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

The InfoGram

Volume 19 — Issue 42 | November 14, 2019

U.S. Secret Service releases new research on school violence

Last week, the U.S. Secret Service (USSS) released "Protecting America's Schools" (PDF, 9 MB), a study of 41 targeted school violence incidents from 2008-2017.

The USSS identified common themes, motives, behaviors and situational factors of the attackers. It also looked at operationally-relevant details. What they found suggests these incidents could have been avoided, and the research supports the need for schools to establish comprehensive targeted violence prevention programs. There were 10 key findings, here are a few:

- All attackers experienced social stressors involving peers or a romantic partner.
- All showed concerning behavior. Most communicated a threat prior to attack, but in many cases the observer did not act or report the concerning behavior.
- Most had a history of school disciplinary actions, were victims of bullying, and/or had negative home life factors.
- Most had observable mental health, behavioral or developmental symptoms.

It is important to note none of the traits – either observed individually or several together – are firm indicators of someone planning an attack. There is no profile of a student attacker.

School administration and local law enforcement that have not yet created a program for preventing targeted violence should seriously consider doing so.

The 2018 USSS guide "Enhancing School Safety Using a Threat Assessment Model" is a good place to start. The operational guide provides basic instructions to schools interested in reducing the risk of students harming themselves or others.

The guide's recommendations are customizable, enabling schools to meet their specific needs and constraints. The USSS stresses both prevention and early intervention are the keys. The threat assessment and mitigation processes contained in the operational guide help schools achieve that goal.

(Source: USSS)

Evacuating a hospital in the middle of a wildfire

In the fall of 2017, leaders at Kaiser Permanente hospital in Santa Rosa, California, were faced with the difficult decision to evacuate the facility in the face of a fast-moving wildfire.

Hospital leadership discusses the events of that night, the decision, the hurdles they faced and other factors in this short interview (PDF, 993 KB) with the Technical Resources, Assistance Center, and Information Exchange, part of the Health and Human Services Assistant Secretary for Preparedness and Response office (ASPR TRACIE).

Staff successfully evacuated 122 patients in 3 hours using a combination of ambulances, private vehicles and city buses. This included emergency department patients and labor/delivery. The interviewees discuss how this evacuation differed from their plans and training and why those deviations worked in this case.

Highlights

U.S. Secret Service releases new research on school violence

Evacuating a hospital in the middle of a wildfire

2020 National Level Exercise to focus on cybersecurity

"Making Mitigation Work" webinar series

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.

Patient tracking was impossible due to the speed of the incident, as was supply tracking, something the facility will be addressing in its emergency plans. They also discuss facility abandonment, the damage to the campus and the decision to remove all supplies and completely restock due to smoke and heat damage – a considerable task.

While over 200 hospital staff lost their homes, not one on-duty staff member left to tend to personal matters. Both the organization and the Federal Emergency Management Agency stepped up to assist staff in the aftermath.

This interview offers a first-hand look at the decision-making process behind an evacuation. Other hospital administrators and emergency planners should read the interview and consider the lessons learned. The document also offers links to related ASPR TRACIE resources on hospital evacuation, recovery and staff support.

(Source: ASPR TRACIE)

2020 National Level Exercise to focus on cybersecurity

Every two years, the Federal Emergency Management Agency (FEMA) leads a National Level Exercise (NLE) testing response to a specific natural disasters or manmade attacks. The NLE strengthens the whole community by conducting a progressive series of preparedness events, culminating in a full-scale exercise.

Preparations for NLE 2020 are underway (PDF, 374 KB), scheduled for Spring 2020. The upcoming scenario involves widespread, adversary-based cyberattack. The exercise will have widespread cyberattacks leading to a domestic national security emergency with significant impacts on critical infrastructure and critical community lifelines.

All levels of government, the private sector, nongovernmental organizations and community groups will participate. Discuss NLE 2020 with your members or leadership now to see if your agency, organization or group may be interested in participating. Details on how to get involved will be released soon. For more information, visit the NLE website or email the NLE mailbox at NLE@fema.dhs.gov.

