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

The InfoGram

Volume 19 — Issue 32 | September 5, 2019

California chemical suicide hospitalizes nine people

A recent hazmat incident in a California hotel is being investigated as a chemical suicide. One person died and nine others were hospitalized.

Chemical suicides involve people mixing easily-attainable chemicals to produce a lethal gas, such as hydrogen sulfide or hydrogen cyanide, in an enclosed space like a car or small room. Instructions to commit suicide in this way are readily available on the internet, unfortunately. It is not seen often and many first responders may not fully know the dangers.

Rushing in to help an unconscious or unresponsive chemical suicide victim may make you the next victim. It's very important to take a moment and look for these common indicators at the scene before proceeding:

- Signs taped to doors or windows warning of dangerous chemicals or gas.
- Tape sealing the edges of doors, windows or vents.
- Look in the windows for chemical containers or chemical fog.
- Take notice of any chemical odors.

The Department of Health and Human Services Chemical Hazards Emergency Medical Management (CHEMM) offers "Chemical Suicides: The Risk to Emergency Responders." The webpage lists toxic gases commonly seen at these incidents and response considerations when managing size up, securing the scene, decontamination, air monitoring and officer safety. CHEMM also offers links to resources from other organizations.

(Source: CHEMM)

NFA superintendent discusses changes to EFO program in podcast

The National Fire Academy (NFA) is refreshing its Executive Fire Officer (EFO) Program beginning in early 2020. NFA Superintendent Chief Tonya Hoover discusses these changes in more detail in a recent podcast produced by the International Association of Fire Chiefs. Significant changes include:

- Program shortened from 4 years to 24 months
- Two stipend trips per year to the NFA.
- Residential courses and blended online learning from home or work
- Cohort learning allowing for groups of students to take EFO classes together.
- Completion of a graduate-level thesis as opposed to four Applied Research Projects.

Prior to attending the first EFO course, students will complete a mediated online course on research methods. During the last residency, students will present their thesis.

Feedback from past students drove many of these changes, especially the cohort

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

learning, where the same group will progress through the program together.

The application period for the new EFO program opens in January 2020 and closes on May 15, 2020. Students currently enrolled in their second, third or fourth year of EFO will continue through the original curriculum.

(Source: U.S. Fire Administration)

Insider Threat Awareness Month

Organizations, agencies and businesses are at risk from insider threats, employees who may use their position within the workplace to cause the organization or other employees harm through negligence or malicious intent. Examples can include workplace violence, sabotage, theft or unintentionally clicking on an email containing a phishing or ransomware attack.

September has been deemed "Insider Threat Awareness Month" by a partnership of federal agencies. The goal of this campaign is to raise awareness of insider threat risks and educate people on how to recognize indicators and report suspicious activities.

While many federal agencies and the military may need to focus on espionage, emergency responder agencies could focus more on cybersecurity phishing and ransomware education and employee morale. Unhappy or disenfranchised employees are more likely to commit acts consistent with what is considered an insider threat, including violence.

The Office of the Director of National Intelligence (ODNI) offers free insider threat training through its National Insider Threat Task Force. The free training could be incorporated into a staff briefing or internal company training program. ODNI also offers a host of other guides, multi-media and links to other federal resources.

During this month, emphasize the importance of safeguarding our workplaces, fellow employees and our nation from the risks posed by insider threats and continue to work diligently to mitigate these risks.

(Source: ODNI)

Webinar: Social Media Monitoring in Public Health Emergencies

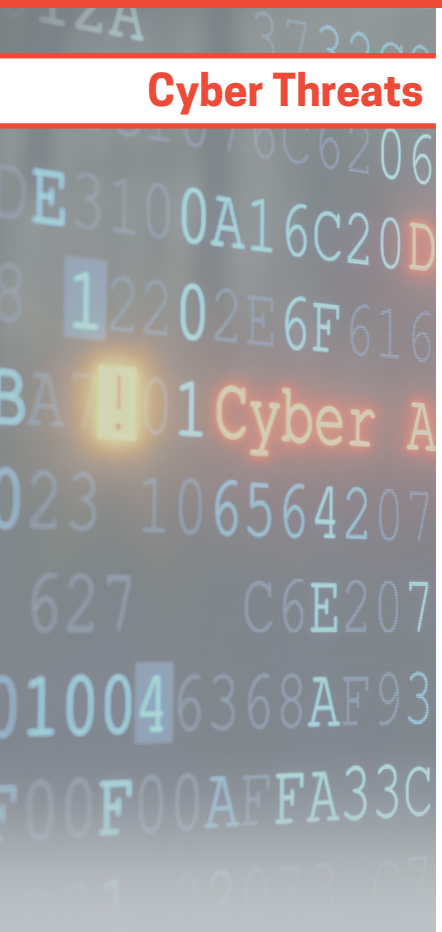
The National Association of County and City Health Officials (NACCHO) and the New York City Department of Health offer a recording of the webinar "Social Media Monitoring in Public Health Emergencies," showing viewers the benefits of social media when monitoring and responding to the spread of (mis)information during public health emergencies.

This 2-hour webinar recording describes the importance of being aware of public sentiment during a public health emergency. It identifies how to use social media bidirectionally to both provide updates and collect public feedback, and shares scalable approaches for managing social media monitoring regardless of organizational budget.

This is a recorded webinar, originally part of a multi-part series to help local health departments build capacity to engage in public health communication. Registration is required to view the recording.

(Source: NACCHO)

Cyber Threats



How Lubbock County fended off a ransomware attack

More than 20 Texas cities have been attacked with ransomware recently. Though state officials won't divulge the targets, the Houston Chronicle reports that the city of Keene was affected, and the city of Borger issued a statement about the effects of its own attack.

But Lubbock County fended off the cyberattack. Judge Curtis Parrish is head of the Lubbock County Commissioner's Court, and says that's because an employee noticed a suspicious file.

"**They did exactly what they're trained to do**, and that's call our IT department immediately," Parrish says. "What we found out was that was a ransomware virus."

(Source: Texas Standard)

CISA Weekly Vulnerability Summaries

The Cybersecurity and Infrastructure Security Agency (CISA) publishes weekly Vulnerability Summaries, **lists of newly recorded vulnerabilities** from the National Institute of Standards and Technology National Vulnerability Database (NVD) in the previous week. The NVD is sponsored by the Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC) and the United States Computer Emergency Readiness Team (US-CERT).

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NVD. In some cases, the vulnerabilities in the Bulletin may not yet have assigned Common Vulnerability Scoring System (CVSS) scores. Visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

(Source: US-CERT)

Gamification can transform company cybersecurity culture

Gamification takes the fun part about games and effectively applies it to situations that are generally seen as not fun or as having no day-to-day value (a.k.a. "busywork"). The heart of effective implementation of gamification revolves around points and incentives; risk-owners that complete cybersecurity tasks correctly and in a timely fashion will be awarded points.

According to findings from the American Psychological Association, competition increases physiological and psychological activation, preparing employees' minds for increased effort and enables higher performance.

(Source: Threat Post)

Hacker claims ability to "turn off" 25,000 cars

Every day millions of us rely on tech to protect our cars from thieves. Immobilizers, for instance, ensure only the owner of the right key fob can start the vehicle.

But now that technology has become a security threat, after **hackers told Forbes they could lock down up to 25,000 cars at once**. It's all thanks to a vulnerability (now fixed) that made it frighteningly simple to quickly take remote control of a car's immobilizer and prevent drivers from starting their vehicle.

(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

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