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

The InfoGram

Volume 19 — Issue 38 | October 17, 2019

NIOSH adds new Fentanyl toolkit

The National Institute for Occupational Safety and Health (NIOSH) added a toolkit to its library of Fentanyl resources for first responders. This new toolkit helps first responders learn how to best protect themselves from exposure to Fentanyl.

Any emergency responders who may encounter drugs or drug paraphernalia during the course of their work should review these materials. This includes law enforcement, EMS providers, fire department personnel, investigators, evidence handlers, special operations and decontamination workers. The toolkit contains:

- Two videos - one shows body camera footage of an officer who was exposed to an illicit drug; the other discusses how to properly don and doff PPE.
- Infographics on spotting illicit drugs; protecting yourself from exposure; selecting PPE; and decontaminating before you go home.
- Two postcards on protecting yourself and protecting your family.

While the new toolkit provides quick reference on Fentanyl dangers and exposure protection, the NIOSH's main page on Fentanyl and illicit drug protection offers more detail on safety. Please see that page for extensive information on PPE, training, decontamination, and handling exposure with working dogs.

(Source: NIOSH)

Want to reduce disaster recovery costs? Spend more on mitigation

2017 natural disaster costs in the United States are estimated to top $300 billion, with nearly half that going to Hurricane Harvey damage. The May 2019 tornado outbreak cost approximately $2.9 billion, and costs associated with the 2018 Camp Fire in California are likely be in the billions as well.

There is no denying that disasters are expensive and seem to get more so every year. Federal, state, local, tribal and territorial agencies or jurisdictions interested in saving money on recovery costs should consider spending more. Yes, spending more, but strategically.

A recent report from the National Institute of Building Sciences (NIBS) found that every $1 spent on disaster mitigation saves $6 on recovery costs. That is quite a return on investment, one that might pinch initially but has the potential to save everyone a lot of money and effort in the future.

Though this study specifically looked at mitigation spending by the Federal Emergency Management Agency, the Economic Development Agency, and Housing and Urban Development, it very likely applies to mitigation spending overall by everyone from local governments to individual households to community organizations.

Some other interesting findings:

- Savings of $7 for every dollar spent on proactive mitigation steps like demolishing flood-prone buildings.

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

- Savings of $4 for every dollar spent on construction exceeding the International Code Council's 2015 model building code ("code-plus" mitigation).

The report discusses specific practices showing significant cost-benefit results. See the full report for the details.

(Source: NIBS)

Hazardous Materials Markings, Labeling and Placarding Guide

The Department of Transportation (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA) offers the "DOT Chart 16 - Hazardous Materials Markings, Labeling and Placarding Guide," available as a printable 4-page document as well as a mobile phone app for both iPhone and Android.

This guide provides general information on standard hazardous materials markings in a quickly-scannable format. This makes it a handy visual aid first responders can print and keep in apparatus, as it may be useful at the scene of an incident during initial size-up.

Note that this guide does not list the 4-digit identification numbers used on placards to denote what hazardous material is being transported. For more information on the numbering system, see the Emergency Response Guidebook (ERG). To get a copy of the 2016 ERG, contact your state coordinator.

(Source: PHMSA)

Webinar: Smart Villages and Resilience to Natural Disasters

In western cultures, we put stronger emphasis on technology and the physical infrastructure and have large budgets to protect and rebuild it. While building and maintaining physical infrastructure is part of the solution, it's important to note that villages across the world manage disasters "off the grid" regularly because they have never been on the grid to begin with (PDF, 2.5 MB).

Nearly 50 percent of the world's population and 70 percent of the world's poor live in rural areas, giving rural resiliency a prominent role in emergency management and its own set of obstacles and challenges.

Smart Villages, an organization focusing on remote villages and their access to modern opportunities and solutions, offers a recording of the webinar "Smart Villages & Resilience," discussing how some villages are better able to respond to disasters than others and how it relates to access to energy.

This webinar brings together experts who have worked in the Caribbean, Thailand, Malaysia and Nepal to discuss disaster and resilience, including how these issues relate to off-grid energy and energy access, agricultural communities, and to look at "smart villages" that are better able to respond to disasters.

Often the kind of social capital emergency managers and nonprofit organizations are trying to build in "modern" communities is the type already successful in small rural villages: a stewardship role in the local environment, ultimately minimizing vulnerabilities to natural disasters (PDF, 291 KB). Understanding how rural villages maintain this attitude can go a long way toward recreating it.

(Source: Smart Villages)

Cyber Threats

Risk of cyberattack to ships and ports

The maritime industry has been discussing how emerging attack surfaces could increase the risk of **cyberattacks capable of crippling ships – or even potentially hijacking autonomous vessels at sea**.

Key public and private interests are aware of the challenges created by connected and automated vessel navigation and propulsion systems, and they have done a good job of engaging with cybersecurity vendors to address emerging risks.

However, there is a glaring area of vulnerability on the port management side that has not been fully discussed or addressed: connected systems at our nation's ports.

(Source: HelpNetSecurity.com)

Famous social engineering attacks

Human beings are essentially social creatures. We like to help one another. We generally defer to people higher up in the hierarchy than we are and trust that other people are honest, mean what they say, and are who they say they are, because questioning any of those things without good reason is rude.

Unfortunately, these **social niceties can turn us into the weakest link in information security**. Too often hacks result not from technical flaws but from what's known as social engineering: human beings allowing themselves to be convinced to let down their guard. Many of the techniques are as old as con artistry itself, but have been updated for the digital age.

(Source: CSOnline)

How cybercriminals exploit simple human mistakes

Whether triggered by work pressure or an attacker, **human vulnerabilities can expose a company to cybercrime**. As more organizations fear "accidental insiders," addressing these vulnerabilities becomes critical.

So long as companies don't understand the implications of cognitive biases, they will continue to pose a significant security risk. ISF's report lists 12 biases, all of which can have different effects on security. One example is "bounded rationality," or the tendency for someone to make a "good enough" decision based on the amount of time they have to make it.

(Source: DarkReading)

5 ways cybersecurity chiefs can support emerging technology

As we head into the 2020s, emerging technologies are both exciting and a bit scary at the same time.

On the positive side, the definition of "government service" is changing before our eyes. From artificial intelligence and the Internet of Things to 5G apps and autonomous vehicles, **the list of startup opportunities promises to revolutionize government (again) over the next decade**.

But, if history has taught us anything over the past two decades, the Achilles' heel to these advances in technology will continue to be cybersecurity.

(Source: Government Technology)

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.