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

The InfoGram

Volume 19 — Issue 39 | October 24, 2019

2019 Wildfire Risk Report, new prediction methods

The 2019 Wildfire Risk Report, released in September, found over 775,000 homes at extreme risk of wildfire damage in the western United States. Estimated reconstruction cost for these homes top $221 billion.

This report evaluates potential exposure of residential properties to wildfire in a defined region. Not surprisingly, California and Texas top the list of states in the high- and extreme-risk categories. Three metropolitan regions in California see 42 percent of residences at high-to-extreme wildfire risk. This is due to population density as well as the expanding residential spread into wildland urban interface areas.

Data from 1985-2018 show an increase in the amount of acreage burned when compared to the overall number of fires. 2018 was another record-breaker with 8.7 million acres burned, the sixth-highest total in over 100 years of data. The 13 states in this report have the highest history of acreage burned and highest loss of life and property, and also possess the highest probability of future property loss due to wildfire.

Planners and emergency managers may have a new tool in their toolbox to help forecast how severe a wildfire may be. Using modeling based on a number of key variables, a new machine learning algorithm can help forecast whether a wildfire will be small, medium or large.

Researchers tested this new modeling technique using Alaska data from 2001-2017. The model predicted 40 percent of ignitions would lead to large fires; ultimately they accounted for 75 percent of the total burned area. They found this model outperformed other algorithms, but that there was still some overprediction in some cases.

If refined to the point where it is more reliable, this kind of modeling can be useful to those in charge of allocating firefighting resources, declaring evacuation warnings and can have an impact on other related fields such as ecology and land management.

(Source: International Journal of Wildland Fire and CoreLogic)

New online webPOISONCONTROL digital triage poison center

In keeping with the times, the Poison Control Center now has an online option. webPOISONCONTROL is a web-based triage tool to guide people who may have been exposed to a poisonous substance through a series of questions to determine toxicity and needed treatment.

This is the first fully automated virtual poison center. Created in-part to meet the changing way the public accesses health information, the interactive tool guides you through specific exposure questions and patient details in the same way a call taker would.

Algorithms also list the expected minor symptoms and the symptoms which require further medical evaluation, specify home treatment where appropriate, define the onset and duration of symptoms, and set a risk window beyond which significant

Highlights

2019 Wildfire Risk Report, new prediction methods

New online webPOISONCONTROL digital triage poison center

CFATS revision: Congress works on new chemical security amendments

Pre-Disaster Recovery Planning Guide for Tribal Governments

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

toxicity is unlikely if clinical manifestations have not already begun.

The logic, algorithms and recommendations powering the tool are written by board-certified toxicology experts, each with decades of experience in poison control.

webPOISONCONTROL is also available as an app for both Android and iPhone. The mobile app has the added feature of product barcode scanning, saving some time for people who need fast answers and have the product packaging nearby.

As always, people can call the Poison Control call center toll-free at 1-800-222-1222.

(Source: webPOISONCONTROL)

CFATS revision: Congress works on new chemical security amendments

Congressional authorization and funding for the Department of Homeland Security's (DHS) Chemical Facility Anti-Terrorism Standards (CFATS) program will expire in April 2020. Legislation has been introduced to amend the program and extend it through May 1, 2025.

CFATS is the first regulatory program focused specifically on security at high-risk chemical facilities. The Cybersecurity and Infrastructure Security Agency (CISA) manages the CFATS program by working with facilities to ensure they have security measures in place to reduce the risks associated with certain hazardous chemicals and prevent them from being exploited in a terrorist attack.

The threat is not just from terrorism, though. Cybersecurity is quickly becoming a serious concern to chemical and industrial facilities – one that still needs to be adequately addressed. Natural events such as hurricanes, tornadoes or earthquakes also pose a significant risk to facilities, workers within the industries and nearby communities.

Recent hearings included testimony calling for adding even more CFATS regulation to chemical and industrial facilities. Some recommendations include adding water treatment and maritime facilities to the program, adding protections against cybersecurity threats, involving employees more and requiring DHS to verify statements by facilities claiming to no longer fall within CFATS jurisdiction.

