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

The InfoGram

Close Your Door program fights fire with science

For years we've known residential fire spreads faster than it did decades ago. Depending on the circumstances, people had about 17 minutes to escape a fire 40 years ago. That number has reduced drastically - today, you have about 3 minutes.

People continue to believe an open bedroom door is safer if they experience a fire, yet research shows closing your bedroom door while sleeping drastically improves the likelihood you will survive. It isolates the fire's flow, reduces room temperature, and keeps both carbon monoxide and smoke levels down.

After proving a closed door could potentially save lives in a fire, the Underwriters Laboratories Firefighter Safety Research Institute (UL FSRI) has committed to share this finding with the world. The Close Your Door safety initiative is the result of over 10 years of UL FSRI research.

The most powerful teaching tool UL FSRI offers is a video of a fire demonstration showing two bedrooms, one with a closed door and one with an open door. This video is under 6 minutes but tackles the common misperception that a closed bedroom door is more dangerous during a fire with sobering realism.

UL FSRI created a site specifically to help firefighters share this life saving information and it includes a toolbox of resources including pre-made social media posts, shorter public service announcement videos, public relations materials, and outreach materials like coloring sheets for kids, flyers, magnets, door hangers and posters.

(Source: CloseYourDoor.org)

Drill of the Dead: mass dispensing during the zombie apocalypse

In 2011, the Centers for Disease Control and Prevention (CDC) published an online campaign making correlations between preparing for a zombie apocalypse and disaster preparedness. The CDC took some heat for it, though, as some thought it was a waste of time and resources.

The campaign drew so much traffic that it crashed the CDC's website.

Disaster preparedness is mundane and agencies struggle to get people to care. This campaign provides some lessons in success: thinking outside the box and using humor can get better results than sticking with the "same old, same old." Also, the CDC successfully targeted a younger audience using different outlets.

A Montana county with only three public health department employees used a zombie scenario around Halloween in a mass dispensing exercise, in part because of the CDC's success.

"Drill of the Dead" engaged the whole community and involved multiple agencies, local schools, the university, non-profits and private sector organizations. Volunteer fire department and hazmat teams conducted decontamination exercises, and local students acted as zombies – complete with moulage – and received zombie bite triage tags and "treat"-ments depending on their costuming and level of infection.

Though it may be seen as a gimmick, using a made-up novel outbreak like "zombie-

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

ism" has a benefit of removing participant expectations or preconceptions they may otherwise fall back on if training for something like influenza.

This very detailed exercise met all the criteria for the Homeland Security Exercise and Evaluation program. Officials talk about exercise planning and execution details in a free 1-hour webinar through the Northwest Center for Public Health Practice.

(Source: NWCPHP)

NIMS Training Program refresh released, FEMA requesting comments

FEMA released the refreshed National Incident Management System (NIMS) Training Program for a 30-day National Engagement Period. This is an opportunity for interested parties to comment on the draft so that it reflects the collective expertise and experience of the whole community.

The NIMS Training Program sets a structure for national training and establishes the roles and responsibilities of FEMA and members of the NIMS stakeholder community. The training program identifies specific activities for developing, maintaining, and sustaining a training program that prepares all incident personnel to understand their respective responsibilities and work together during incidents.

The revised NIMS Training Program introduces training Focus Areas based on incident personnel's position and responsibility. The Focus Areas include the Incident Command System, Joint Information System, Emergency Operation Center and the Multiagency Coordination Group.

FEMA will host a series of 60-minute engagement webinars in the beginning of June to highlight key proposed changes to NIMS and answer participant questions about submitting feedback. All webinars are open to the whole community.

To provide comments on the draft, complete the feedback form and submit it to FEMA-NIMS@fema.dhs.gov by June 21, 2019, 5 p.m. Eastern.

(Source: FEMA)

CISA hosting webinar on upcoming 2019 hurricane season

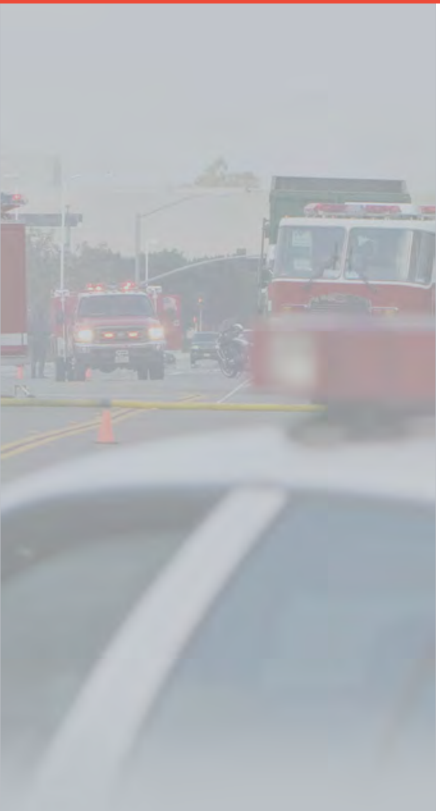
The Cybersecurity and Infrastructure Security Agency (CISA) staff and partners will discuss lessons learned from the historic 2017-2018 hurricane season in an upcoming webinar.

