Threats



New Orleans declares state of emergency following cyberattack

The City of **New Orleans has suffered a cybersecurity attack serious enough for Mayor LaToya Cantrell to declare a state of emergency**.

The attack started at 5 a.m. on Friday, December 13, according to the City of New Orleans' emergency preparedness campaign, NOLA Ready, managed by the Office of Homeland Security and Emergency Preparedness. NOLA Ready tweeted that "suspicious activity was detected on the City's network," and as investigations progressed, "activity indicating a cybersecurity incident was detected around 11 a.m." As a precautionary measure, the NOLA tweet confirmed, the city's IT department gave the order for all employees to power down computers and disconnect from Wi-Fi. All city servers were also powered down, and employees told to unplug any of their devices.

(Source: Forbes)

"Password" falls in the ranks of favorite bad passwords

SplashData evaluated more than 5 million passwords leaked on the Internet to compile this year's list of risky passwords. In first place was "123456," holding the top spot from last year, followed by "123456789" and "qwerty." While it's positive to learn people are less frequently using "password" to secure their accounts, SplashData says, it warns **many continue to employ easily guessable words and alphanumeric patterns**. Many modern websites and applications prevent these simple passwords from being used; however, some older ones still allow it.

There were a few consistent passwords on this year's list, among them "princess," "iloveyou," and "welcome." New entries included "1q2w3e4r" and "qwertyuiop," which may seem complicated to some but likely won't trick hackers who can guess simple keyboard patterns.

(Source: Dark Reading)

Six cybersecurity predictions for 2020

Data breaches will likely continue to increase not only in terms of volume, but also in terms of severity in the coming year. Remember, it only takes one compromised credential to impact millions — millions of dollars, millions of customers, millions of lost opportunities, etc.

Here are five more cybersecurity predictions for 2020:

- Successful ransomware attacks will double.
- Misplaced understanding of cloud security will increase risk.
- More state election boards will be hacked.
- 2020 will bring the rise of securing machine identities.
- Phishing will continue to evolve beyond email to SMS and video.

(Source: Forbes)

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