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

The InfoGram

Volume 19 — Issue 41 | November 7, 2019

Ambulance workers four times more likely to get injured on the job

For every 100 paramedics and emergency medical technicians (EMTs) in the United States, between 8 and 9 experience an occupational injury requiring treatment in a hospital. While 8-9 percent may seem like a small amount, it is more than 4 times the rate for workers in any other profession in the United States.

These numbers are based on data from the National Institute for Occupational Safety and Health (NIOSH).

Repetitive duties such as lifting patients, bending and kneeling lead to more back injuries, sprains and strains. The second leading cause is exposure to blood and bodily fluids. These hazards are constant within the profession, but risk of injury can be managed through exercises and stretching or, in the case of exposure to harmful substances, proper use of PPE.

Assaults on ambulance workers comes in as third. While reported assaults make up a small portion of total injuries, the number is still 22 times higher than any other occupation. Researchers also believe this number is underreported.

Some things ambulance workers can do to avoid occupational injuries:

- Review and use proper lifting techniques.
- Do exercises and stretches aimed at strengthening muscles and joints used for common work-related duties.
- Report assaults and patient violence to help bring attention to the problem and give researchers and lawmakers a better data to work with.

(Source: OHSOnline)

Registration now open for CDP's Tribal Training Week 2020

Registration is now open for the Center for Domestic Preparedness' (CDP's) Tribal Training Week 2020, the largest annual tribal training event the Department of Homeland Security holds.

The event will run from March 28 to April 4, 2020, on the CDP campus in Anniston, Alabama, and feature 15 courses in eight different training lanes, in addition to a number of evening activities. Five of the training lanes will culminate in an integrated capstone exercise with students working though a mass casualty scenario featuring multiple events and dozens of live actors.

Those interested in attending the training week should contact David Hall, the CDP's Tribal Nations Training Coordinator, at david.hall@fema.dhs.gov. Registration closes on March 25, 2020.

In 2019, more than 230 responders from 46 Tribal Nations and 45 Tribal agencies attended Tribal Training Week. Activities included presentations by a number of the CDP's training partners from across the country as well as evening lectures on topical issues such as active shooter response and cybersecurity.

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.

The event kicked off with a feast of a variety of traditional Native American dishes, followed by a formal opening ceremony in the CDP's headquarters building.

See the CDP's website for a full list of available training opportunities.

(Source: CDP)

New Cyber Essentials answers the question "Where do I start?"

Cyber attackers are becoming less discriminate in their targets. If you aren't the federal government or a large business, it's easy to think you're a less-attractive target.

But a quick look at the news shows this is not the case. Small entities have not historically been part of the national cybersecurity dialogue, and the result is that they aren't as aware of the risks much less how to prepare for them.

Small and local government agencies and small businesses needing guidance can start with the Cyber Essentials. This new national initiative from the Cybersecurity and Infrastructure Security Agency (CISA) is a set of easy to adopt and understand, community-endorsed cybersecurity practices constituting "the basics." They are CISA's answer to the question heard often from stakeholders – "Where do I start?"

The Cyber Essentials are written for those with limited or no knowledge of cybersecurity practice or terminology but who nevertheless are responsible for safeguarding their organizations.

This is intended to be the first of many Essentials releases as part of the broader campaign. CISA will refine and develop future supplemental Essentials products and resources based on feedback from the Essentials audience and partners.

(Source: CISA)

Webinar: Surviving the Service - Cardiac, Cancer, Behavioral Threats

The International Public Safety Association (IPSA) is offering the free webinar "Surviving the Service: Cardiac, Cancer, Behavioral Threats and the Role of Early Detection" on Thursday, November 14, 2019, from 12-1:15 p.m. Eastern.

Members of the uniformed services have unique occupational health risks. Each year countless men and women of law enforcement, fire and EMS lose their lives or suffer permanent disability from preventable occupational health risks.

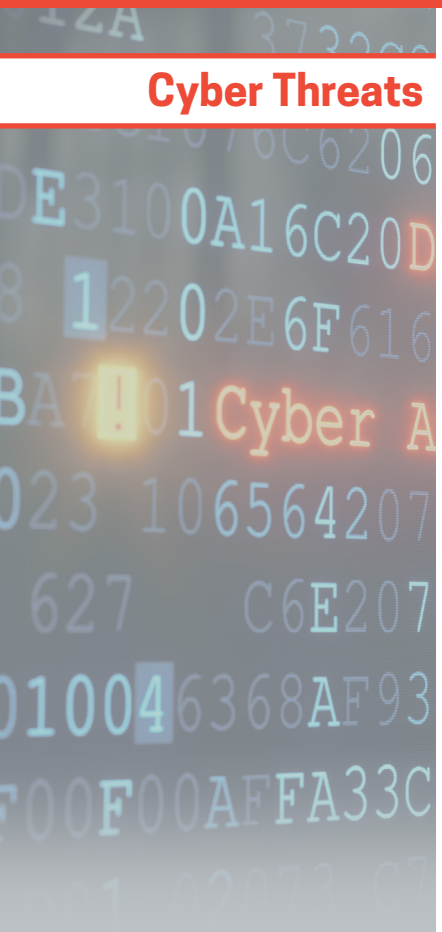
FireRescue1 calls it the trifecta of fire service occupational death: cardiovascular, cancer and suicide. A stronger push for prevention is needed along with regular visits to the doctor to ensure early detection and timely treatment.

This webinar will discuss current science and emerging research on the critical role early detection plays in assuring outcomes that have the highest survival opportunities and return to work. Learn how regular annual exams and screening can lead to early detection of potentially deadly medical conditions.

Registration is required for this webinar. For other webinars, events and publications, see the IPSA website.

(Source: IPSA)

Cyber Threats



2019's scariest hacks and vulnerabilities

Yes, this is one of those end-of-year summaries. And it's a long one, since 2019 has been a disaster in terms of cybersecurity news, with one or more major stories breaking on a weekly basis.

See this zdnet article for a **summary for the past 10 months of security incidents, data breaches and vulnerabilities** organized by month.

(Source: zdnet)

Low-tech social engineering attacks

Frank Abagnale is probably the most famous low-tech hacker since Son'ka the Golden Hand and the man who stole the Mona Lisa. Abagnale famously used social engineering to help facilitate financial scams where he used false identities to forge checks and cash them. Abagnale ended up being sentenced to 12 years in prison for fraud. He is now a regular at cybersecurity and regulatory compliance conferences.

Low-tech and social engineering are good bedfellows. Low-tech social engineering tricks often dovetail with their high-tech cousins to carry out a cyberattack. **Learn the common low-tech social engineering tactics you should avoid**.

(Source: Infosec)

Majority of 2019 breaches were result of unapplied security patches

Despite a 24 percent average increase in annual spending on prevention, detection and remediation in 2019 compared with 2018, patching is delayed an average of 12 days due to data silos and poor organizational coordination, a study finds.

Looking specifically at the most critical vulnerabilities, **the average timeline to patch is 16 days**.

At the same time, the risk is increasing. According to the findings, there was a 17 percent increase in cyberattacks over the past year, and 60 percent of breaches were linked to a vulnerability where a patch was available, but not applied.

(Source: HelpNetSecurity)

U.S. government and military travel details left exposed online

Significant amounts of **sensitive data about employees of the United States government and military personnel could now be in the public domain** following its exposure in a data leak.

Data exposed by the unsecured web bucket, which could be accessed by anybody without the use of any passwords, included: full name, date of birth, home address, phone number, dates and costs of travel, and partial credit card details.

(Source: HotForSecurity)

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.