The webinar is for federal, state, local, tribal, territorial and private sector partners whose responsibility it is to protect and rebuild critical infrastructure systems and interdependencies.

CISA invites you to participate in the webinar, scheduled for Tuesday, June 11, 2019, from 10-11:30 a.m. Eastern. Presenters will cover CISA's role and resources in hurricane preparedness and response activities. It will also feature presentations from the National Oceanic and Atmospheric Association Liaison to the National Operations Center and the Federal Emergency Management Agency's (FEMA) National Business Emergency Operations Center.

- Registration link.
- Audio Conference Bridge: (800) 779-8419
- Participant Passcode: 9077541

(Source: CISA)



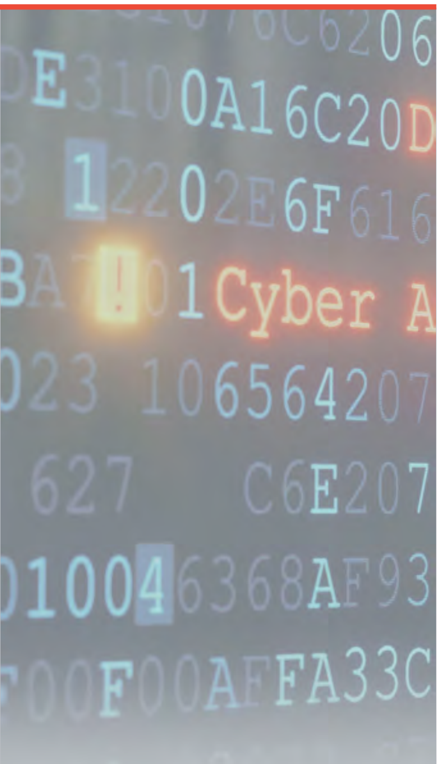
Fair Use Notice:
This InfoGram may contain copyrighted material that was not specifically authorized by the copyright owner.

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.

Cyber Threats



Health industry cybersecurity practices: managing threats

“Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP),” produced by the Department of Health and Human Services, aims to raise awareness, provide vetted cybersecurity practices and **move organizations towards consistency in mitigating the current most pertinent cybersecurity threats to the sector**. It seeks to aid healthcare and public health organizations to develop meaningful cybersecurity objectives and outcomes. The publication includes a main document, two technical volumes, resources and templates.

(Source: DHHS)

Massive dedicated denial of service attacks increase 487 percent

New Kaspersky Lab research shows that **distributed denial-of-service (DDoS) attacks surged by 84 percent in the first three months of 2019**. This growth reverses the downward trend that was recorded throughout 2018. Compared to the first quarter of last year, larger attacks involving 100 GB or more increased by a staggering 967 percent.

(Source: TechRepublic)

Money not the only thing hackers are after in ransomware attacks

When hackers launch a ransomware attack against companies, they’re usually after money. But when ransomware strikes a government agency, the **hackers may be after something other than money**. They might intend to create disruption and gain “street cred.” This opens other avenues for negotiation and does not necessarily mean paying ransom, but rather managing risk.

(Source: GCN)

Lessons learned from the Baltimore ransomware clean-up

It’s been three weeks since the City of Baltimore’s networks were shut down due to a ransomware attack, and it may be weeks more before the city’s services return to something resembling normal.

To top it off, unlike the City of Atlanta—which suffered from a Samsam ransomware attack in March of 2018—Baltimore has no insurance to cover the cost of a cyberattack. So **the cost of cleaning up the RobbinHood ransomware will be borne entirely by Baltimore’s citizens** and will far exceed the approximately $70,000 ransom.

(Source: ArsTechnica)

Over 90 percent of Internet of Things transactions are unencrypted

A new report looked at millions of connections from Internet of Things (IoT) devices on enterprise networks and found over 40 percent of them do not encrypt their traffic. The devices included **smart watches, smart printers, smart TVs, digital home assistants, medical devices**, digital video recorders, media players, data collection terminals, digital signage media players, industry control devices, networking devices, 3D printers and even smart cars.

(Source: CSOonline)

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