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

The InfoGram

Volume 20 — Issue 43 | Oct. 22, 2020

DHS Regional Resiliency Assessment Program

The Regional Resiliency Assessment Program (RRAP) is a voluntary program to review specific critical infrastructure jointly with local agencies and authorities. It analyzes security and resilience gaps, guides risk management decisions and can improve partnerships between the public and private sectors.

Projects are generally at least a year and include data collection and analysis along with continued technical assistance to enhance the infrastructure's resilience. Data exchange opportunities often include first responder capability assessments, voluntary facility and security surveys, and targeted studies.

Examples of RRAP projects:

- Physical internet infrastructure vulnerabilities in Loudon County, Virginia. The area serves as the primary global internet traffic hub on the east coast.
- New York City's healthcare supply chain.
- Transportation infrastructure in the Western Washington earthquake zone (PDF 226 KB), coincided with the Cascadia Rising exercise.
- Identifying biosecurity hazards and gaps in the Texas panhandle's beef industry.

RRAP projects are selected each year by the Department of Homeland Security (DHS) with guidance from federal, state and local partners. Those interested in projects can email Resilience@hq.dhs.gov for more information.

(Source: DHS)

Converge training tackles a variety of topics

The Natural Hazards Engineering Research Infrastructure (NHERI) CONVERGE training facility offers a series of 30- to 60-minute online training modules covering a variety of emergency management topics. Courses assist hazards and disaster researchers and research teams from a range of disciplines, including engineering and geophysical sciences, in applying social science best practices to extreme events research.

Information in these modules accelerates training of hazards and disaster researchers with a special emphasis on students, situational researchers and those interested in joining or leading interdisciplinary teams. The modules cover a wide range of topics and are designed to help prepare researchers to carry out extreme events research that is coordinated, comprehensive, coherent, ethically grounded, methodologically sound and scientifically rigorous.

An example of current training and future offerings:

- Disaster Mental Health.
- Social Vulnerability and Disasters.
- Conducting Emotionally Challenging Research.
- Understanding and Ending Gender-Based Violence in Fieldwork.

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

Please subscribe to receive updates and information on new CONVERGE training modules and other free online resources.

(Source: CONVERGE)

Role of ventilation, electrical wiring on arson investigation

Many variables affect how fires progress and grow, including ventilation and air flow. New research from the National Institute of Justice (NIJ) and Underwriters Laboratories looks at how ventilation affects arson fires – and how arson investigators may not fully appreciate how this variable affects their investigations.

The role of ventilation in a fire, such as an open door or window, changes the fire patterns. Researchers claim fire investigators may have a "lack of knowledge of post-flashover and ventilation-controlled fire damage." Misreading fire patterns and incorrectly identifying them as arson can lead to unnecessary prosecution and jail time for a crime that didn't actually occur.

This experiment looks not only at how ventilation affects fire patterns but also at how fire progression may be gauged from damage to electrical wiring. Using six different types of cords, testers found all eventually lost their insulation and tripped power circuits. The physical damage documented by the experiment similar regardless of the type of circuit protections used.

More research and education is needed to ensure fewer fires are unnecessarily ruled as arson.

(Source: NIJ)

Transportation Rail Incident Preparedness and Response training

Transportation of crude oil and ethanol has increased in the United States over the past decade, driven in-part by the shale oil boom. According to the Association of American Railroads, nearly 400,000 barrels of crude were transported each day in 2019; 99 percent of shipments occur without incident.

Yet incidents do sometimes happen and first responders need to be ready. The Pipeline and Hazardous Materials Safety Administration (PHMSA) offers a training program providing critical information on best practices related to rail incidents involving hazard class 3 flammable liquids, including crude oil and ethanol.