(Source: FEMA)

"Making Mitigation Work" webinar series

Emergency managers working to bolster their mitigation strategies should check out the "Making Mitigation Work" webinar series.

The series began in August 2019 as a way to highlight effective mitigation policies, practices and research. Each free 1-hour webinar tackles a different problem, topic or success story. This series is a joint project between the Natural Hazards Center and the Federal Emergency Management Agency.

Webinars are scheduled monthly through September 2020. Upcoming scheduled topics:

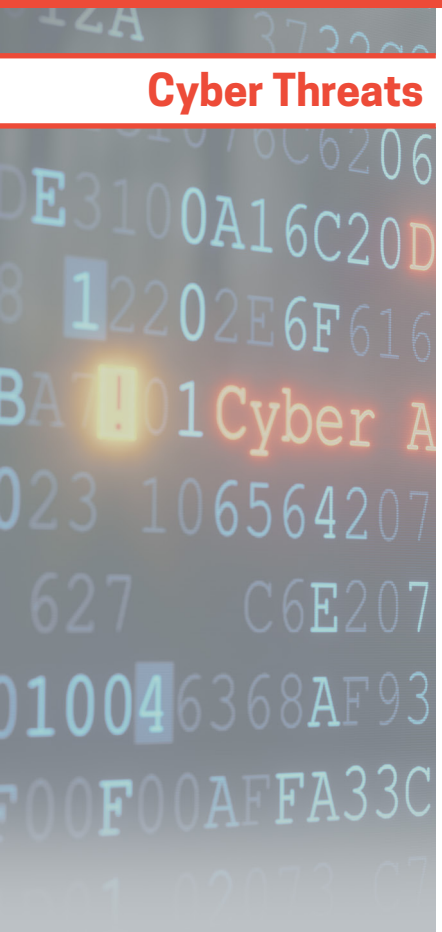
- January 14, 2020 - No Code. No Confidence: A Campaign to Strengthen National Building Code Awareness.
- February 11, 2020 - How Mitigation Helped Houston Households in Hurricane Harvey.

Registration is required for each offering, see each topic for registration link. All past webinars are available for viewing.

In addition, each webinar is worth one contact hour of emergency management training within the International Association of Emergency Managers certification program. See the Continuing Education Credits website for more information.

(Source: Natural Hazards Center)

Cyber Threats



CISA updates threat disclosure policy

The Cybersecurity and Infrastructure Security Agency (CISA) since its inception has taken a collaborative approach as part of its mission to lead civilian cybersecurity efforts from within the Department of Homeland Security.

As part of that approach, **CISA will open up its upcoming binding operational directive (BOD) on vulnerability disclosure policy for comment in the coming months**, giving agency and industry partners an opportunity to compare notes on the best way to securely share threat information.

The updated vulnerability disclosure policy will help formalize the process for researchers and ethical hackers, enlisted through agency bug-bounty programs, to give agencies a heads-up about previously unknown cyber weaknesses without alerting malicious actors.

(Source: Federal News Network)

Employees know vulnerabilities exist but can't resolve them quickly

There is a sharp remediation gap between when organizations first detect vulnerabilities and when those issues are ultimately resolved, a survey reveals.

The survey also found companies overwhelmingly do not have staff to handle security demands, and leveraging current vulnerability management tools is one of their greatest cybersecurity challenges.

Additionally, just 29 percent of companies will complete the migration to Windows 10 by January 14, 2020, the end of support deadline for Windows 7, placing an enormous number of systems at risk.

(Source: HelpNetSecurity)

Hospital data breaches could be killing patients

Data breaches at hospitals appear to be having a serious impact on patient care, increasing mortality rates for years after an incident, according to new research.

Researchers at Vanderbilt University and the University of Central Florida analyzed breach data for 3000 hospitals from 2012-2016 in an attempt to estimate the relationship between breach remediation efforts and care quality. Department of Health and Human Services breach data and Medicare Compare's public data on hospital care measures provided the data sources.

What they found was shocking: an increase in 30-day mortality rate for heart attacks that translated to 36 additional deaths per 10,000 heart attacks per year. Mortality rates apparently continued to rise for about three years after a breach before tapering off.

(Source: Infosecurity Magazine)

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