(Source: CISA)

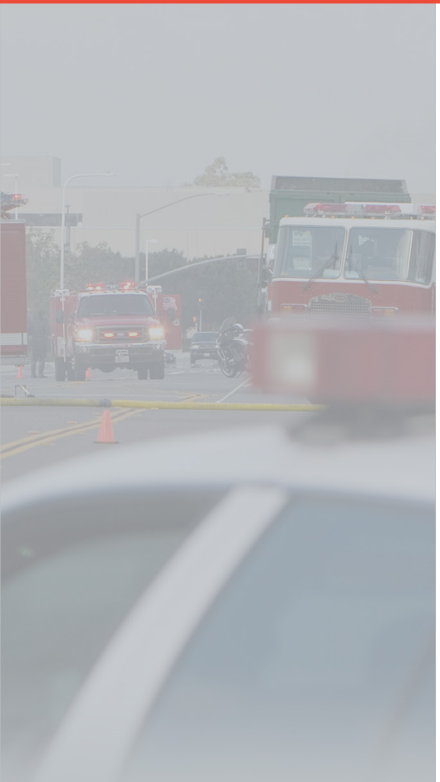
Pre-Disaster Recovery Planning Guide for Tribal Governments

The Federal Emergency Management Agency (FEMA) just released Pre-Disaster Recovery Planning Guide for Tribal Governments, designed to prepare tribal governments for recovery efforts from future disasters by engaging with the whole community and planning for recovery activities that are comprehensive and long term.

The guide provides a range of planning activities, from basic to formal steps that include establishing recovery leadership, engaging the community, identifying existing resources and creating new partnerships that can help all tribal governments build resilience.

FEMA developed the guide in alignment with its 2018-2022 Strategic Plan goal of maturing the National Disaster Recovery Framework. The guide is the final product in a series of three pre-disaster planning guides: the Pre-Disaster Recovery Planning Guide for State Governments was released in 2016 and the Pre-Disaster Recovery Planning Guide for Local Governments was released in 2017.

(Source: FEMA)



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

Attacks bypassing multi-factor authentication on the rise

Last month, the FBI sent a security advisory to private industry partners detailing the **rising threat of cyberattacks that can bypass multi-factor authentication** (MFA) solutions. The FBI made it very clear that its alert should be taken only as a precaution, and not an attack on the efficiency of MFA, which the agency still recommends.

(Source: zdnet)

Vulnerabilities in 3rd-party software a risk to medical devices

The Food and Drug Administration (FDA) is informing patients, health care providers and facility staff, and manufacturers about **cybersecurity vulnerabilities that may introduce risks for certain medical devices and hospital networks**. The FDA is not aware of any confirmed adverse events related to these vulnerabilities. However, software to exploit these vulnerabilities is already publicly available.

A security firm has identified 11 vulnerabilities, named "URGENT/11." These vulnerabilities may allow anyone to remotely take control of the medical device and change its function, cause denial of service, or cause information leaks or logical flaws, which may prevent device function.

(Source: FDA)

Access rights not updated for nearly half of employees changing roles

Almost half of employees who switch roles within a company retain unnecessary network access rights, according to the results of a new survey.

The online survey questioned 400 people, of whom 70% were IT professionals, about what happened in their company when new staff were onboarded and when current employees switched roles or were deprovisioned.

Asked whether unnecessary access rights are removed when employees change roles, 45 percent of the respondents said "no." This statistic swells in importance when paired with the knowledge that more survey respondents worked for the government (14.5 percent) than for any other industry.

(Source: Infosecurity Magazine)

What cybercriminals steal when they hack hospitals

When hospitals have access to your electronic medical record, you get better care. Depending on what you're admitted for, readily available digital health information could be the difference between life and death.

But information made digital is information made hackable. Hackers nab more than just your credit cards, social security number and other demographic and financial information tied to your identity. **Hospital breaches include theft of sensitive health information**. It's modernity's big tradeoff between data access and data security. It's also a challenge for the next generation of precision medicine because a big-data-scale aggregate of detailed, sensitive health information is crucial for developing tomorrow's treatments and cures.

(Source: Forbes)

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