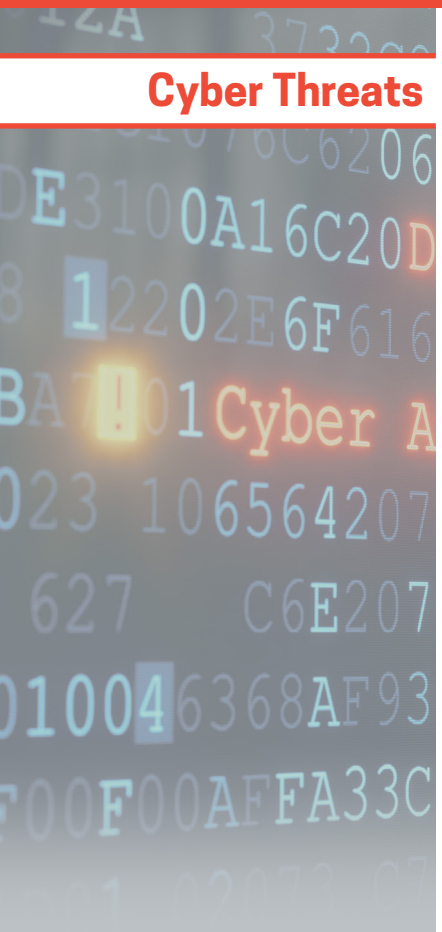
Transportation Rail Incident Preparedness and Response (TRIPR) High Hazard Flammable Trains offers a flexible approach to training first responders and emergency services personnel in hazard class 3 flammable liquids pre-incident planning and response.

The module contains an Instructor Lesson Plan, Student Workbook, Emergency Response Supplemental Information, Reference Sheet and an Evaluation Checklist.

Increased transportation of crude oil and ethanol by rail calls for increased awareness, better hazardous materials planning and more robust training to better respond to incidents when they happen. A key component of this initiative is to learn from past experiences and to leverage the expertise of public safety agencies, rail carriers and industry subject matter experts to prepare first responders to safely manage incidents involving flammable liquid unit trains.

(Source: Department of Transportation)

Cyber Threats



When you can't have it all, build cyber resiliency instead

One challenge government entities and the public sector face is how to secure legacy IT systems without the budgetary, labor or infrastructure resources required to upgrade them. Even when new staff and new technology are included in the roadmap, the transition time is inevitably longer than can be afforded.

One solution is to build resilience into existing infrastructure. Effective cyber resiliency ensures data protection as well as operational and business continuity – going beyond traditional cybersecurity defense to build a more adaptive, proactive and embedded security stance.

(Source: HSToday)

New NIST tool helps assess why employees click on phishing emails

Researchers at the National Institute of Standards and Technology (NIST) have devised a new method that could be used to accurately assess why employees click on certain phishing emails.

The tool Phish Scale uses real data to evaluate the complexity and quality of phishing attacks to help organizations comprehend where their (human) vulnerabilities lie.

Any company or organization that takes its cybersecurity seriously conducts regular phishing training exercises to see if its employees can distinguish between real and phishing emails. These trainings aim to increase employee vigilance as well as teach them to spot signs of phishing attacks masquerading as legitimate emails.

(Source: WeLiveSecurity)

Meet 'Egregor,' a New Ransomware Family to Watch

Researchers have been analyzing a new ransomware family that calls itself "Egregor." Attackers behind the malware typically operate by breaking into organizations, stealing sensitive data and running the malware to encrypt their files.

Researchers say it contains anti-analysis techniques such as code obfuscation and packed payloads. In one of its execution stages, the payload can only be decrypted if the proper key is entered. This means the file can't be analyzed unless someone enters the same command line used to run the payload.

Egregor's ransom note promises that if the ransom is not paid within three days, the attackers will leak part of the stolen data and alert the victim company's partners and clients via mass media so they know of the breach.

(Source: DarkReading)

Gangs are shifting targets and upping their ransom demands

Ransomware attacks continue to grow, which also suggests ransomware gangs are upping ransomware demands and getting more sophisticated about how they calculate the ransom they try to extort.

With attackers actually stealing company data, ransomware attacks are also becoming data breaches, which for some companies can bring additional risk of fines from regulators. Indeed, in some cases attackers were thought to name their ransom according to the regulatory fines organizations would have to pay.

(Source: zdnet)

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